CIGRE Green Books
Compact Studies

CIGRE
Study Committee B5: Protection and Automation

Peter Bishop
Nirmal-Kumar C. Nair *Editors*

IEC 61850 Principles and Applications to Electric Power Systems

Second Edition

cigre

Springer

CIGRE Green Books

Compact Studies

Series Editor

CIGRE, International Council on Large Electric Systems, Paris, France

CIGRE presents their expertise in compact professional books on electrical power networks. These books are of a self-contained concise character, covering the entire knowledge of the subject within power engineering. The books are created by CIGRE experts within their study committees and are recognized by the engineering community as the top reference books in their fields.

Peter Bishop · Nirmal-Kumar C. Nair
Editors

IEC 61850 Principles and Applications to Electric Power Systems

Second Edition

With 187 Figures and 31 Tables

cigre

Springer

Editors
Peter Bishop
HVDC and Operational Engineering Grid Delivery
Transpower New Zealand Ltd.
Wellington, New Zealand

Nirmal-Kumar C. Nair
Department of Electrical Computer and Software Engineering
University of Auckland
Auckland, New Zealand

ISSN 2367-2625 ISSN 2367-2633 (electronic)
CIGRE Green Books
ISSN 2509-2812 ISSN 2509-2820 (electronic)
Compact Studies
ISBN 978-3-031-24566-4 ISBN 978-3-031-24567-1 (eBook)
https://doi.org/10.1007/978-3-031-24567-1

This second edition of the book includes publication quality corrections. The technical content remains unaltered.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Foreword

CIGRE Study Committee B5—Protection and Automation focuses on protection, control, monitoring and metering and aims to cover the whole power system, end-to-end related to this topic, from transmission systems, to distribution systems, including generation and HVDC systems.

Study Committee B5 promotes the synthesis and dissemination of state-of-the-art practices, recommendations and information about power system protection and automation on a worldwide basis. Its main activities cover the principles, design, application and management of power system protection, substation control, automation, monitoring, recording and metering, as well as the associated internal and external communications and interfacing for remote control and monitoring. SC B5 aims to be an independent analyzer of different solutions and provider of high-quality unbiased publications and contributions to the electrical supply industry.

Members of SC B5 from all regions of the world provide a global perspective on the issues and challenges facing the protection of electrical power systems, aimed at top and medium management and technical staff of utilities, suppliers and consultants, universities and research centres, including young and experienced engineers alongside standardisation organisations.

CIGRE Study Committee B5 strategic technical directions address the main objectives set by CIGRE Technical Committee. The strategic directions set by SC B5 aim to facilitate the human development and application of new technology to improve the efficiency of the engineering, design, operation and maintenance of protection and automation of electric power systems and keeping the spirit of collaboration that distinguishes CIGRE among other organisations around the world.

SC B5 has worked with the IEC 61850 Standard for more than 20 years. IEC 61850-based power system protection and automation systems have significant technical and commercial advantages over the conventional ones, and it is time to deploy the technology and take full advantage of its benefits for the power industry. In this CIGRE Compact Studies book, the experience related to IEC 61850 system from SC B5 members are addressed.

I would like to give a special recognition to Mr. Peter Bishop and Dr. Nirmal Nair for their contributions as Editors of this Green Book. Please enjoy the further study of this book!

Oslo, Norway
April 2022

Rannveig Loken
CIGRE Study Committee B5 Chair

Preface

This CIGRE Green Book aims to provide a compact overview on IEC 61850 principles and applications to electric power systems. It is compiled using technical brochure and technical paper material that is based on existing practice of IEC 61850 systems (application, use and approach) that gives stakeholders from different disciplines (and levels of knowledge) an understanding of systems in use, their features, how they are applied and approach for implementation. It covers the complete lifecycle from specification, deployment, operation to maintenance and replacement.

IEC 61850 is the international Standard applicable to Protection, Automation and Control Systems (PACS). The scope of IEC 61850 implementation continues to grow in a wide range of areas including

- protection,
- automation,
- System Control And Data Acquisition (SCADA),
- metering and
- condition monitoring.

IEC 61850 provides the engineering definitions and processes for configuration and parameterisation of the functions required for digital communication between Intelligent Electronic Devices (IEDs) in the substation and the related system requirements. It is therefore not a protocol itself but rather the configuration of IEDs with interoperability to communicate using a protocol. It is a key part of a digital substation.

The readers of this Green Book will vary in the extent of familiarity with IEC 61850 as a concept and indeed their experience in using it. As the application of the IEC 61850 has many different aspects, there would be very few, if any, who would dare to say they “know it all” even after the many years that it has been in active deployment around the world.

IEC 61850 systems provide users with the opportunity to review primary and secondary functionality they wish to implement and their existing philosophies, not just in the area of communications but in all areas of existing and emerging power systems.

These changes will impact on many fields such as primary system design, protection design, SCADA design, system architecture, governance, operational work and site commissioning.

The target audience includes both primary and secondary system engineers, power system planners, technicians, teachers and researchers tasked with exploring, developing, delivering these systems. The audience will also include engineers from non-B5 Study Committees. Since IEC 61850 covers multiple disciplines, it will assist protection, SCADA, communication and Information Technology staff by detailing how IEC 61850 will affect their systems. This Green Book is a compact study for a broad audience, and while PAC details are included, it is not intended to be a comprehensive IEC 61850 technical reference book solely for Protection and Automation engineers.

The overall Green Book provides a "concise" practical guide for any organisation and associated users embarking on the adoption or expansion of IEC 61850 in its engineering processes and system deployments. It gives examples of approaches and applications of systems that have been implemented. While it could be read cover-to-cover in its entirety, some may focus particularly on the chapters that are especially relevant to them. The following serves as a rough guide to the principle chapters for each activity "theme". This also serves as a "checklist" of the readiness of any organisation to commence an adoption project and where consideration of each chapter fits into the plan.

Activity theme	Chapters	Description
Need and Benefits	Chap. 1 – IEC 61850 as an Enabler to Meet Power System Challenges	This sets out the broader reasons and advantages for applying IEC 61850-based system. Illustrating its application to meeting emerging and traditional power system challenges.
Concepts	Chap. 2 – Introduction to IEC 61850 Systems	This provides an overview of the standard, its history and some concepts.

Activity theme	Chapters	Description
User Specification	Chap. 3 – IEC 61850 User Specifications, Standards and End Users	The variety of implementations and functional requirements requires a strong approach to user specification to ensure the system meets all needs.
Communication Architecture and Required Services	Chap. 4 – IEC 61850 Communication Architectures and Services	This describes and provides examples of LAN arrangements with options and considerations to meet your performance and operational needs.
	Chap. 5 – Time Synchronisation for IEC 61850 Systems	This describes time synchronisation and its criticality depending on your implementation. It includes considerations methods and examples.
	Chap. 6 – Cybersecurity Integration with IEC 61850 Systems	As a LAN-based communication technology, cyber security measures must be a specific inclusion in the deployment considerations.
Planning and Design	Chap. 7 – Planning and Design for IEC 61850 Implementation	With concepts, need and requirements described in the previous activity themes, this gives some guidance to the process of system lifecycle planning and design based on previous user experience.
System Implementation and Testing	Chap. 8 – Implementation for IEC 61850 Functional Schemes	Review of worldwide examples of different types of functional schemes (goose and sampled values) and their implementation considerations.
	Chap. 9 – Testing of IEC 61850 System Solutions	Theory is nice, but this is where it all comes together requiring a different approach to traditional testing to prove the readiness for operational use.
	Chap. 10 – Vendor Interoperability of IEC 61850 Systems	Key considerations for ensuring multi-vendor device interoperability to achieve full benefit of IEC 61850 solutions. As a vendor-agnostic engineering process, there is a requirement to understand the requirements for selecting devices that meet the functional and interoperable requirements of the system.
Substation & Inter-Substation Applications	Chap. 11 – CT/VT Sampled Value Acquisition Applied to IEC 61850	CT/VT Sampled Values, if you choose to implement, is the mechanism of digitalisation of all the primary sensor signals that allows elimination of many wires from the CTs, VTs and other sensors. Emerging developments are discussed.

Activity theme	Chapters	Description
	Chap. 12 – Process Bus Applications in IEC 61850	The process bus is described as the digital communication connection between the bay level devices and the process level devices such as circuit breakers and instrument transformers or associated digital merging units. Many considerations are involved in associated applications which form an important part of a digital substation—this has been termed "Process Bus" as it refers to messages only related to the process equipment, i.e. this is a significant step in completing the fully "digital substation" moving completely away from all analogue signals. Global examples are shared.
	Chap. 13 – Wide Area Implementations of IEC 61850 Substation Systems	IEC 61850 now incorporates communication between substations. Wide area applications that incorporate both samples values and GOOSE commands are increasingly important in our interconnected power system. As a system dealing with all of the utility operational communication requirements, the wide area aspects need particular understanding.
	Chap. 14 – IEC 61850 for SCADA Applications	Digital control and supervision of the power systems and it functions helps advance to the operation of the power system and early disability of issues that require attention
Maintenance and Asset Management	Chap. 15 – Maintenance and Asset Management for IEC 61850 Systems	Maintenance and asset management is different for IEC 61850 systems, particularly with the absence of wiring, less use of traditional drawings and increase in available intelligence. The absence of physical isolation and test links is the start of the operational requirements, but the vast array of easily accessible data can aid in dramatically improving reliability and resilience of the system, and hence of the primary power system.

Activity theme	Chapters	Description
Beyond the Substation Applications	Chap. 16 – Applying IEC 61850 Applications Beyond Substations	Application and examples of IEC 61850 outside of conventional three-phase AC transmission and distribution systems are growing, particularly its use in electric traction systems, electric vehicles, wind & hydro generation plants and HVDC applications.

Wellington, New Zealand — Peter Bishop
Auckland, New Zealand — Nirmal-Kumar C. Nair

Acknowledgments

This book is based on existing CIGRE technical documents and the active participation of a group of experts to produce the chapters. The COVID pandemic made it impossible for the writing team of experts from across the world to meet the preferred way, i.e. in-person. Instead, their patience to work together through several online meetings is appreciated. These experts have added valuable new material, along with the inclusion of historical material. We acknowledge their dedicated role, along with the previous working groups and paper authors who have produced the related technical brochures and papers on the associated topics.

We are also indebted to study committee B5 chair Rannveig Loken for her active support, participation and encouragement in the process of completing the manuscript. As this book concept was originally initiated in 2014 (before our effort was reinitiated in 2018 with an agreed terms of reference), we also acknowledge previous SC B5 chair Iony Patriota de Siqueira and initial book convenor Ian Young for their initial development.

We thank Volker Leitloff for his significant feedback and review of draft book chapters. Other valuable feedback and support is appreciated, particularly from Klaus-Peter Brand, Daniel Espinosa and Richard Adams.

We are also indebted to a wide range of organisations for their support in terms of the contributions provided by their employees and endorsing the use of case studies and examples included in the book. Particular thanks to Scottish Power, Transgrid Australia, Landsnet Iceland, RTE France, Statnett Norway, National Grid UK, Vector NZ for the case studies and examples. We also acknowledge and thank University of Auckland and Transpower NZ Ltd. for granting Nirmal Nair and Peter Bishop respectively considerable time, support and physical meeting facilities while they coordinated and managed the completion of the book manuscript. The several face-to-face editorial meetings between us as the editors in Auckland, Wellington and Christchurch, during 2020–2022, have helped shape the quality and value of this much awaited book among protection, automation and control system professionals, practitioners and researchers across the electrical power system sectors globally.

Personally, we would also like to thank our family and friends for their moral and emotional support to help complete this important assignment for CIGRE B5 study committee. This was particularly important as, like others globally, we navigated our professional commitments also from home during various levels of lockdown periods during the last couple of years.

A big thanks to readers and particularly practising engineers from the electricity infrastructure space for keeping the lights on across your networks. Hopefully, this book will help engineers educate, understand and apply IEC 61850 better, as it is increasingly important for today's electricity networks.

Further thanks to the International Electrotechnical Commission (IEC) for permission to reproduce information from its International Standards. All such extracts are copyright of IEC, Geneva, Switzerland. All rights reserved. Further information on the IEC is available from www.iec.ch. IEC has no responsibility for the placement and context in which the extracts and contents are reproduced by the author, nor is IEC in any way responsible for the other content or accuracy therein.

Wellington, New Zealand
Auckland, New Zealand
April 2022

Peter Bishop
Nirmal-Kumar C. Nair

Contents

Editors and Contributors

About the Editors

Peter Bishop is presently Principal Protection and Automation Engineer with Transpower NZ Ltd., the transmission utility in New Zealand. He holds an Electrical and Electronic Engineering Degree from the University of Canterbury (NZ) and is a Chartered Professional Engineer.

Peter has over 25 years' experience in power system protection engineering support and management for a transmission utility and protection manufacturer. This experience has included protection operation and application analysis, setting studies, simulation and testing, training, investigations and project support. He was a member of a cross-functional team which travelled internationally gathering experience and information on substation automation for future application for Transpower. In recent years at Transpower, he has managed the protection technical support response for power system faults, equipment failures and outages.

Peter is convenor of CIGRE Australia B5 mirror panel and has been a co-special reporter at the 2017 SC B5 colloquium.

Nirmal-Kumar C. Nair received his B.E. in electrical engineering from Maharaja Sayajirao University, Vadodara, India, M.E. (Gold Medal) in high voltage engineering from Indian Institute of Science, Bengaluru, India, and Ph.D. in electrical engineering from Texas A&M University, College Station, USA. He has held several professional and research positions in India, USA and New Zealand (NZ). Currently, he is a tenured faculty at the Department of Electrical, Computer Engineering and Software Engineering at University of Auckland, New Zealand.

His interests include power systems analysis & operation, protective relaying, automation & optimisation in the context of smart grid, electricity markets and integration of DG/renewable sources into bulk power system. He has special ongoing interest in voltage collapse, blackouts, resilience, cyber-physical security and special protection schemes. To date, he has contributed to about 290+ refereed conference and journal papers and has been actively offering his services by reviewing for several reputed journals and conferences. He has co-authored two books, several book chapters and inventor on two patents around areas relevant to power system relaying and automation. He is passionate about developing lifelong learning opportunities for engineers, energy policy and media engagements around zero-carbon energy transition/adaptation

Nirmal serves as Executive of CIGRE New Zealand (NC) National Committee since 2008, Secretary (2014–2017), Treasurer and Event Manager (2018–2021) and currently Technical Chair (2022). He won the competitive bids to host CIGRE Auckland 2017 that incorporated CIGRE B5 Colloquium, CIGRE Administrative Council meeting and CIGRE-AORC Technical and administrative meeting altogether between 11 and 17 September 2017. He has been the event manager for CIGRE NZ events since 2017, focusing on end-to-end theme with increased focus on sub-transmission/distribution voltages.

For CIGRE B5, he has been NZ Observer Member (2010–2018) and currently serves as Technical Advisor for New Network Requirements (2019–) and Tutorial Advisory Group Member (2017–). He has actively contributed towards the development of CIGRE B5 (2019–2028) strategic plan. He has been involved with five B5 working groups (four completed with one as Convenor and three as Regular Member, one ongoing as Convenor); two Task Forces completed including one for B5 Green Book; five CIGRE Paris papers and four CIGRE regional event papers; 2018 Special Reporter to B5 Preferential subject and 2021 CIGRE Centennial B5 Tutorial Contributor. He received recognition as CIGRE Distinguished Member in 2018.

Contributors

Mark Adamiak Adamiak Consulting LLC, Paoli, USA

Alex Apostolov OMICRON Electronics, Los Angeles, USA

Peter Bishop Transpower NZ Ltd, Wellington, New Zealand

Calum Dalmeny Chronos Technology, Lydbrook, UK

Herbert Falk OTB Consulting Services LLC, Troy, USA

Marcel Geor Microchip Technology Inc., Lower Hutt, New Zealand

David Hewings Network Rail, Cardiff, UK

Dennis Holstein OPUS Consulting Group, Seal Beach, CA, USA

Rod Hughes Rod Hughes Consulting, Aberfoyle Park, SA, Australia

Pablo Humeres Flores CGT Eletrosul, Florianopolis, Brazil

Richard Hunt Quanta Technology, Raleigh, NC, USA

Anders Johnsson Vattenfall Eldistribution, Solna, Stockholm, Sweden

Rannveig S. J. Løken Statnett, Oslo, Norway

Priyanka Mohapatra Scottish Power, Glasgow, Scotland

Nirmal-Kumar C. Nair University of Auckland, Auckland, New Zealand

Janez Zakonjšek Relarte Ltd., Bohinjska Bistrica, Slovenia

IEC 61850 as an Enabler to Meet Power System Challenges

1

Peter Bishop and Pablo Humeres Flores

Abstract

This chapter sets out the broader reasons and advantages for applying IEC 61850-based systems. The significant global societal and related power system changes are explained. Resulting power system challenges are stated. The chapter then illustrates the features and applications of IEC 61850-based systems to enable solutions that meet the emerging and traditional power system challenges.

Keywords

Power system • Society • Challenges • Global • Transformation • Technology • IEC 61850 • Enabler

1.1 The Changing Power System and Related Drivers

The profound transformations undergoing the electrical industry in recent decades are in a large way reflective of changes in our society. These transformations bring new requirements and opportunities for the power sector, and particularly to Protection, Automation and Control System (PACS). Features of the IEC 61850 standard make it an enabler in developing and applying schemes that address the challenges from the societal and resulting power system changes. IEC 61850 is

P. Bishop (✉)
Transpower NZ Ltd., Wellington, New Zealand
e-mail: peter.bishop@transpower.co.nz

P. Humeres Flores
CGT Eletrosul, Florianopolis, Brazil
e-mail: hpablo@cgteletrosul.gov.br

P. Bishop and N.-K. C. Nair (eds.), *IEC 61850 Principles and Applications to Electric Power Systems*, CIGRE Green Books, https://doi.org/10.1007/978-3-031-24567-1_1

also well suited to continue address traditional power system and protection and automation challenges [1].

The world is moving towards being more socially and economically inclusive. This means more people demanding a more comfortable living that needs energy. On the other hand, environmental awareness points to the need for other sources of energy, which will even change over time as it is possible to develop new knowledge and, consequently, new technologies. The interesting thing is that in this scenario, electricity has a fundamental role. Being the option applied by the final devices (motors, cars, lighting, heating, etc.) it is possible to change the matrix of the sources that produce energy (nuclear, coal, water, sun, wind, etc.) over time while maintaining the same infrastructure that distributes the energy and without affecting the final devices used.

To apply the grid changes that are required in the near future, there is also pressure on utilities (transmission, distribution and generation) to implement grid projects quickly, economically and with existing human resource levels. Features of IEC 61850 are also an enabler to help meet these utility pressures.

1.1.1 Changes in Society

While the twentieth century was a time of rapid and significant societal change and growth, continuing growth and change appears to be accelerating in the initial years of the twenty-first century.

During the twentieth century, there were great shifts in the way many people have lived. This occurred due to changes in technology, economics, culture, medicine and politics. The rate of change has continued into the twenty-first century with further technological progress, rise in the global economy, urbanisation and concern over world social and environmental issues.

Also with the greater use of technology, growth of economies and increased travel there is a greater expectation for reliability and cost-effectiveness of systems that support greater living standards.

1.1.2 Environmental Change

Concern for the environment and associated guardianship has been present throughout history, particularly in some cultures and in some parts of the world. However, particularly with increased awareness of increasing global environmental issues there is a greater call for action. Environmentalism advocates for the preservation, improvement and sustainable care for the natural environment.

Environmental issues of rising concern include pollution, reducing natural resources, and climate change. Increasing global warming due to large-scale greenhouse gas emissions and altered weather patterns leading to severe weather extremes are features of climate change.

The burning of fossil fuels for energy consumption is a major cause of the greenhouse gas emissions. Power systems have traditionally emitted greenhouse gases with the burning of coal, oil and gas fossil fuels to generate electricity. With society and government policy pressure, power systems are in the process of changing to move away from electricity based on fossil fuel generation.

It is also noted that extreme weather conditions are having a significant effect on power systems, whether it be increased risk for forest fires or damage during more severe hurricanes.

1.1.3 Technology Change

Over centuries, innovative methods and new technologies are developed and deployed. Emerging technologies are wide ranging across educational technology, information technology, nanotechnology, optics, biotechnology, cognitive science, psychotechnology, robotics and artificial intelligence. While these technologies are being applied across our society, significant application is occurring within power systems particularly in the areas of renewable generation, energy storage and communication networks.

1.1.4 Social Change

Social change refers to shifts overtime in behaviour and cultural values. Contributing factors include changes in population, technology and information systems.

In recent decades, a significant redistribution has occurred in global population. The world is becoming more globally interconnected, sharing values and aspects of concern. Also developing countries are becoming a greater proportion of the world population. Along with increases in standard of living and societal systems in many countries of the world, there are greater expectations for accelerated advances in the development, reliability, cost-effectiveness and sustainability of infrastructure. These changes have influenced how power systems have changed. Figure 1.1 illustrates some specific areas of change impacting on the electricity industry.

1.1.5 Changing Power Systems and Energy Sector

Electricity supply systems play a key role among all critical infrastructures in contemporary societies. From the supply of water, goods, gas, oil, medical services, home automation, telecommunication, security and many other infrastructure sectors, all depend on the reliable and economic supply of electricity.

Following the current revolution brought about by societal changes including “smart things” and the explosive growth of the Internet, electricity supply systems

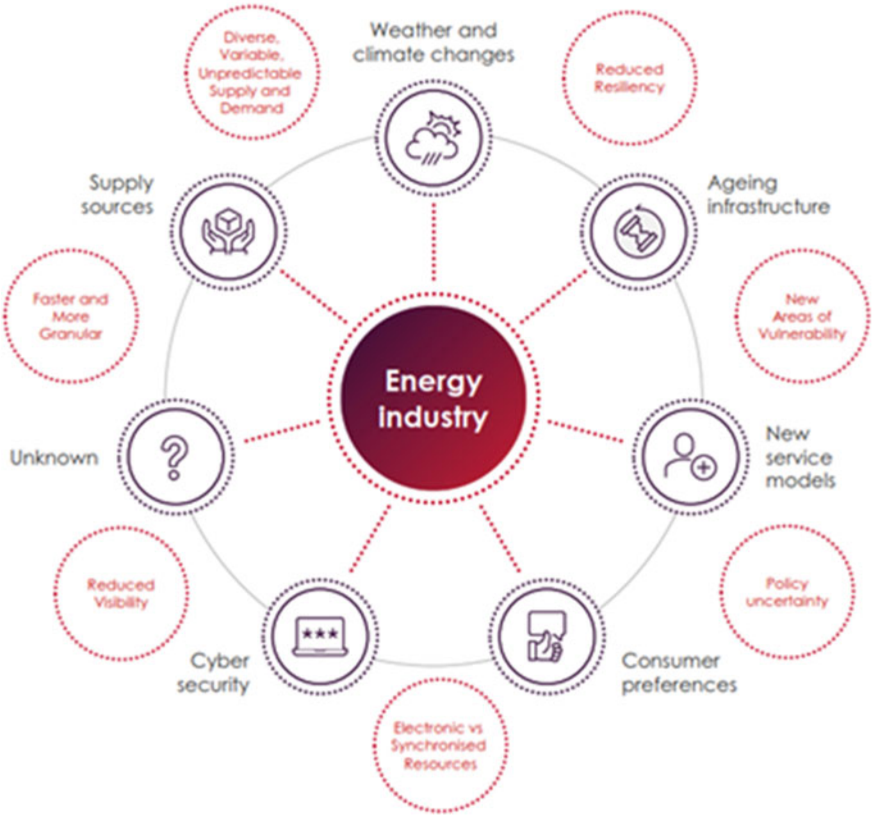


Fig. 1.1 External influences on the power industry (*Source* CIGRE 2018 Paris Keynote Presentation)

must keep pace with all these changes in order to continue to provide the quality of service necessary for these applications. Most of the changes and innovations in power system components and overall power system planning and operation methods are paralleled with developments in other industries, which have been adopted slowly from their relevant sectors, e.g. power electronics, robotics and information technology. Power systems are likely to become more transactional, based around the concept of service provision, and this will require reliable and robust data to support the economic cost recovery mechanisms [1].

The trend of making use of alternative energy resources is resulting in the restructuring of the electric power grid as we know it today. It is estimated that over the next 20 years, millions of windfarms and multi-megawatt photovoltaic plants will be connected to transmission networks and that tens of millions of Distributed Energy Resources (DER)—both renewable and non-renewable—will be connected worldwide to the grid—to both transmission and distribution networks. Existing bulk energy storage technologies, like pumped storage schemes, will be complemented by new technologies such as batteries and flywheels. Distributed Energy Resources will be connected mostly at the lower network voltages, many of which were not designed to cater for embedded generation. As shown in Fig. 1.2, the current structure of electrical grids is usually represented as a linear connection among the generation, transmission, distribution and consumer, where the transfer of power occurs in a one-way direction. With the evolution of distributed generation and storage, the future electrical network is seen as a complicated smart grid, capable of interconnecting and transferring power between many different sources, in a two-way direction. The endpoints can vary from any kind of power plant like photovoltaic, small hydro, Stirling machines, nuclear, battery storage, geothermal, wind, fuel cell, combined cycle, combustion turbines, reciprocating engines, tidal power, etc. These distributed sources and destinies can also be combined as virtual power plants, and managed as a unique source, and also operated interconnected or isolated from the rest of the grid in case of emergencies, as a microgrid [2].

The full exploitation of all new technologies available in the generation, transmission, distribution and consumer domains of power systems is only possible with the availability of modern resources for communication among devices, systems and players, identified as one of the main pillars of a smart grid. These communication trends include developing automation requirements, the needs for advanced metering infrastructure (AMI) and inter-substation communication and the telecommunication network convergence (packet-based switching network capable for transmitting multiple services simultaneously) [1].

In parallel to the trends in telecommunication convergence, the information processing in the power sector is steadily adopting the main developments from information technologies. The fifth generation of informatics, featuring distributed

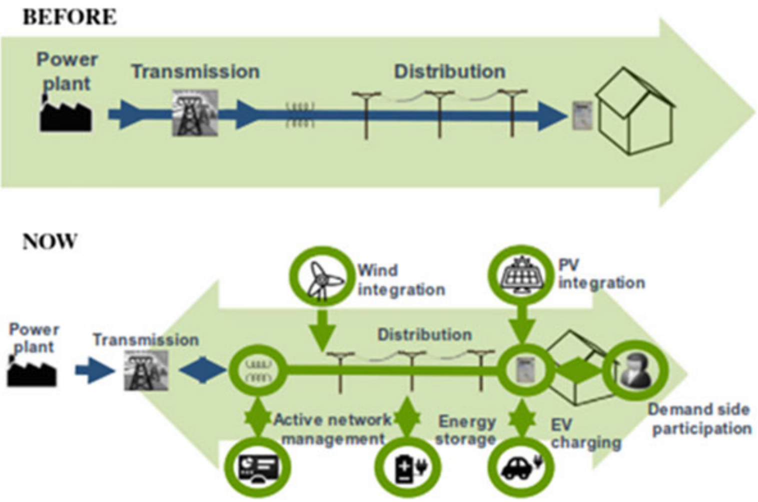


Fig. 1.2 Unidirectional power flows are becoming multi-directional (*Source* CIGRE Green Book 'Electricity Supply Systems of the Future', Introduction and Overview, Figure 21)

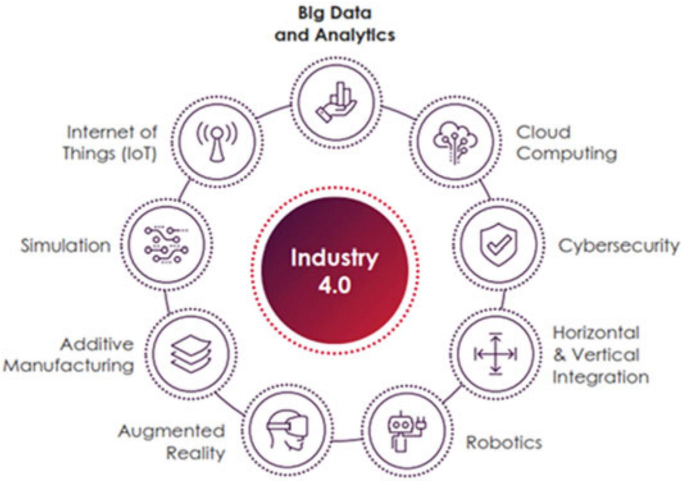


Fig. 1.3 Industry informatic trends (*Source* CIGRE 2018 Paris Keynote Presentation)

hardware and software, is being deployed in digital substations, and seen as one of the main drivers for the development of future applications. Aspects such as remote access systems and cybersecurity are key considerations for power system implementations. Reference is made to Fig. 1.3 which highlights industry informatic trends [1].

As part of the evolution of power system automation, the development of a fifth generation of implementation technology is underway. This fifth generation is related to the use of distributed hardware and automated software. New types of high-voltage sensor systems are being employed, such as Rogowski coils, gas voltage sensors and optical sensors. Besides employing all new developments in informatics and telecommunication, mainly guided by the standard IEC 61850, substation and inter-substation automation are being planned with new applications based on the concept of synchrophasors. Refer to Chap. 13. Control centre automation is the central focus of current development aiming to provide intelligence to the grid operation. Figure 1.4 highlights a range of distributed data sources and the flow of information across the power systems. It also shows the associated data processing sites where automation functionality is applied.

There are also societal trends and governmental and international polices which will have a huge impact on the future grid [1]:

- Environmental considerations and agreements (Kyoto protocol and Paris accord on climate change) are limiting options for generating type and power line construction.
- Disengagement from nuclear power in some countries.

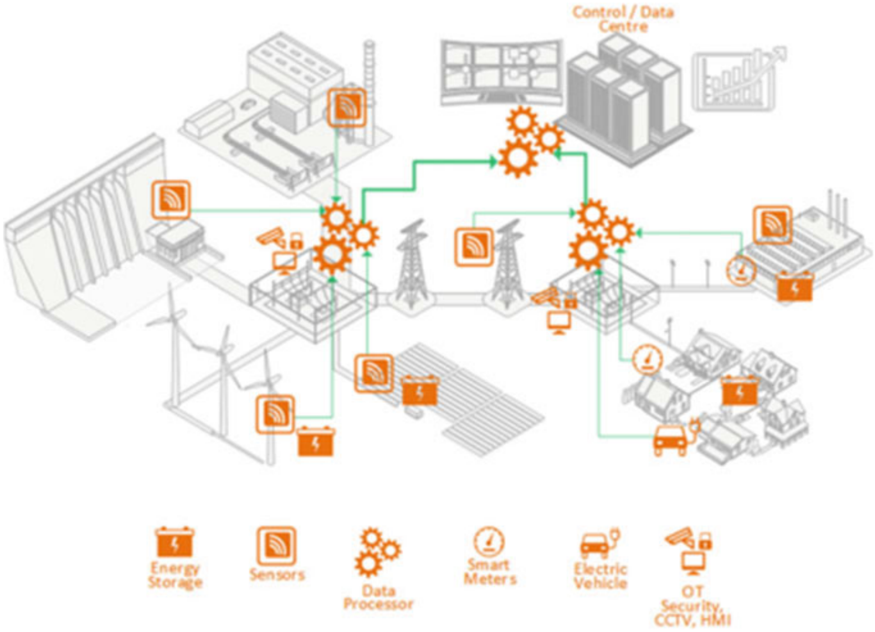


Fig. 1.4 Information flow with distributed data sources and data processing sites (*Source* CIGRE Green Book 'Electricity Supply Systems of the Future', Information Systems and Telecommunications, Figure 17)

- Regulations (prioritisation of Renewable Energy Source (RES), tariff incentives (production tax credits), interface requirements for DER).
- Energy market, exchange clearing authority, energy exchange trade, market for system services (voltage and frequency regulation, peak load generation and peak supply management).

Power system stakeholder and consumer expectations have also changed with systems and technology being implemented. A more reliable, more available, safer, cost optimised, smarter and leaner power system is expected.

1.2 Resulting Power System Challenges

With the many changes in society (discussed in the previous section) reflected in the changes appearing in power systems, there are new power system challenges to deal with.

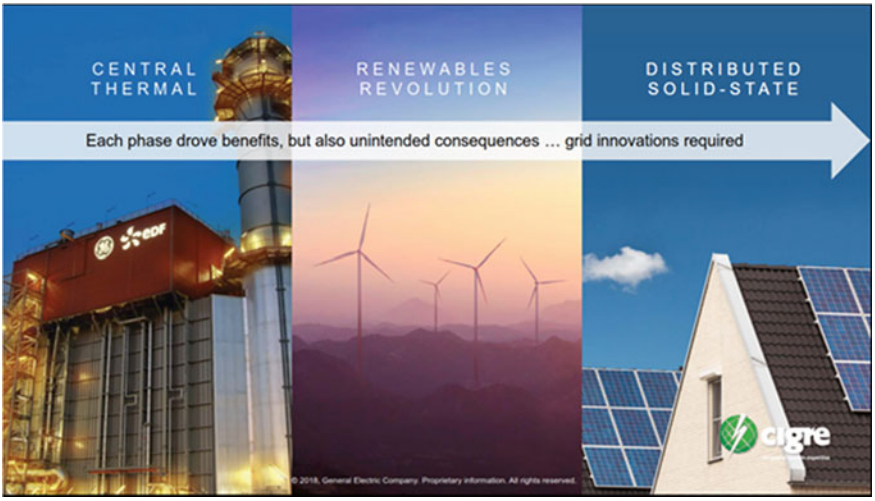
1.2.1 Climate Change Challenges

Climate change action is leading to an increase in the direct use of electricity as an energy source and energy load. Electricity energy is directly converted in heating, transportation and industrial systems. Different forms of distributed renewable generation are being installed. This has provided a number of challenges. The worldwide move away from fossil fuel generation to forms of renewable generation is changing the power system and where generation is located. This is illustrated in Fig. 1.5. In some areas of the world, there is an increase or greater reliance on interconnections between countries to share energy, as shown in Fig. 1.6 [2].

Distributed Energy Resources are being increasing connected at lower network voltages, many of which were not designed to cater for embedded generation. This creates stability and power flow reversal issues requiring new protection and automation solutions.

Generation trends will likely change from predominantly large base load power plants connected at the transmission level to a mix of large dispatchable plants at transmission level along with a large amount of embedded generation with varying degrees of dispatchability, much of it from DER (including energy storage). These embedded DER devices will provide opportunities, or problems, depending upon one's viewpoint such as islanding of parts of the network under certain conditions [2].

However, many DER devices do not possess the fault response and ride through capabilities of conventional generators and may compound stability issues during



CENTRAL THERMAL

RENEWABLES REVOLUTION

DISTRIBUTED SOLID-STATE

Each phase drove benefits, but also unintended consequences … grid innovations required

© 2018, General Electric Company. Proprietary information. All rights reserved.

Fig. 1.5 Transition away from fossil fuel generation (*Source* CIGRE 2018 Paris Opening Panel Presentation)

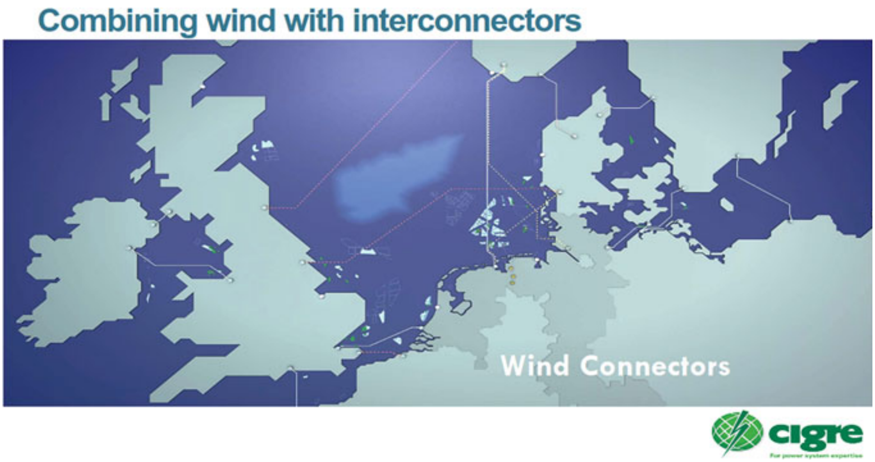

Combining wind with interconnectors
Wind Connectors
cigre
For power system expertise

Fig. 1.6 Energy transition and more interconnected grids (*Source* CIGRE 2018 Paris Opening Panel Presentation)

disturbances and faults. This may also imply more constraints for the fault clearance times of the existing network. Despite the limited dispatchability today of many DERs, the main control centres need their actual status to have a complete picture of generation connected to the network. There is an increased need for dispatch, and demand control systems and associated communication.

This requirement could drive Distribution State Estimation which may require synchronised measurements (synchrophasors) to implement due to the vastness and single-endedness of the distribution system [2].

1.2.2 Technology Change Challenges

Technological change is also having a big impact on the power system and presenting many challenges. Modern advances in fields including materials, optics, semi-conductors and production techniques have led to advances in primary equipment solutions for generating and enabling transfer of power such as battery storage, solar and wind generation, cable, instrument transformers/sensor, HDVC and FACTS systems. Resulting challenges include scheduling the different types of generation and applying these technologies into different parts of the power system with different features. Secondary challenges include the continuing development of control and protection systems to deal with the different characteristics of these systems such as low fault current contribution and need for controlling different modes of operation. Other technological change is in the secondary systems area of communication, information and automation technologies. Optical fibre is replacing copper wire for communication of information. Digital signals are now being applied further into the substation at the process level where they

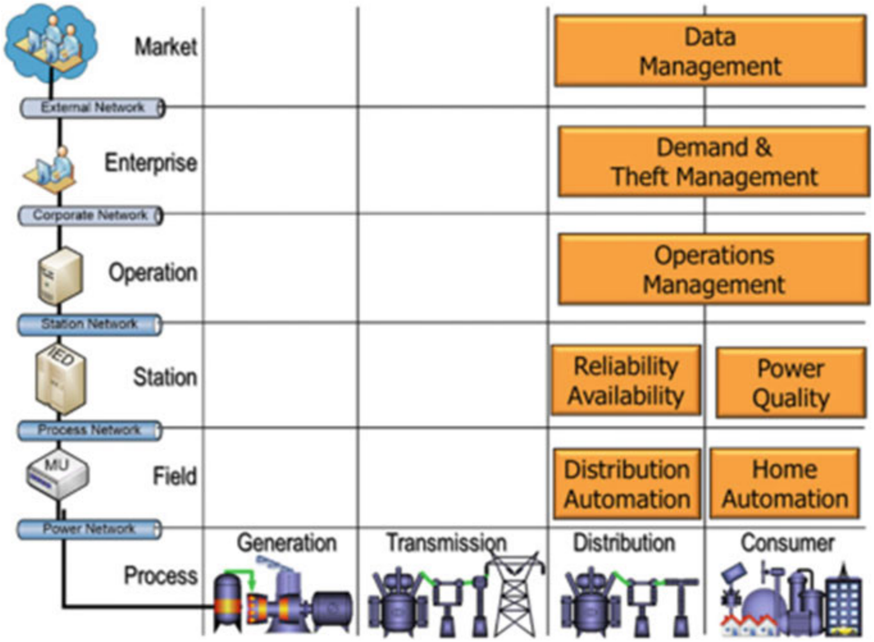


Fig. 1.7 Application opportunities at different levels with communication of digital signals for distribution and consumer systems (*Source* CIGRE Green Book 'Electricity Supply Systems of the Future', Introduction and Overview, Figure 39)

interface directly with the primary equipment. Within power systems, this has been evidenced by smaller smarter multifunctional devices with increased inter-device and inter-substation communication capabilities. The applications available through the communication of digital information at different levels are illustrated in Fig. 1.7 for distribution and consumer systems. Challenges include interoperability when connecting devices from different manufacturers, the need for better tools to develop and operate systems, ensuring systems are cyber secure and better training for schemes particularly for commissioning and testing personnel.

1.2.3 Challenges from Social and Societal Change

Social and societal change has increased expectations for reliability, resilience, safety, cost optimisation and performance of the power system. This has also been fuelled by universal technological change and advancements with associated solutions where the above performance expectations have been met. The challenge is to meet these greater performance expectations for the changing power system and how it is operated, particularly regarding the different and developing types of primary equipment and interconnected power system networks. For the power system technological changes discussed above, there are protection and automation opportunities to provide an increased levels of performance through PACS to monitor and ensure system integrity for normal and special power system operational conditions and primary equipment.

1.2.4 Utility Challenges

Utilities have the traditional job of developing, operating and maintaining their power systems. With the changes and extra power system challenges described in this chapter, there is additional pressure on utilities to address the challenges and develop and implement the required systems within tight time frames, with existing human resources and at optimised cost. We cannot expect utilities to grow many times in size, especially considering there is presently a shortage of engineers and other people educated to work in the power industry. Thus, the power system utilities have to work smarter and accomplish more.

1.2.5 CIGREs Ten Issues to Address for Network Supply System of the Future [1]

CIGRE's Technical Council has compiled the following list of ten issues that must be addressed in order to guarantee the full development of the network supply system of the future:

Issue 1—Active Distribution Networks.

- Bidirectional power and data flows in distribution level,
- Control and coordination of many small units,
- Need for decentralised, intelligent control,
- Massive implementation of smart metering and demand-side response,
- Market and regulatory changes to manage efficiency, equity and cost recovery,
- Distribution network architectures that include microgrids and virtual power plants.

  Issue 2—Massive Exchange of Information.

- Advanced metering with massive need for exchange of information,
- New measured parameters, architectures of information, communication technologies and algorithms,
- Identification, requirements and standardisation of the data to be exchanged,
- Disaster recovery and restoration plans,
- Cybersecurity and access control.

Issue 3—Integration of HVDC/Power Electronics.

- Impact on power quality, system control, security and standardisation,
- Appropriate models for network performance analysis,
- Harmonic distortion and filtering,
- Designs and controls to provide benefits and performance enhancements to reliability,
- Need new standards and grid codes,
- Increased use of DC at end-use premises.

Issue 4—Massive Installation of Storage.

- Need and impact on power system development and operation,
- Construction: materials, installation and costs, environmental impact, efficiency of charge/discharge cycles, weight and size density, life-time estimation models,
- Operation: modelling, management, sizing, co-operation with RES and DSM, islanding, peak reduction.

Issue 5—New Systems Operations/Controls.

- New concepts for system operation, control and market/regulatory design,
- Stochastic generation and modified loads due to DSM/storage,
- Evolution of power system control at continental, country, regional and local level,
- Increased level of automation,
- New competencies for system operators.

Issue 6—New Concepts for Protection.

- To respond to the developing grid and different generation characteristics,
- Wide-area protection systems (WAPS),
- Decreasing short circuit and flow reversal,
- Coordination with fault ride through (FRT),
- Inadvertent and intentional islanding detection.

Issue 7—New Concepts in Planning.

- New environmental constraints and solutions for active and reactive power flow control,
- Risk-based planning with many uncertainties, addressing the interaction of transmission and distribution,
- Comparison between new technological options,
- Changing economic, market and regulatory drivers.

Issue 8—New Tools for Technical Performance.

- New customer, generator and network characteristics,
- Advanced tools, methods and multi-agent techniques for the solution of dynamic problems, power balancing, harmonic performance, probabilistic and risk-based planning,
- Advanced modelling for loads, active and adaptive control strategies and bridging the gap between three-phase and positive sequence modelling.

Issue 9—Increase of Underground Infrastructure.

- Consequence on the technical performance and reliability of the network,
- Technologies for uprating existing lines,
- New submarine and underground cables,
- Impact on stability, transients, overvoltages and network management.

Issue 10—Need for Stakeholder Awareness.

- Technical and commercial consequences, and engagement in the network of the future,
- In the planning phase: demonstrate benefits, account for public views,
- In the construction and operation phases: demonstrate compliance with environmental standards and obtain support for the necessary actions.

IEC 61850 assists to address many of the issues stated, particularly in the areas of active distribution networks, information exchange, system operation and new concepts in protection. Reference is made to other chapters of the book particularly Chaps. 3, 4, 6, 12, 13, 14 and 16.

1.3 Features of IEC 61850 that Facilitate Solutions to Meet the Challenges

1.3.1 Protection, Automation and Control to Address Both Emerging and Traditional Challenges

The developments of new technologies in electrical power systems need to be closely followed by equivalent developments in PACS. As discussed in previous sections, this relates mainly to the introduction of new generation, transmission and distribution methods that require adaptation of traditional methods of protection, control and automation. These emerging challenges come mainly from the development of inverter networks, microgrids, prosumers with distributed generation and storage, electric vehicle support systems and physical and cybersecurity.

However, these emerging challenges also result from social change and shifts in expectations regarding aspects such as reliability and grid optimisation. Sections below explain that IEC 61850-based schemes are well suited to address these challenges [1].

The migration from a traditional power system with a flow from generation, transmission to distribution with full control of the utility to a system in which generation and consumption can be anywhere in this chain and without direct control from the power company, requires the need to safely interconnect the protection, automation and control system of each part of the chain. The dynamics of the participation of new players and systems will happen on a large scale and in a short time. The older traditional solutions do not meet this change because they mean re-engineering for each change in the system, replacing devices, configurations and negotiating the interfaces between each system. The IEC 61850 standard is based on a data model, with defined functions, which do not depend on the devices applied or the internal solution of each one of them. Therefore, it allows this future scenario to be adequately addressed—where solutions with different technologies can interconnect and be controlled by a PACS that needs to understand the existing functions and information.

Traditional power system and protection and automation objectives (such as switchgear interlocking) also continue to require PACS solutions. IEC 61850 continues to also be an enabler to these solutions and often provides additional benefits.

With the required power system changes highlighted in this book, there are also challenges for utilities in economically implementing projects on time and with limited human resources. There is presently a lack of engineers and other people educated to work in the power industry. Power generation, transmission and distribution utilities need to work smarter and accomplish more in building and extending the network to meet short timelines. Standardised processes, solutions and tools are important prerequisites to be able to work more efficiently. Application of IEC 61850 facilitates solutions to meet these utility challenges.

1.3.2 General Features of the IEC 61850 Standard

IEC 61850 will feature prominently in the protection, automation and control solutions employed for the networks of the future—especially its ability to provide self-description and generic configuration. It also covers sampled values of current and voltage in the process bus. This facilitates the use of new technologies such as non-conventional instrument transformers (LPIT) [2]. Originally developed for use inside substations, it has been extended to cover substation-to-substation and substation-to-EMS communication.

1.3.3 General Advantages of IEC 61850 Compared with Other Standards

First and foremost, IEC 61850 is not “just” a standard for a communications protocol such as IEC 60870-5-1xx series, DNP3.0, Modbus, etc. It is a complete set of standards covering environmental requirements, project management, engineering process and tools, function modelling, conformance testing and large numbers of application recommendations and guidelines.

IEC 61850 is becoming the “well known” and best standard which covers the communications at all the three levels of equipment in a substation, namely at Station Level, Bay Level and Process Level. This is illustrated in Fig. 1.8. Other standards cover the communications at only one or two of these three levels because most standards were developed for specific purposes [3].

IEC 61850 specifies high-speed event-driven communication rather than polling as used in centralised communication. The applied client–server architecture allows also to have instead of a single master many clients, e.g. for redundancy purposes.

The advantages of IEC 61850 compared to other communication standards include:

- Ethernet (a particular local area computing network protocol) use to allow a device to send a message whenever it needs (event driven communication), and there is no master device governing which device can talk at any given time. A centralised communication system can create a bottleneck because when the

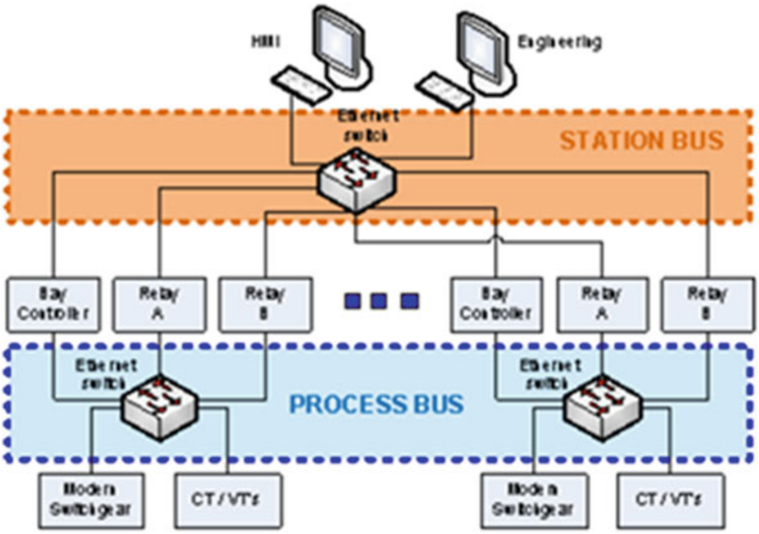


Fig. 1.8 Station bus and process bus connecting IED levels (*Source* CIGRE Technical Brochure 427, Figure 1)

master fails other devices cannot communicate, which is resolved by the now used client–server architecture,

- Multicasting (i.e. one device sending a message simultaneously to several devices inside one logical LAN segment) is simple in Ethernet and improves the performance of time-critical messages. This reduces network message traffic and communication time by eliminating the need to repeat messages to individual devices sequentially,
- Monitoring of the system, which contributes to its reliability, since having real-time information on the health of the functions, devices and local communication infrastructure, it is possible to take corrective and preventive actions more quickly and efficiently,
- TCP/IP is the transmission control protocol of the Internet. IEC 61850 facilitates data transfer through public or private data networks by using TCP/IP also. Data of other protocols based on Ethernet and TCP/IP, such as web-services data for remote maintenance, can be transmitted in parallel via the same communication infrastructure,
- Any changes in communication technology in the future will cause minimum changes in the abstract models and services and may only require mapping to a new profile,
- The data model is clearly defined and is also easy to extend without losing the interoperability,
- It defines a series of data names and associated rules for extension (logical nodes and their attributes) that clarify the interpretation between the different projects actors and facilitate the integration of the different components of the system as well as the integration of the system with its environment (primary devices, remote control),
- Unlike legacy protocols such as Modbus, IEC 61850 devices can self-describe themselves to client applications without any manual configuration of the data objects. Self-description facilitates automatic configuration,
- Unlike legacy protocols, IEC 61850 specifies a standard configuration language based on XML and using the logical nodes described above. This allows formally exchanging configuration data between system tools and avoids the manual association of data references between tools,
- Time synchronisation methodologies over Ethernet such as SNTP and PTP are a key component of IEC 61850. SNTP time synchronisation accuracy in the range of 1 ms is sufficient for event reporting but not for process bus. PTP is designed to compensate for these switching delays with a time synchronisation accuracy better than 1 microsecond and is suitable for process bus applications [3, 4].

1.3.4 Summary of Applications, Features and Advantages of Applying IEC 61850 Schemes

In assisting to facilitate solutions for the various power system challenges previously described, some applications, features and advantages of applying IEC 61850 schemes are summarised below and are expanded on in later chapters. Refer to Chap. 7 for details of critical design and implementation strategy to make use of these advantages.

- **Facilitates exchange of information and use of logical schemes for applications where data is dispersed to meet distributed and renewable generation challenges**
  - The interfacing aspects and functional blocks needed by most applications are described in the IEC 61850 standard, as well as the network architecture for building local and wide-area PACS.
  - In addition to opening up secondary protection and automation solutions, it also enables enhanced primary equipment and system operation solutions both within a substation and between sites.
  - Applications within the substation include circuit breaker interlocking, autoreclosing and synchronism checking schemes, transformer hot standby schemes, busbar protection.
  - Application between substations are expanding and include wide-area load shedding, DER generation schemes, anti-islanding schemes.
  - The monitoring and control of the future grid will require faster, secure and wide-area flow of information. IEC 61850 defines fast communication mechanisms for use within and between substations and other external sites. Refer to Fig. 1.9.
  - In some countries, the exchange of information between DER connected to LV, MV and HV grids and external operators for grid stability and control purpose are defined on the base of IEC 61850.
- **Standardised schemes for faster implementation and reduced errors**
  - The development of standardised protection and control schemes for specific types of substation configurations, bay layout and primary equipment has the potential to save time, resources and cost once the designs are finalised for use in future applications.
  - A major benefit of IEC 61850 is interoperability. IEC 61850 standardises the data model and services required to interface with substation IEDs. This responds to the utilities' desire of having easier integration for different vendors' products, i.e. communication interoperability. It means that data is accessed in the same manner in different IEDs from either the same or different IED vendors, even though, for example, the protection algorithms of different vendors' relay types remain different.
  - IEC 61850 defines also the Substation Configuration description Language (SCL) which allows the configuration of an automation system to be defined and the setting of the standardised parameter of IEDs from different manufacturers to be fixed by the user or any of the manufacturers involved.

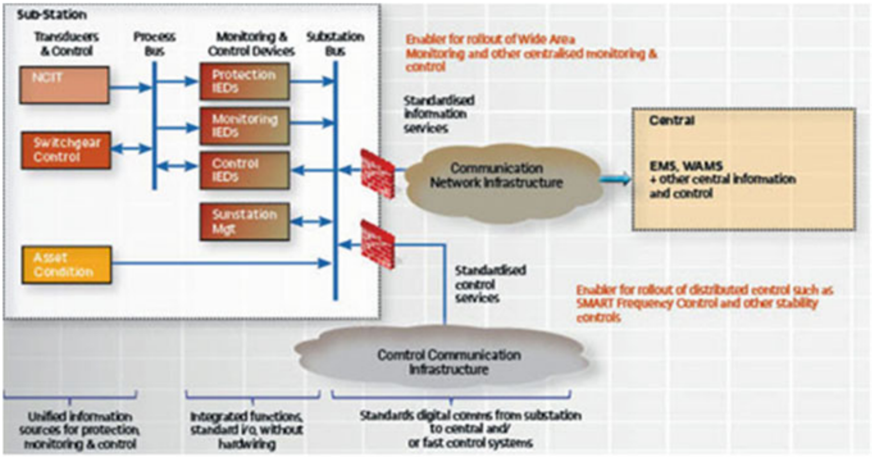

Sub-Station
Transducers & Control
Process Bus
Monitoring & Control Devices
Substation Bus
NCIT
Switchgear Control
Protection IEDs
Monitoring IEDs
Control IEDs
Sunstation Mgt
Asset Condition
Enabler for rollout of Wide Area Monitoring and other centralised monitoring & control
Standardised information services
Communication Network Infrastructure
Central
EMS, WAMS + other central information and control
Standardised control services
Enabler for rollout of distributed control such as SMART Frequency Control and other stability controls
Comtrol Communication Infrastructure
Unified information sources for protection, monitoring & control
Integrated functions, standard i/o, without hardwiring
Standards digital comms from substation to central and/ or fast control systems

Fig. 1.9 Different wide-area applications—exchange of information (*Source* PAC World magazine—FITNESS—Future Intelligent Transmission Network Substation—Future proofing: Wide Area Control and Protection)

- Refurbishments, augmentations and replacements are also facilitated by the defined object models and communications avoiding re-engineering of the same information engineered originally, e.g. an overcurrent element sending an operate signal to a circuit breaker.
- The move to an integrated virtual specification and implementation provides the significant benefit of reusable, and therefore reliable, engineering.

- **Greater focus on more economical solutions**
  - Substation costs that are related to substation functionality and operation include primary and secondary equipment, cabling, and engineering and commissioning. Engineering and commissioning costs are reduced by maximising the amount of testing at the factory and minimising the amount of testing required on-site. Substation costs related to civil works, project management and design in new build or replacements require large investment, can be reduced by smaller physical size, fewer supporting structures, and smaller cable ducting, less copper cables and reducing engineering effort. A significant contribution to the minimisation of these costs is through IEC 61850-based standardisation of design.
  - Due to less hardwiring in the substation and with a digital fibre-based approach, engineering is simpler and less expensive both in the initial phase, when the substation is built, and in any modifications made later due to changes needed for any reason.
- **Faster implementation with less on-site testing plus reduced primary outage time**
  - Installation of IEC 61850-based systems (after the first pilot installation) takes less time because nearly all the problems have already been solved in the IED conformance test, the system test as mentioned above and in the

FAT. The problem left open is the completeness of the FAT regarding system components and the process interface to the switchgear.

- **Smaller footprint**
  - IEC 61850 schemes use of digital sensors, digital signals over fibre and integrating functions into fewer overall devices can help to reduce the footprint at substations. Traditional installations used many large copper cables, bulky instrument transformers and many devices within a larger relay room.
- **Supervision, monitoring and analysis of schemes**
  - Implementation of IEC 61850-based protection schemes offers some significant advantages over conventional hard wired schemes. The continuous repetition of GOOSE messages by the protection and communications devices and the streaming of sampled values from the merging units provide reliable indication about the status of the interface and communication path function-to-function. Such reliability and failure detection simply cannot be achieved in wire-based schemes for each and every signal and is often only detected through scheduled testing or more catastrophically when the scheme fails to operate. Refer to Chap. 15 for more details on this aspect.
- **Safety**
  - There is a risk to life of working with CT secondary circuits. While the hazard is mitigated by design and working practices, it can be eliminated through replacement of conventional CTs with LPITs. The associated operational and maintenance task hazard and its reduction by use of process bus are also covered in Chap. 15.

References

1. CIGRE Green Book.: Electricity Supply Systems of the Future". CIGRE Technical Council, Springer Nature, Switzerland AG (2020). https://doi.org/10.1007/978-3-030-44484-6
2. CIGRE Technical Brochure 629.: Co-ordination of Protection and Automation for Future Networks, CIGRE WG B5.43 (2015). https://e-cigre.org/publication/629-coordination-of-protection-and-automation-for-future-networks
3. CIGRE Technical Brochure 540.: Applications of IEC 61850 Standard to Protection Schemes, CIGRE WG B5.36 (2013). https://e-cigre.org/publication/540-iec-61850-standard-to-protection-schemes
4. CIGRE Technical Brochure 326.: The Introduction of IEC 61850 and its Impact on Protection and Automation within Substations, CIGRE WG B5.11 (2007). https://e-cigre.org/publication/326-the-introduction-of-iec-61850-and-its-impact-on-protection-and-automation-within-substations

Introduction to IEC 61850 Systems

2

Rod Hughes, Peter Bishop, and Nirmal-Kumar C. Nair

Abstract

This chapter introduces the IEC 61850 standard. To provide background and assist understanding of aspects covered further in the book, it explains the structure of the standard, some initial concepts, summarises its history, discusses compliance and the need to gain expertise.

Keywords

IEC 61850 • Structure • History • Data model • Physical device • Logical device • Logical Node • Common data class • Data attribute • Compliance

2.1 What is IEC 61850

The series of IEC 61850 Standards "Communication networks and systems for power utility automation" (the subject matter of this Compact Green Book) is based on the need expressed by the industry to have devices used for protection and automation which are interoperable via a communication link at least to the same degree as hardwired devices. The primary utility drivers, as discussed in Chap. 1, are for lower costs and increased flexibility of substation automation. The

R. Hughes (✉)
Rod Hughes Consulting, Aberfoyle Park, SA, Australia
e-mail: rgh@rodhughesconsulting.com

P. Bishop
Transpower NZ Ltd., Wellington, New Zealand
e-mail: peter.bishop@transpower.co.nz

N.-K. C. Nair
University of Auckland, Auckland, New Zealand
e-mail: n.nair@auckland.co.nz

P. Bishop and N.-K. C. Nair (eds.), *IEC 61850 Principles and Applications to Electric Power Systems*, CIGRE Green Books, https://doi.org/10.1007/978-3-031-24567-1_2

objective of IEC 61850 Standard is therefore to provide an engineering and IED configuration that meets performance and cost requirements, and which supports future technological developments. Key to the usefulness of IEC 61850-based systems is the open exchange of information between Intelligent Electronic Devices (IEDs). IEC 61850 supports the specification, design, implementation and operational requirements of electrical infrastructure automation functions in terms of engineering, data model and secure communication mechanisms.

At the outset it is essential to understand what the Standard sets out to provide, and what it does not. IEC 61850-1 Chap. 4 "Objectives", paragraph 4 states:

> *the purpose of the standard is neither to standardise (nor limit in any way) the functions involved in substation operation nor their allocation within the Power Utility Automation System. The application functions will be identified and described in order to define their interface and then their communication requirements (for example, amount of data to be exchanged, exchange time constraints, etc.).*

IEC 61850 is therefore an "enabler" of the automation system implementation, but is not a defined implementation for any particular project. The asset owner, asset operational staff and systems integrator are all required to work together to choose the right implementation of functions and communication options to suit their requirements that will then allow the selection of an appropriate combination of IEDs to meet those requirements. This is a subtle but notable change compared with conventional wire-based engineering processes of selecting the devices initially and thereafter deciding with how they can be connected. It is therefore "function based" rather than "device based" as can often be the case with prescribed panel wiring templates and prescribed IED selections.

Furthermore, as stated in the "Objectives" clause, whilst "interoperability" is a specific objective of IEC 61850, "interchangeability" of one IED with another is not. It is fair to say, however, that IEC 61850 goes a long way towards facilitating the engineering processes associated with the selection of alternative IEDs. If the alternative IED supports the same data model (Model Implementation Conformance Specification—MICS) and communication functions (Protocol Implementation Conformance Specification—PICS) as the original IED, then much of the IEC 61850 configuration engineering can remain the same, possibly even importing the same Part 6 engineering files to the new IED tools. However, there are many other proprietary aspects outside of/beyond the IEC 61850 systems that will still need to be addressed such as physical size, terminations, I/O arrangements, port arrangements, front panel indications, controls, language, internal logic definitions, etc.

The scope of IEC 61850 is power utility automation for all types of networks and voltage levels. The scalability of the Standard and of the supporting communication technology that is used allows the application from generation (all forms), storage, transmission, distribution and end consumer levels of electricity infrastructure. The title of the Standard in 2002 as "Communication networks

Table 2.1 Functional domains covered by IEC 61850

Protection	Power quality	Event record management
System operation monitoring	Metering	Alarms
System controls	Scheduling	…
Automation	Condition monitoring	

and systems in substations" changed in 2010 to "Communication networks and systems for power utility automation" to recognise that the Standard will be used also outside the fence line of the substation for (in no particular order or priority). Table 2.1 below lists some of the wider functional domains covered by the Standard.

Whilst the title of the Standard is "Communication networks and systems …", the Standard does not prescribe how a particular local area network (LAN) or wide area network (WAN) is to be implemented and configured. Part 90-4 "Network engineering guidelines" does give some advice about certain aspects to consider with regards to traffic/bandwidth management configuration of the switches/routers and so-called bumpless network design using solutions such as IEC 62439-3 High-availability Seamless Redundancy (HSR) rings and/or Parallel Redundancy Protocol (PRP) duplicate LANs.

The reference to "power utility" is therefore far broader than the general use and comprehensively address all aspect of existing and emerging electrical power systems. The application encompasses all forms of electricity infrastructure, e.g. the Standard includes aspects in Table 2.2.

In particular, the high investments in the substation communication technologies and the strong move of this into all areas of industrial processes (the Internet of Things—IoT) will allow using IEC 61850 effectively from the highest voltage levels to the lower voltage consumer end of this application range, which can be understood by the reader through the various chapters of this book. Chapter 16 identifies the uptake of this in diverse application areas like traction, electric-charging infrastructure, HVDC, etc.

As also stated in IEC 61850-1 Chap. 4,

Table 2.2 Asset domains for IEC 61850

Substations of all voltage levels, AC and DC	Hydro power dam and water flow	Electric vehicles
Overhead transmission lines	Distributed energy resources	Energy storage systems
Underground cables	Wind turbine mechanics and environment	Industrial and mining consumers
Generation (all types)	Traction	

> *The communication standard IEC 61850, to the maximum extent possible, makes use of existing standards and commonly accepted communication principles.*

Fundamentally, the Standard is not "*just a mere protocol*" in a communications sense. As further described in this chapter, it is rather three core elements for engineering and implementation of the automation system:

- a structured definition of an engineering process, three engineering tools and six file types (Part 6),
- the data model within devices as Logical Devices, Logical Nodes, Data Objects and Data Attributes (Part 7 series), and
- three protocols of MMS, GOOSE and Sampled Values (Part 8 and 9).

such that information can be exchanged correctly between functions within devices over whatever communication media and protocol is used.

The other core aspects of IEC 61850 are to be well understood in varying degrees by various different personnel at different stages of the engineering and operation cycle are:

- environmental withstand specifications (Part 3),
- project management and "actor" involvement (Part 4)
- function modelling (Part 5)
- IED compliance certification (Part 10).

To achieve interoperability for IEDs, also all layers of the protocol stack including media definitions have been standardised by a well-defined selection out of main stream communication technology.

Based on an object-oriented approach and the use of main stream communication technology, IEC 61850 provides significant benefits to users which are uniquely at least in this combination [1].

2.2 Overview of the IEC 61850 Series Concept

At the time of publication of this Green Book, there are some 33 published Parts of the IEC 61850 Standard, some as Edition 1, some already at Edition 2, and some as Edition 2.1.

Some Parts of IEC 61850 are fully approved official **International Standards (IS)** [2]. Some other Parts point to key specifications but as yet have only been released as official **Technical Specifications (TS)** [3] as "good recommended practice", but not officially "standardised", whist others are "industry general guidelines" as **Technical Reports (TR)** [4].

There are also some additional 30 other Parts in development of their Edition 1, and hence, it is important for users to be informed about new releases as they occur, and to have access to the previous editions of the Parts that have had new Editions.

The purpose of the Green Book is to provide a reasonably concise, but thorough, wide audience practical view of implementing of IEC 61850-based systems and the range of applications to meet power system challenges. Before going further into the implementation journey, it is also necessary to have a thorough understanding of the Standard itself, or of reference material that aids in that understanding and references "good industry practice". CIGRE has been a key contributor to the body of knowledge with several Technical Brochures identifying "good industry practices" and many papers at many worldwide events discussing implementation experiences—refer to Appendix A Bibliography and References. Many of these references are also specifically referred to in the associated chapter of this Green Book.

Each Part of the Standard as shown in Fig. 2.1 defines a specific aspects of the system and/or the IED:

- IEC 61850-1 gives an introduction and overview of the IEC 61850 series,
- IEC 61850-2 contains the glossary of specific terminology and definitions used in the context of power utility automation systems within the various parts of the Standard,
- IEC 61850-3 specifies the general requirements of the communication network with regard to the quality requirements, environmental conditions and auxiliary services,

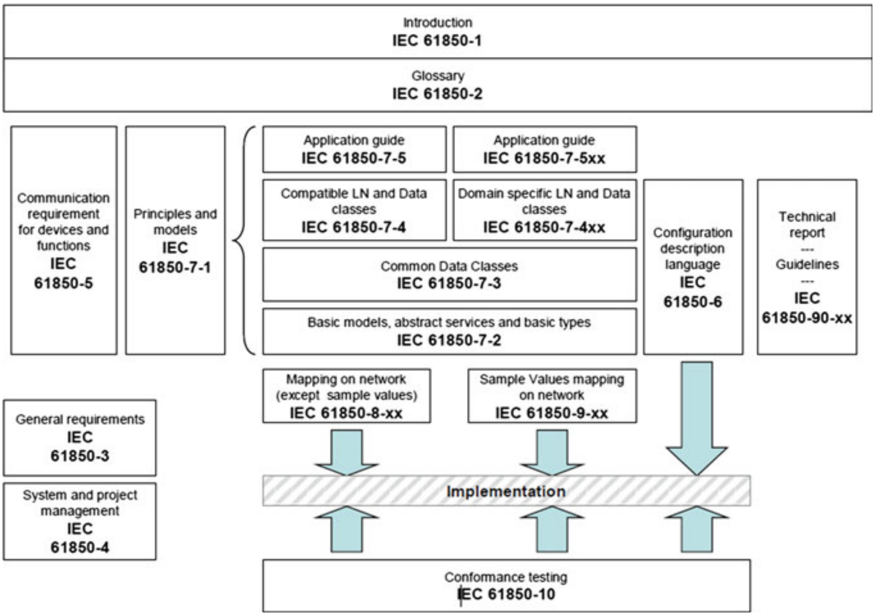


Fig. 2.1 Relation between modelling and mapping parts of the IEC 61850 series (IEC 61850-7-1, Figure 1)

- IEC 61850-4 pertain to the system and project management with respect to the engineering process, the life cycle of the PACS and the quality assurance from the development stage to the discontinuation and decommissioning of the PACS.
- IEC 61850-5 specifies the communication requirements of the functions being performed in systems for power utility automation and to device models. Most known functions and their communication requirements are identified, but there are rules for provision of "proprietary extensions" to the Standard if absolutely necessary.

The following Parts of IEC 61850 define the basic principles and modelling methods used by the IEDs,

- IEC 61850-6 specifies a file format for describing communication related IED (intelligent electronic device) configurations and IED parameters, communication system configurations, switchyard (function) structures and the relations between them. The main purpose of the format is to exchange IED capability descriptions and system level descriptions between engineering tools of different manufacturers in a compatible way. The defined language is called substation configuration description language (SCL). Mapping specific extensions or usage rules may be required in the appropriate parts.
- IEC 61850-7 has a few sub-Parts which, for many general users, are arguably best explained in "reverse order" to "drill down" into the data model structure
- IEC 61850-7-5 defines the usage of information models for substation automation applications. It gives clear examples on how to apply LNs and data defined in IEC 61850-7-4 for different substation applications. The examples cover applications from monitoring function to protection blocking schemes. Other domain-specific application guides which are within the scope of IEC technical committee 57 are defined in the IEC 61850-7-5xx series1. Examples are hydropower and distributed energy resources domains,
- IEC 61850-7-4 defines specific information models for substation automation functions (e.g. breaker with status of breaker position, settings for a protection function)—what is modelled and could be exchanged. Other domain-specific information models within the scope of IEC technical committee 57 are defined in the 61850-7-4xx series,
- IEC 61850-7-3 has a list of commonly used information (e.g. for double point control, three-phase measurand value, etc.)—what the common basic information is,
- IEC 61850-7-2 provides the services to exchange information for the different kinds of functions (e.g. control, report, get and set)—how to exchange information.

There may be Object Classes defined for various other application domains outside the scope of IEC technical committee 57, e.g. wind energy under technical committee 88. They are relevant to Fig. 2.1 only if they are built according to the approach of the IEC 61850 series.

The three communication “protocols” (MMS, GOOSE, SV) used in IEC 61850 systems are described in the following Parts:

- IEC 61850-8-1 defines the specific event and reporting means to communicate information between IEDs (e.g. the application layer, the encoding)—how to serialise the information during the exchange, i.e.
- Manufacturing Messaging Service (MMS) used for SCADA, reporting and controls
- Generic Object-Oriented System Event (GOOSE) for function status and changes
- IEC 61850-9-2 defines the Sampled Value (SV) mechanism for communicating real-time analogue values (22 sensors defined in Part 7-4 T group Logical Nodes: current, voltage, temperature, pressure, vibration, flow, …)
- In the case of current and voltage instrument transformers, and although effectively superseded by parts of IEC 61869 in 2016 with some notable differences, the UCAIUG industry association [5] issued a **guideline** (i.e. not a Standard as such) for CT and VT Sampled Value implementation often referred to as IEC 61850-9-2LE “Implementation Guideline for Digital Interface to Instrument Transformers using IEC 618509-2”.

2.3 Some Basic Concepts

As shown in Fig. 2.2, IEC 61850 enables integration of all protection, control, measurement and monitoring functions within a substation. In order to allow an open allocation of functions to IEDs, communication interoperability is provided between functions of a substation that are residing in equipment (physical devices) from any combination or selection of suppliers. The functions may be split physically into parts performed in different IEDs but communicating with each other (distributed function). Therefore, the communication behaviour of such parts called Logical Nodes (LN) supports the requested interoperability of the IEDs. The functions (application functions) of a Protection Automation and Control System (PACS, the broader sense of a Substation Automation System SAS), are control and supervision, as well as protection and monitoring of the primary equipment and of the grid. Other functions (system functions) are related to the system itself, for example supervision of the communication [6].

The Standard should be considered along with other key associated Standards such as the broader protection function requirements of the IEC 60255 series, IEC 61869 series for Instrument Transformers as applied for current and voltage sensors under the overall IEC 61850-9-2 Sampled Value definitions, IEC 62771 for high-voltage switchgear/controlgear digital interfaces and IEC 61400 for wind farms.

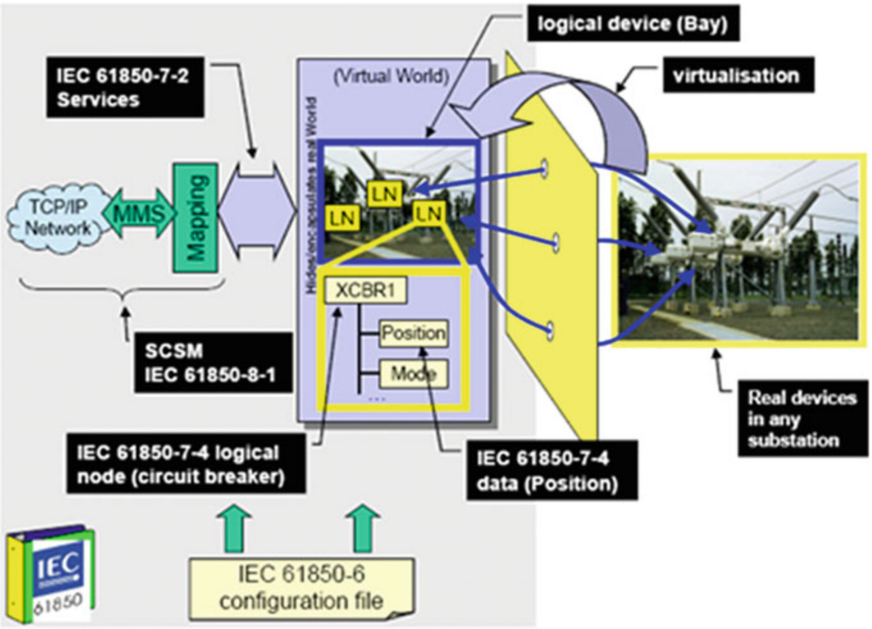

logical device (Bay)
IEC 61850-7-2 Services
(Virtual World)
virtualisation
Hides/encapsulates real World
TCP/IP Network
MMS
Mapping
LN
LN
LN
XCBR1
Position
Mode
...
SCSM IEC 61850-8-1
Real devices in any substation
IEC 61850-7-4 logical node (circuit breaker)
IEC 61850-7-4 data (Position)
IEC 61850
IEC 61850-6 configuration file

Fig. 2.2 IEC 61850 integration of functions (*Source* CIGRE Technical Brochure 540, Figure 4-1)

The IEC 61850 Standard defines the information and information exchange in a way that it is independent of a specific implementation (i.e. it uses abstract models). The Standard also uses the concept of virtualisation which provides a view of those aspects of a real device that are of interest for the information exchange with other devices. Only those details that are required to provide interoperability of devices are defined in the IEC 61850 series.

The Standard has been scoped so as not to prescribe particular functional requirements but provides a platform on which functions can be realised more consistently. However, it does not purport to be the unique Standard for the features and capabilities for any IED as offered in the competitive market. Whilst many aspects have been structured in the Standard, it should not be taken as blind "plug-and-play".

To ease understanding, the data model of any IEC 61850 IED can be viewed as a hierarchy of information. The categories and naming of this information are standardised in the IEC 61850 specification.

Referencing Fig. 2.3, the levels of this hierarchy can be described as follows:

Physical Device (PD)
It identifies the actual IED within a system.

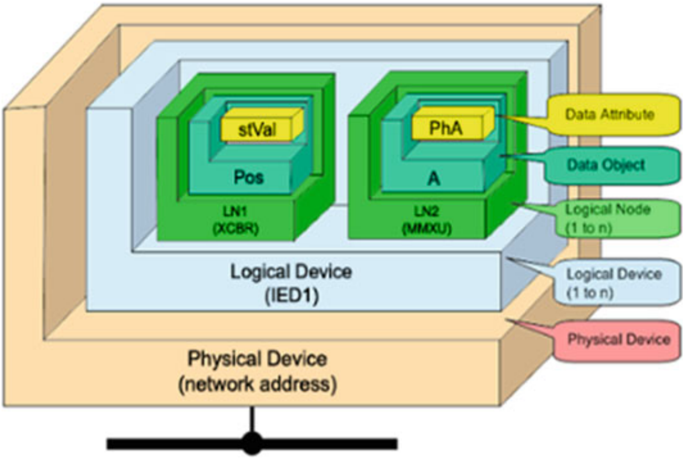


Fig. 2.3 Data model levels of hierarchy (*Source* CIGRE Technical Brochure 540, Figure 4-2)

Logical Device (LD)

It identifies groups of related Logical Nodes within the Physical Device. The allocation of Logical Nodes to specific Logical Devices is not defined in the Standard.

Logical Node (LN) (Part 7-4)

It identifies the major functional areas within the IEC 61850 data model. Logical Nodes are instantiated in an IED or computer using prefix characters and/or an instance number according to the vendor's implementation requirements, i.e. the available LNs in any particular IED is vendor-dependant as defined in the IED Capability Description (ICD) file (defined in Part 6) and Model Implementations Conformance Specification (MICS) document (created for Part 10 Certification).

Data Object (DO) (Part 7-4)

A Data Object is a set of sub-aspects of a Logical Node according to the requirements of the Logical Node's data and operating model with certain DO as mandatory, others optional and yet others "conditional" according to the vendor's implementation:

- Status information,
- Measured information,
- Controllable status information,
- Controllable analogue set point information,
- Status settings,
- Analogue settings.

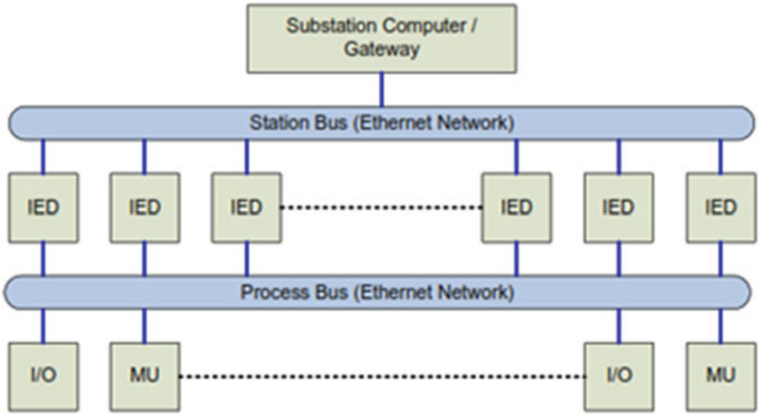

Substation Computer / Gateway
Station Bus (Ethernet Network)
IED
IED
IED
IED
IED
IED
Process Bus (Ethernet Network)
I/O
MU
I/O
MU

Fig. 2.4 Hierarchical IED levels with station and process bus ethernet network connections (*Source* CIGRE Technical Brochure 540, Figure 4-3)

Common Data Class (CDC) (Part 7-3)
A common data class is a composite set of data attributes which further define the individual aspects of each of the individual DOs, e.g. status information will require status value, quality and time stamp plus other aspects for substitution, blocked, etc.

Data Attribute (DA) (Part 7-3)
This is the actual data (measurement value, status, description, etc.). For example, <<.stVal>> (status value) indicating actual position of circuit breaker for Data Object type <<.Pos>> of Logical Node type XCBR.

Part 5 of the IEC 61850 Standard introduces a view of a substation automation system comprising three hierarchical levels (station, bay and process), and hence, two levels of communication network connecting these hierarchical levels are described—the station bus and the process bus, although these may co-exist on the same LAN cable. This is discussed further in Chap. 4.

A simplified diagram with the communications architecture of an IEC 61850 station and process bus-based substation automation system is shown in Fig. 2.4.

2.4 Brief History

The industry's experiences have demonstrated the need and the opportunity for developing standard communication protocols, which would support interoperability of IEDs from different vendors. Interoperability in this case is the ability to operate on the same network or communication path sharing information and commands.

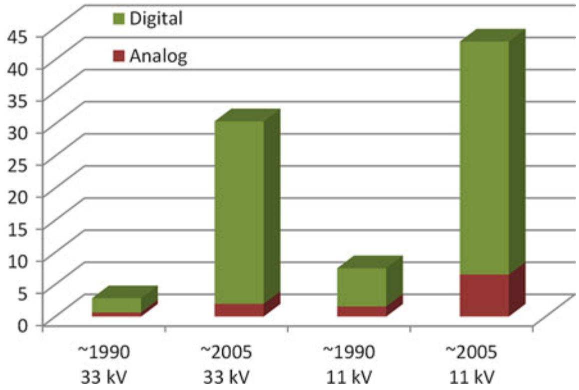


Fig. 2.5 IO count per bay increases at 33 kV and 11 kV (*Source* [7])

As a Standard, IEC 61850 has somewhat unique genesis in the mid-1990s. It can be said that many Standards are driven by a need to "standardise" various existing approaches to a particular issue. In the case of IEC 61850, whilst the issue had been identified, its approach to the solution was not an averaging of available solutions, but rather started as a complete new approach from a "blank sheet of paper" as to what the right solution would be in the context of how these systems are to be specified and implemented in an engineering process.

The issue that was facing the power industry was the rapid explosion in the need for information about the power system. One large distribution utility in Australia reported that in the period between 1990 and 2005, their 33 kV substations experienced an increase of their Input/Output (I/O) points changed from just a few to nearly 30 per bay, and at 11 kV from six to over 40 per bay as shown in Fig. 2.5.

The significance of the data explosion is not only in the hard wiring for these points, but also in the engineering effort to configure the systems to transport that information and indeed in the consistency of different vendors in how they provided that information to the engineering process as well as to the communication port. Interoperability became the buzz word, nominally around the real-time communication between the Intelligent Electronic Devices (IEDs) due to a proliferation of propriety and standard protocols (it has been suggested that there are as many as 50 different available protocols). However, the problem of having a common understanding of information as an aspect of interoperability was even more critical in the specification, engineering and implementation phases prior to placing in service.

The IEC 61850 Standard was based partly on UCA2.0, a substation automation concept developed in the USA under EPRI. Work on both Standards had begun in the early 1990s. In 1997, IEEE/EPRI and IEC TC57 decided to merge both standards to provide a global and unique substation automation solution.

The IEC 61850 Standard can now be considered mature, with the principles of Edition 1 of Parts 1–10 largely unchanged since 2002, but overall it continues to be expanded with more applications. It has been successfully deployed in tens of thousands of substations and systems at all voltage levels typically from 6 kV and above since the first "core" Parts were released by IEC Technical Committee 57 "Power systems management and associated information exchange" [8], Working Group 10 et alia over the 2002–2004 period. However, the scope of implementation continues to grow in

- protection,
- automation,
- System Control And Data Acquisition (SCADA),
- metering,
- condition monitoring.

In 2006, the application of IEC 61850 for wind farms and the turbines was released under the remit IEC Technical Committee 88 "Wind energy generation systems" [4] dealing with not only the electrical systems, but the associated mechanical aspects and even the tower itself.

IEC 61850 continues to further grow as one of the key enablers of the so-called Smart Grid with distributed energy resources and integration of new renewable energy systems among the mix of energy sources that it supports.

IEC Technical Committee 57 [8] established Working Groups 10, 11, 13 and 14 (since rationalised to just WG 10 as the custodian of the IEC 61850 Standard) to develop a Standard to become known as IEC 61850.

IEC 61850 is structured around three key elements:

- an engineering process covering system specification, IED capability and ultimate system implementation and maintenance
- a common semantic for all data and settings in the IEDs
- a set of three tailored communication protocols to suit the needs of secondary systems supporting electrical power systems for performance and reliability within a communications environment.

It is these three components that set IEC 61850 apart from general protocols and ensure an ongoing presence as the basis of electrical power system secondary systems engineering.

The overall title of the IEC 61850 series was initially:

"**Communication networks and systems in substations**"

This was changed with the release of Edition 2 of some parts to highlight that the application was beyond the "substation fence" to be:

"**Communication networks and systems for power utility automation**"

The reference to power utility in this sense is any owner of electricity infrastructure.

It is also to be noted that the overall series title does not define the series as a "protocol", but rather the complete network and system for information exchange.

Initially, the Standard consisted of 14 Parts as listed in Table 2.3 which could be called the "core Parts" of the Standard as they did, and still, set out the fundamental principles of the Standard.

Table 2.3 Initial 14 parts of IEC 61850

Part	IEC document type	Title (Edition 1)
-1	Technical Report	Introduction and overview
-2	Technical Report	Glossary
-3	Technical Specification	General requirements
-4	International Standard	System and project management
-5	International Standard	Communication requirements for functions and device models
-6	International Standard	Configuration description language for communication in electrical substations related to IEDs
-7-1	International Standard	Basic communication structure for substation and feeder equipment—Principles and models
-7-2	International Standard	Basic communication structure for substation and feeder equipment—Abstract communication service interface (ACSI)
-7-3	International Standard	Basic communication structure for substation and feeder equipment—Common data classes
-7-4	International Standard	Basic communication structure for substation and feeder equipment—Compatible logical node classes and data classes
-8-1	International Standard	Specific Communication Service Mapping (SCSM)—Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3
-9-1	International Standard	Specific Communication Service Mapping (SCSM)—Sampled values over serial unidirectional multidrop point to point link Part 9-1 was later withdrawn in favour of Part 9-2
-9-2	International Standard	Specific Communication Service Mapping (SCSM)—Sampled values over ISO/IEC 8802-3
-10	International Standard	Conformance testing

Since then, many additional Parts have been released to provide specific information about the use of the Standard in specific applications. Some Parts have had a slight change in their individual title in subsequent versions 2.

In the case of wind power, a separate IEC Technical Committee, TC 88, issued under their remit IEC 61400-25 as a series of Parts describing the use of IEC 61850 in that domain.

Over the period 2010–2013, the core Parts were re-issued as Edition 2 of those Parts to clarify certain aspects and refine the implementation in certain areas.

A common error is to reference "Edition 2 of the Standard" as clearly there are many Parts of the Standard still as Edition 1 and many Parts that are yet to be issued as Edition 1; hence, there will always be a mixture of current Parts as Edition 1, edition 2 and even more Editions undergoing development as IEC 61850 is being used across various sectors and application areas as described in the various chapter of this Green book.

Table 2.4 lists most of the additional Parts of IEC 61850 that have been released since the initial release in 2002–2004. These Parts provide further explanation of certain applications of IEC 61850.

Table 2.4 Additional parts since initial release 2002–2004

Subsequent additions	Title
IEC 61850-1-2	Guideline on extending IEC 61850
IEC 61850-6-100	SCL Function Modelling for Substation Automation
IEC 61850-6-2	Configuration description language for extensions for human machine interfaces
IEC 61850-7-410	Basic communication structure—Hydroelectric power plants—Communication for monitoring and control
IEC 61850-7-420	Basic communication structure—Distributed energy resources logical nodes
IEC 61850-7-5	IEC 61850 modelling concepts
IEC 61850-7-500	Basic information and communication structure—Use of logical nodes for modelling application functions and related concepts and guidelines for substations
IEC 61850-7-510	Hydroelectric power plants—Modelling concepts and guidelines
IEC 61850-7-520	DER—Modelling concepts and guidelines
IEC 61850-7-6	Guideline for definition of Basic Application Profiles (BAPs) using IEC 61850
IEC 61850-7-7	Basic communication structure—Machine-processable format of IEC 61850-related data models for tools
UCA IUG "IEC 61850-9-2LE"	Interim Guideline for application of IEC 61850-9-2 for CT/VT applications Replaced by IEC 61869–9
IEC 61850-10-3	Functional testing of IEC 61850 based systems
IEC 61850-80-1	Guideline to exchanging information from a CDC-based data model using IEC 60,870–5-101 or IEC 60,870–5-104
IEC 61850-80-2	IEEE Standard for Exchanging Information Between Networks Implementing IEC 61850 and IEEE Std 1815.1 Distributed Network Protocol (DNP3)
IEC 61850-80-3	Mapping to web protocols—Requirements and technical choices
IEC 61850-80-4	Translation from the COSEM object model (IEC 62056) to the IEC 61850 data model
IEC 61850-80-5	Guideline for mapping information between IEC 61850 and IEC 61158–6 (Modbus)
IEC 61850-8-2	Specific communication service mapping (SCSM)—Mapping to Extensible Messaging Presence Protocol (XMPP)
IEC 61850-90-1	Use of IEC 61850 for the communication between substations
IEC 61850-90-10	Models for scheduling
IEC 61850-90-11	Methodologies for modelling of logics for IEC 61850 based applications

(continued)

Table 2.4 (continued)

Subsequent additions	Title
IEC 61850-90-12	Wide area network engineering guidelines
IEC 61850-90-13	Deterministic networking technologies
IEC 61850-90-14	Using IEC 61850 for FACTS and power conversion data modelling
IEC 61850-90-15	DER Grid Integration
IEC 61850-90-16	Requirements for System management
IEC 61850-90-17	Using IEC 61850 to transmit power quality data
IEC 61850-90-18	Modelling alarm handling for IEC 61850
IEC 61850-90-19	Applying Role Based Access Control (RBAC) to IEC 61850
IEC 61850-90-2	Using IEC 61850 for communication between substations and control centres
IEC 61850-90-20	Guideline for redundant IEDs with IEC 61850
IEC 61850-90-21	Use of IEC 61850 for travelling wave fault location system
IEC 61850-90-22	SCD based substation network auto-routing with visualisation and supervision support
IEC 61850-90-23	Model extensions to IEC 61850 to support microgrids
IEC 61850-90-24	Mapping of IEC 62351–7 on IEC 61850
IEC 61850-90-25	Model update based on Users feedback
IEC 61850-90-26	IED Specification Description
IEC 61850-90-3	Using IEC 61850 for condition monitoring diagnosis and analysis
IEC 61850-90-4	Network engineering guidelines
IEC 61850-90-5	Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118
IEC 61850-90-6	Use of IEC 61850 for Distribution Automation Systems
IEC 61850-90-7	Object models for power converters in distributed energy resources (DER) systems
IEC 61850-90-8	Object model for E-mobility
IEC 61850-90-9	Object models for electrical storage systems
IEC 61850-9-3	Precision time protocol profile for power utility automation (IEEE 1588)
IEC 61850-99-99	Communication network in hydropower plants

One such key area enhanced in IEC 61850-7-4 Edition 2 was the clarification definition of the mechanisms used for “isolation” processes for a device or specific function during test procedures and addition of the <<Sim>> “Simulation mode”. When testing a system, there will be a large part of the system that remains in normal operational configuration and hence receiving and sending “live signals”. Isolation of a Device Under Test (DUT) or Function Under Test (FUT) requires all the other devices and functions to understand the meaning of signals received from the DUT/FUT and respond, or not in an appropriate manner. Despite the existence of most of the test modes in “Edition 1”, there was a proliferation of vendor and user proprietary mechanisms to “isolate” or rather control the behaviour of other devices/function during testing procedures. As a result of Edition 2 of Part 7-4, these processes have been more fully explained and enhanced to be used as a common set of mechanisms. Hence, it is a strong recommendation that any purchase of IEDs now insist on IEDs compliant to Edition of Part 7-4. A notable benefit of Ed2 IEDs is the enhanced handling of Logical Devices and the grouping of Logical Nodes under the behaviour and mode controls of the LD/LN.

No consideration of Edition 1 to Edition 2 would be complete with a specific comment about Logical Node GGIO (Generic process Input/Output) defined in Part 7-4. Edition 1 description was misunderstood by some vendors which led to devices claiming a huge number of GGIO instances, far more than would be warranted according to the physical I/O of the IED. Edition 2 clarified the use of GGIO is restricted to physical I/O to the device where the purpose of that physical I/O was not catered for by either an existing Logical Node, or by the implementation of a “private” Logical Node defined according to the rule for Private Namespaces. Compliance to Edition 2 of Part 7-4 has therefore ensured that the objective of a defined semantic for all signals has been respected, which in turn eliminates confusion in the engineering process by incorrect use of GGIO.

It is also to note that as the in-service life of secondary equipment can be in excess of 20 years, it may be necessary to have access to previous Editions of each Part as the in-service equipment may only be compliant to a previous Edition.

Communication between “Station Level” (Local control and SCADA) and “Bay Level” (the protection IEDs) has been in use since the 1980s with different kinds of serial protocols. These protocols have been mostly proprietary protocols, and in some cases, only devices from the same vendor were possible to connect into a vendor-supplied network. IEC 60870-5-103 introduced in the 1997 defined protection function communication; the control part of communication was freely configurable. Station level automation with PC-based station level user interfaces was possible in the first PACS solutions. Station bus with serial communication provided the ability to transfer more information from bay level to station level and Control Centre level. All this information was possible to implement with only one or some serial communication cables instead of many or even tens of traditional copper wire pairs. Communication speed was typically on the order of some tens of kilobytes per second.

Process level communication and process bus have also existed since the late 1980s with various general status and command communication protocols and eventually the release of IEC 60044-8 (2002) for Sampled Values.

Commercial applications of process bus are in service, but many are in the pilot stage. Process bus architecture and compatibility of devices have not yet been at a level for mass roll out; however, a process bus profile has recently been defined in IEC 61869-9.

In the bay IED level, modern numerical technology has provided possibility to insert many functions into the same physical hardware, with “Edition 2” offering enhanced handling of the Logical Device grouping and control of the Logical Nodes. Many new protection and control functions have also been introduced. Many new functions for maintenance purposes, for example self-supervision, integrated event monitoring and disturbance recording have been common IED-functions already about 15 years period of time. Clearly, a cyber-secure IoT will be developed to monitor all aspects of the utility. Due to this evolution, there has been functional integration towards fewer number of physical IED’s. A greater level of functional integration has been evolving at all voltage levels.

2.5 Compliance

In as much as IEC 61850 deals with interoperability, it does not imply a simplistic “plug-and-play” approach to equipment selection and system implementation.

Part 10 sets out a regime for determining Compliance to the Standard—specifically in terms of the core Parts 6, 7-1, 7-2, 7-3, 7-4 and the implemented protocols of Part 8-1 and/or 9-2. In particular, the term “Compliance” refers specifically to devices that have undergone testing to that regime by specifically accredited test houses which are endorsed by the UCA International Users Group [5].

Indeed, the wording of the Certificate of Compliance at first seems somewhat unusual:

> *This device has not been shown to be non-conforming to ….*

Whilst being a “double negative”, it is an accurate statement reflecting firstly the testing processes and secondly the aspects that the vendor has requested to be tested.

It is to note that some equipment suppliers’ information claims “conforms to IEC 61850”, but this may simply mean that their device passes the environmental withstand requirements defined in Part 3 which, whilst important as a device selection criteria, is not specifically nominated in the official set of Parts required for the Certificate of Compliance defined in Part 10.

IEC 61850 sets out various mandatory compliance requirements as well as a number of options, with their own mandatory and optional components, in various aspects which the equipment vendor is free to implement as they see fit for their products. Therefore, IEC 61850 does not guarantee that a particular vendor’s compliant device has the functions that the **Systems Integrator** needs for a specific application and implementation. However, official Certified Compliance by a UCAIUG Accredited testing laboratory does guarantee that you will have access to all the documentation, files and information necessary for you to select equipment that has the functions and interoperability that you need for your implementation.

There is a further aspect of “version compliance” and “backward compatibility”. Whilst individual IEDs are tested and confirmed to be compliant with a specific version of the various Parts of the Standard, the ultimate system will remain in service for several decades over the life of the substation and hence there will inevitably be different generations of IEDs in service with different version compliance with different compatibility issues. As an example, Part 7-4 Ed2 introduced a standardised way of managing testing configuration which may be significantly different to the more proprietary testing function implementation which therefore presents a an "interoperability/compatibility" issues. These issues are addressed in more detail in Chaps. 8 and 10.

2.5.1 Editions and Amendments

The IEC has certain processes and terminology for updating of Standards. Parts of IEC 61850 have already moved on from their original Edition 1 to become Edition 2 and perhaps even further having Amendment 1 of Edition 2.

Under IEC processes, a Standard is a document that has been formally voted into acceptance by the various voting countries. As discussed above, this would be called an "International Standard" [2].

Other associated and official IEC documents would be referred to as Technical Specifications (TS) [3] or Technical Reports (TR) [4].

When document is updated, e.g. IEC 61850-7-4 [9], it may take the form of

- a complete new Edition of the document, e.g. IEC 61850-7-4 Ed2 released in 2010 [10]

  Such documents are compete "standalone" official Standard documents with all sections and text included

  or
- an Amendment to the Edition, e.g. IEC 61850-7-4 Amd1 to Ed2 [11]

  Such official Standard documents are only set of changes to the Edition, e.g. "replace section xxx with the following: …"

Certificates of Compliance will therefore refer to the tests carried out in respect of the Edition, or the Amendment to the Edition which implies separate Certification to the respective Edition.

In order to provide a better reader experience of having to refer to both the Edition and the Amendment documents simultaneously, the IEC in some cases issues a "Consolidated Version" document as the merge of the two official Standard documents. The Consolidated Version is referenced as a "point suffix" to the Edition, e.g. IEC 61850-7-4 Ed2.1 [12]. However, it is NOT an official Standard as it has not been voted on; hence, Certificates of Compliance cannot be issued stipulating Consolidated Version "Ed2.1".

2.5.2 Forward and Backward Edition/Amendment Compliance Compatibility

The versions of the Standard introduce some issues regarding compatibility both of the real-time communications processes and handling of different compliance regimes during the engineering process [13].

- Backward compatibility is an IED (device and tools) compliant to a newer Edition/Amendment being able to operate correctly in conjunction with IEDs (devices and tools) compliant to older Edition(s)/Amendment(s).
- Forward compatibility is an IED (device and tools) compliant to an older Edition/Amendment is able to operate correctly in conjunction with IEDs (devices and tools) compliant to newer Edition(s)/Amendment(s).

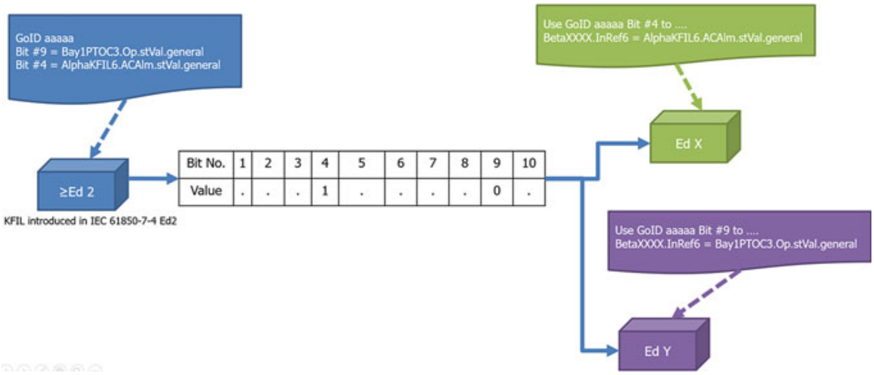
At least for a certain duration after new Editions/Amendments are issued, vendors can choose to which Edition/Amendment they seek compliance. Equally is not mandatory that a vendor seek to "upgrade" their existing Certifications, nor seek "backwards" certification.

From a user perspective, it is important to understand, how the new versions of the Standard will affect projects considering an IED (device and tool) compliant to:

- a newer Edition/Amendment is added to an existing system that was previously created using IEDs, tools and SCL files compliant to an older Edition(s)/Amendment(s) of the Standard.
- an older Edition/Amendment is added to a new system that is being built using IEDs, tools and SCL files compliant a newer Edition(s)/Amendment(s) of the Standard.

Firstly, it is to note that the real-time messages being sent from any IED (publisher, client or server) messages do not contain any specific identifier in the header or the Data Set that the message was created or that the contents of the message is based on any particular Edition/Amendment.

As shown in Fig. 2.6, GOOSE and Sample Value Data Sets are just a bunch of 1's and 0's. An IED may subscribe to a particular GOOSE or SV message, and accordingly be configured to use a particular bit(s) of the Data Set for a particular purpose. The compliance of the Publisher and of the Subscriber is of no consequence to the real-time message. In this example, the GOOSE Publisher is clearly compliant to at least Edition 2 as its Data Set includes information from the<<KFIL>>Logical Node which first appeared in IEC 61850-7-4 Ed2. The two Subscriber IEDs could theoretically be of any compliance and just use the bit(s) it needs. It suffices that the engineering process to configure each of the respective IEDs has correctly identified each bit(s) in the message and how it is used.


GoID aaaaa
Bit #9 = Bay1PTOC3.Op.stVal.general
Bit #4 = AlphaKFIL6.ACAlm.stVal.general
≥Ed 2
KFIL introduced in IEC 61850-7-4 Ed2
Use GoID aaaaa Bit #4 to ....
BetaXXXX.InRef6 = AlphaKFIL6.ACAlm.stVal.general
Ed X
Use GoID aaaaa Bit #9 to ....
BetaXXXX.InRef6 = Bay1PTOC3.Op.stVal.general
Ed Y

Bit No.	1	2	3	4	5	6	7	8	9	10
Value	.	.	.	1	.	.	.	.	0	.

Fig. 2.6 Bits on the "wire" have no reference to the edition of the sender or receiver (*Source* [7])

Obviously, an IED compliant to an earlier Edition/Amendment cannot send any bit(s) associated with a function that was only firstly defined in a later Edition/Amendment. If such is critical, the only solution is to upgrade the IED firmware or replace the IED completely.

An IED compliant to a more recent Edition/Amendment can use any bit(s) it receives from any device regardless of the sender's Edition/Amendment compliance.

However, MMS messages may be "evidently" related to different Editions/Amendments by the "nature" of the Command or Response/Report being sent.

- A Client IED compliant to an earlier Edition/Amendment cannot send commands uniquely defined as of a later Edition/Amendment, and may not be able to understand the response or Report sent by a Server IED compliant to a newer Edition/Amendment.
- A Client IED compliant to a newer Edition/Amendment maybe sending Commands that a Server IED compliant to an older Edition/Amendment cannot understand.
- A Server IED A Client IED compliant to an earlier Edition/Amendment may not understand, and hence be able to respond to commands sent by a Client IED compliant to a newer Edition/Amendment.
- A Server IED compliant to a newer Edition/Amendment maybe sending information that cannot be understood by a Client IED compliant to an earlier Edition/Amendment.

The final aspect of compatibility is the ability of the various IEC 61850-6 System Specification Tools, System Configuration Tools and IED Configuration Tools to import/export the System Configuration Language (SCL) files according to specific Editions. As an example, a tool developed and working under an IEC 6185-6 Edition 1 regime is not likely to be able to import or export the<<.SED>>or<<.IID>>files introduced in Edition 2. Furthermore, the tools should preferably have the ability to select which Edition the various files are imported/exported as.

Further information on the Edition compatibility issues is provided in IEC 61850-7-1 Ed2 Amd1, Annex K [14].

2.6 The Need for Expertise—Training

Whilst this book and other references provide guidance on technical implementation and application examples, it is paramount above all things to have a proper understanding of the technology. This applies to the needs in regards to developing a Business Case for embarking on the journey through to implementation philosophy, specification, implementation, factory acceptance testing, site acceptance testing, commissioning, in-service operation, maintenance and refurbishments/augmentations.

Training comes in various forms such as:

- reading web sourced material including CIGRE Technical Brochures
- in-person training
- vendor-based training
- specialised training providers.

References

1. CIGRE Technical Brochure 326.: The Introduction of IEC 61850 and its impact on Protection and Automation within Substations. CIGRE WG B5.11 (2007). https://e-cigre.org/publication/326-the-introduction-of-iec-61850-and-its-impact-on-protection-and-automation-within-substations
2. IEC International Standards (IS). https://www.iec.ch/publications/international-standards
3. IEC Technical Specifications (TS). https://www.iec.ch/publications/specifications
4. IEC Technical Reports (TR). https://www.iec.ch/publications/technical-reports
5. Utility Communication Architecture International Users Group (UCAIUG).: https://www.ucaiug.org/
6. CIGRE Technical Brochure 540.: Applications of IEC 61850 Standard to Protection Schemes. CIGRE WG B5.36 (2013). https://e-cigre.org/publication/540-iec-61850-standard-to-protection-schemes
7. Rod Hughes Consulting Pty Ltd.: https://rodhughesconsulting.com/: IEC 61850 Training Courses
8. IEC Technical Committees.: https://www.iec.ch/technical-committees-and-subcommittees#tclist
9. IEC 61850-7-4 Edition 1. https://webstore.iec.ch/publication/20080
10. IEC 61850-7-4 Edition 2. https://webstore.iec.ch/publication/6017
11. IEC 61850-7-4 Amendment 1. https://webstore.iec.ch/publication/27066
12. IEC 61850-7-4 Consolidated Version 2.1. https://webstore.iec.ch/publication/66551

13. PAC World Magazine.: Versions of the standard—what you need to know. Christoph Brunner, Chair of IEC TC57 WG10. https://www.pacw.org/versions-of-the-standard-what-you-need-to-know
14. IEC 61850-7-1 Consolidated Version 2.1. https://webstore.iec.ch/publication/67536

3 IEC 61850 User Specifications, Standards and End-Users

Alex Apostolov and Anders Johnsson

Abstract

The first section of this chapter covers the typical functions defined by specification standards, such as process interface, protection, control, automation, monitoring and recording. This is followed by the description of a four-step specification process starting with the template reflecting the protection, automation and control philosophy, followed by defined scheme, applied scheme and finally instantiated scheme for a specific power system component. The next section of the chapter covers IEC 61850-based specification tools such as the system configuration language, its files and specification tools. The documentation related to each of the specification steps is described later. The final section of the chapter introduces the different users groups that are providing feedback or helping with the maintenance of the standard such as the UCA international users group, ENTSO-E and the IEC TC 57 working groups, as well as the IEEE power system relaying committee.

Keywords

Substation PAC functions • Standards • Standardisation process • Documentation • Users

A. Apostolov (✉)
OMICRON Electronics, Los Angeles, USA
e-mail: alex.apostolov@omicronenergy.com

A. Johnsson
Vattenfall Eldistribution, Solna, Stockholm, Sweden
e-mail: anders.johnsson@vattenfall.com

P. Bishop and N.-K. C. Nair (eds.), *IEC 61850 Principles and Applications to Electric Power Systems*, CIGRE Green Books, https://doi.org/10.1007/978-3-031-24567-1_3

3.1 Specification Standards [1]

Many utilities are facing the challenge of having to prepare new specifications for substation automation or of having to adapt their existing specification to reflect the latest developments and new possibilities that are available for modern substation automation solutions.

A sustainable specification for substation automation shall ideally be prepared in such a way that it is focussing on functionality, performance, reliability, evaluation, project management and services to ensure a fair participation and evaluation of the bidders.

A substation automation system shall provide on the one hand all the functions that are required for the correct and safe operation of the primary equipment that is contained in a specific substation as well as for the adequate protection and condition monitoring. On the other hand, it has to incorporate compatible communication interfaces for the connection of the substation to one or more network control centres.

The scope of functionality of a substation control system depends on the following aspects:

- Size and significance of the substation.
- Range of voltage levels concerned.
- Operational philosophy (for testing, commissioning, operation and maintenance).
- Availability requirements as criteria related to the substation's criticality and significance in the grid or for consumers.
- Integration of the substation control functions into the user's network management concept, with a varying number of network control levels and a different distribution of functions between network control centres and substation control.
- Decoupling of the renewal cycles between substation control, power system management and transmission technology.
- In case of retrofit, the integration into the user's existing substation environment in terms of interfaces to the existing equipment and co-ordination with secondary devices for dedicated protection and monitoring that are not substituted by new IEDs that are integrated into the new substation automation system.

The consequences of the features of the IEC 61850 standard therefore are as follows:

- As has always been the case, the functions need to be specified; however, there is a new consideration of specifications that were previously "wire-based".
- It has to be decided whether the selection of devices is left to the Systems Integrator, whomever that may be or is limited by some pre-selection of devices homologated by the utility.

- Availability figures, operational/maintenance procedures and failure scenarios have to be discussed to get the most appropriate communication architecture.
- The environmental conditions have to be specified very much the same as before but some of these conditions might be decisive criteria for the selection of the communication architecture and, especially, of the communication media, e.g. copper cable or glass fibre.
- If the switchgear, CTs and VTs already exist, the specific type of process interface is important information for the System Architecture specification.
- If the process interface can be selected (conventionally hardwired or serially linked), this might have some important impacts on the optimisation process for the solution to be offered.

3.1.1 Process Interface Functions

In an electric power substation, the primary equipment can be considered as the "process". Most functions implemented in a substation operate based on the monitoring of the state of the primary equipment and the values of the electric power system.

Protection, automation, control and monitoring functions are required for all power system voltages. In general, these functions do not directly interact with the primary equipment, but rely on devices that provide process interface functions, such as:

- Switchgear interface.
- The switchgear interface provides the substation protection, automation and control system signals representing the status of the circuit breakers or switches and also applies the trip and close signals from the PACS to operate them when necessary.
- The process interface functions related to switchgear in IEC 61850 can be represented using logical nodes XCBR and XSWI.
- Analogue interface.
- The analogue interface converts the primary analogue signals into secondary signals that can be handled by the different SPACS devices in the substation.
- The process interface functions related to analogue signals in IEC 61850 can be represented using logical nodes from the T group, such as TCTR and TVTR.

3.1.2 Protection Functions

Substation protection functions monitor the electric power system parameters. They provide for necessary protection and isolation facility of all power circuits like generators, feeders, transformers, bus-coupler, reactors, etc. They provide alarm and trip commands under abnormal conditions and hence contribute to preserve the system from damage.

Protection functions can be:

- Local—implemented in a single device with direct acquisition of energising quantities from the local process interface. An example is phase overcurrent protection.
- Distributed—when different components of the protection function are located in different devices and they communicate over the network to implement the function. An example is busbar protection.
- Centralised—when all components of the protection function are implemented in a central device.

In IEC 61850, protection functions are implemented using logical nodes from group P. An example is PTOC for an overcurrent protection element.

Protection functions are implemented using peer-to-peer communications services.

3.1.3 Control Functions

Control functions perform purposeful actions, in general initiated by a human operator or automation, on different components of a substation or power plant to meet specified objectives. They work based on process variable quantities, specific to particular functional units of the plant.

In addition to control functions associated with specific control levels, there can also be control functions that link input and output variables across several control levels. For example, a breaker control function operates based on information on the status of the breaker and its disconnector switches as input variables and operates on the breaker's trip and close coils as output variables.

Control functions also can be local, distributed and centralised.

In IEC 61850, control functions are implemented using logical nodes from group C. An example is CSWI used to control circuit breakers and switches.

Control functions are typically implemented using client–server services, but also can be based on the use of peer-to-peer communications services.

3.1.4 Automation Functions

Automation functions are self-acting artificial functions whose behaviour is governed either by given decision rules or continuously in time by defined relationships, while the output variables of the function are created from its input and state variables and the decision-making rules.

Automation functions assist human operators in electric power systems in order to improve the safety and efficiency of operation. They also perform tasks that cannot be completed by operators fast enough to meet the performance requirements.

Automation functions also can be local, distributed and centralised.

In IEC 61850, automation functions are represented by logical nodes from group A. An example is AVCO used for automatic voltage control.

Automation functions are typically implemented using peer-to-peer communication services.

3.1.5 Monitoring Functions

Monitoring functions perform systematic collecting and analysing of measurable parameters that would give useful information about the condition of equipment and different system components and identify deviations from its expected performance to forecast the likelihood of potential failure.

Monitoring functions also can be local, distributed and centralised.

In IEC 61850, monitoring functions are represented by logical nodes from group S for supervision and monitoring. An example is SCBR used for circuit breaker monitoring and supervision.

Generally, global supervision functions use client–server MMS report implemented with SCADA/HMI servers. IEC 61850 monitoring functions provide mechanisms to be implemented using peer-to-peer communication services.

3.1.6 Recording Functions

Recording functions perform systematic collecting and storing of measurable parameters and status information that would give useful information about the operation of equipment and different system components to identify deviations from its expected performance during a specific electric power system event.

Recording functions also can be local, distributed and centralised.

In IEC 61850, recording functions are represented by logical nodes from group R for protection-related functions. An example is RDRE used for disturbance recorder function.

Recording functions are typically implemented using peer-to-peer communication services.

3.1.7 Reporting Functions

Reporting functions apply transformations to stored data and make the results available to the end-user to provide information or satisfy business needs such as control and maintenance.

Reporting can be:

- Unbuffered.
- Buffered.

In IEC 61850, reporting functions are associated with logical nodes from all groups.

Reporting functions are implemented using dedicated communications services.

3.1.8 Communications Functions

Communications functions support the data and information exchange between the different components of the protection, automation and control system.

Communications functions are implemented using different communication types:

- Client–Server.
- Peer-to-peer.

3.2 Specification Process [2]

In order to improve the efficiency of all aspects of utility operations, the specification process should be based on standard protection, automation and control schemes integrating the different functions described in the previous sections of this chapter.

The development and implementation of standard protection, automation and control schemes require the definition of a utilities' internal standardisation process that is understood and accepted by all participants that are involved in the life cycle of electric power systems assets.

The process needs to specify:

- Protection, automation and control philosophy
- Setting and other parameters
- Functional and performance requirements for the different types of applications
- Integration constraints
- Adaptability to application variations and changes to technology
- Long-term stability and sustainability
- Design efficiency.

In order to meet the above requirements, the standardisation process should go through several standardisation phases as described in the following sections. The specifications made at each stage are inherited by all later stages in the process.

A scheme that is subject to the standardisation process described below should be selected based on user-specific specifications resulting in a different set of functional and performance requirements. The following sections give an overview of the four phases of the standardisation process. A generator bay is taken as an

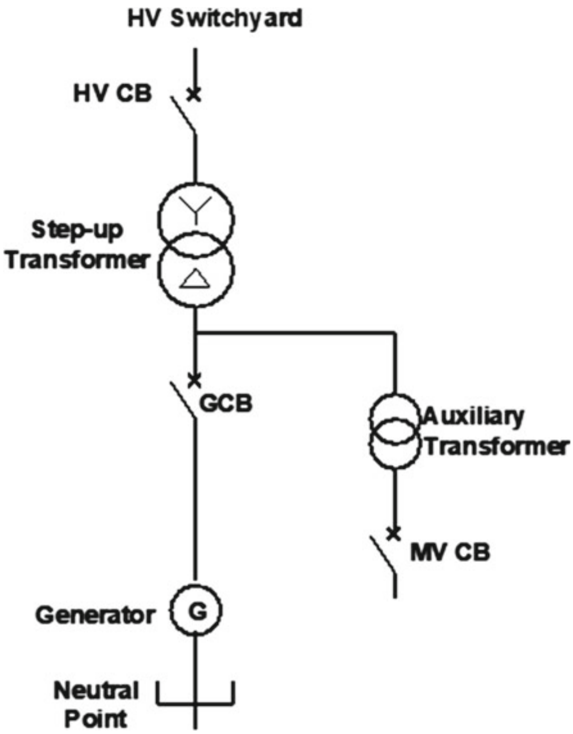


Fig. 3.1 Generator bay single-line diagram (*Source* [2])

example to illustrate the development process. The basic single-line diagram of the primary system is shown in Fig. 3.1.

3.2.1 Standard Scheme—Template

This is the conceptual description of the scheme and is typically the formalised description of the application of protection and control philosophy to a specific type of electric power system equipment. The templates should include all of the necessary components of the documentation of each subsequent stage. Refer to Fig. 3.2.

At this stage, the functional requirements and integration constraints need to be defined. These are in detail requirements associated with busbar topology, voltage level, communications, bay type (e.g. transformer, line, etc.), resulting in some interfaces and functions being defined. Moreover, system issues such as reactive power generation, power system earthing situation, station criticality or protection philosophy must be covered.

Items that are left “generic” at this stage are types of primary equipment or IEDs. They may be considered but are not specified at this stage (Table 3.1).

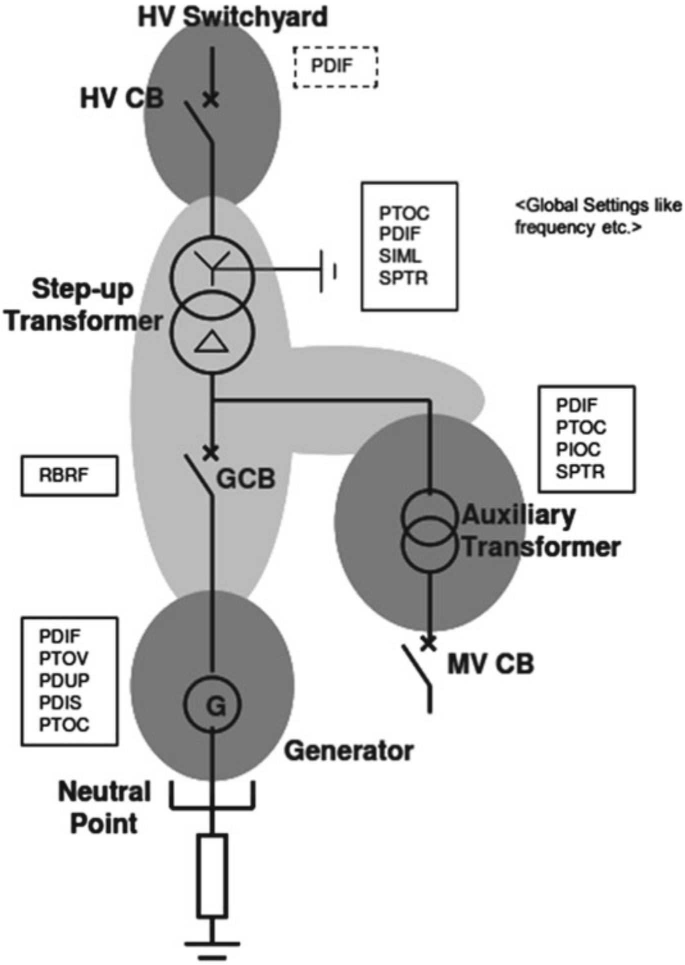


Fig. 3.2 Example stage "A": definition of different protection zones (*Source* [2])

3.2.2 Standard Scheme—Defined

This development stage of a standard scheme defines the primary plant and the hardware interfaces with the specific type of bay covered by the scheme and can be used for the same or similar types of new or existing installations without ANY changes in external wiring, signalling and equipment. Allocation of functions to generic or abstract IEDs is also defined at this stage. Refer to Fig. 3.3.

Table 3.1 Legend of logical nodes (LNs) according to IEC 61850-7-4

Logical node	IEEE C37.2	Description
PDIF	87G, 87T, …	Differential protection
PTOV	59G, 59GN	Overvoltage protection
PDUP	32	Reverse power protection
PDIS	21	Distance (impedance) protection
PTOC	51/51N/46	Time overcurrent protection
PIOC	50	Instantaneous overcurrent protection
RBRF	50BF	Breaker failure protection
SIML	26T	Insulation medium supervision (liquid, e.g. oil)
SPTR	63T, 49T	Power transformer supervision

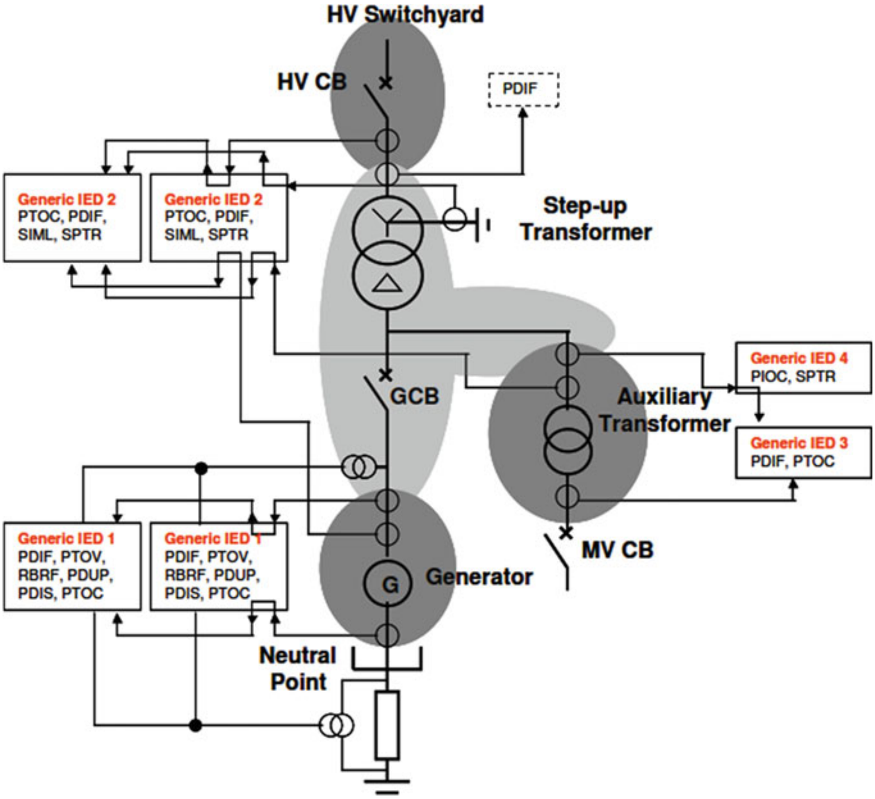


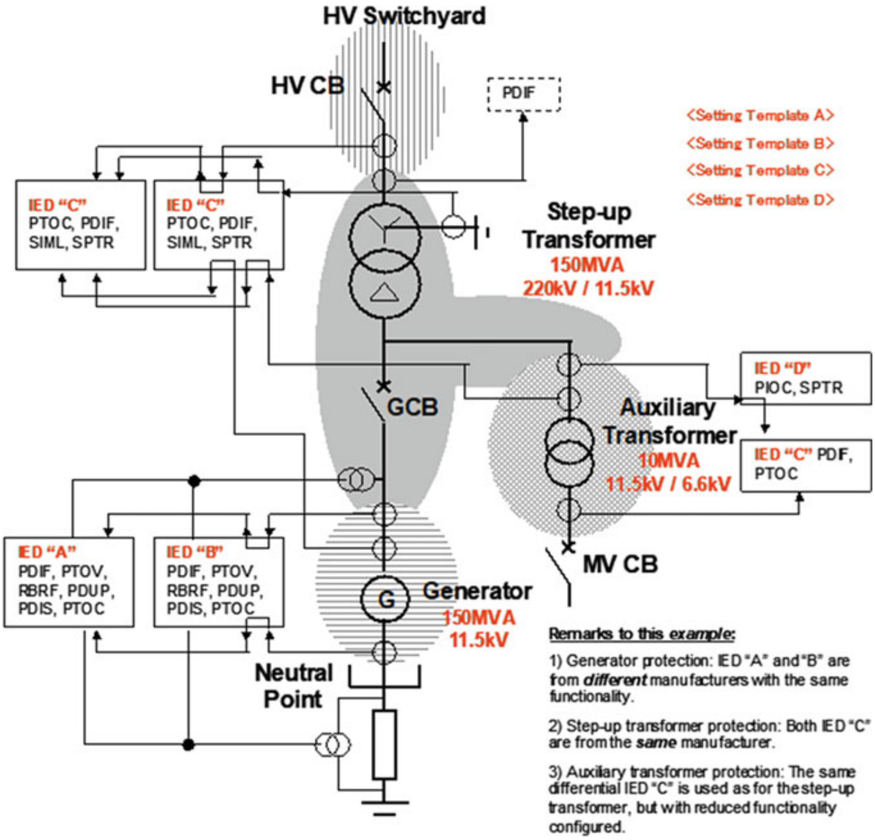
Fig. 3.3 Example stage "B": basic protection functions and interfaces defined (*Source* [2])

3.2.3 Standard Scheme—Applied

This is typically considered by a utility as a “standard scheme”. This includes the use of approved specific IEDs or other secondary equipment. The IED selection should ensure that all functions and functional elements defined for the scheme template in stage “B” are available in the selected IEDs. The global settings, including programmable scheme logic, of the IEDs are introduced at this level of standardisation. However, at this stage there are still no local settings or other site-specific configuration parameters. Refer to Fig. 3.4.

A standard scheme is a scheme which can be used for same or similar types of new or existing installation without ANY changes in internal wiring, signalling, equipment or enabled functional elements.

In case the user wants to use different IEDs (e.g. from different vendors) for the same scheme, it will result in a different scheme template implementation that meets the requirements of the above definitions.



Remarks to this example:

1) Generator protection: IED “A” and “B” are from *different* manufacturers with the same functionality.

2) Step-up transformer protection: Both IED “C” are from the *same* manufacturer.

3) Auxiliary transformer protection: The same differential IED “C” is used as for the step-up transformer, but with reduced functionality configured.

Fig. 3.4 Example stage “C”: IEDs defined, equipment data fixed (*Source* [2])

3.2.4 Standard Scheme—Instantiated

This is a site-specific implementation of the standard scheme (i.e. an instantiated standard scheme template from stage “C”). Site and application-specific settings are implemented at this stage, and all hardware is defined. Refer to Fig. 3.5.

While instantiation excludes any modifications besides setting parameters and site-specific naming, specialisation on stage “D” offers the opportunity to adapt the standard scheme typically to variations in primary Hardware (HW) components.

Note: In special cases, other modifications can be considered. This may appear as a deviation from the standardisation process; however, it takes advantage of the developed standard scheme for a special application that may not justify going back to stage “C” of the process.

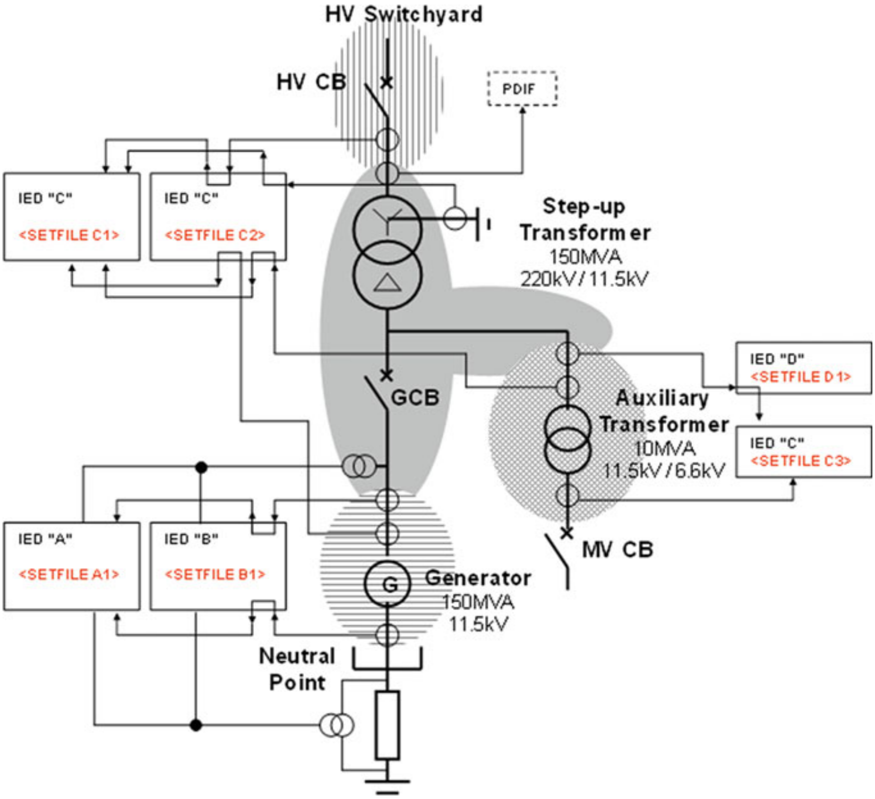


Fig. 3.5 Example stage “D”: everything specified, including setting files (*Source* [2])

3.3 Specification Tools [3]

The engineering of substation protection, automation and control systems based on IEC 61850 is a very complex multi-step process that requires precise specification of the primary and secondary system, their connectivity, functionality and performance.

The engineering process may involve the following:

- Users
- Manufacturers
- Consultants
- Integrators.

They are all involved at different stages of the engineering process. To ensure the most efficient delivery of the final substation protection, automation and control system, it is necessary to use a top-down approach based on advanced specification tools.

3.3.1 System Configuration Language (SCL)

IEC 61850 part 6 (Configuration description language for communication in electrical substations related to IEDs) is a key part of the standard that allows engineering tools to create files that are used to describe the capabilities of the IEDs, the functions that are in use and the communication between various functions that are implemented in these IEDs. These files are used with test systems to configure the test devices. The file with the .SCD extension (Substation Configuration Description) contains the information of all IEDs in the system and their communication configuration. This file will also contain information about IEDs that may be physically missing. Some IED configuration tools export only files with .CID extension type (Configured IED Description) that contains the configured functions, messages to be received by the IED and the communication parameters of the IED. The test system configuration tool reads the SCD file (or multiple CID files) to get all information about the IEDs in the system or parts of the system to be tested. The use of engineering tools and SCD, ICD and CID files is illustrated in Fig. 3.6. Refer to Chap. 7 for further information and considerations regarding tools and configuration.

3.3.2 SCL Files

IEC 61850 defines several types of files required to support the intended engineering process. An IED or a system solution compliant with the standard has to support the use of the files described below. This can be implemented directly in the IEDs or achieved through tools delivered with the system.

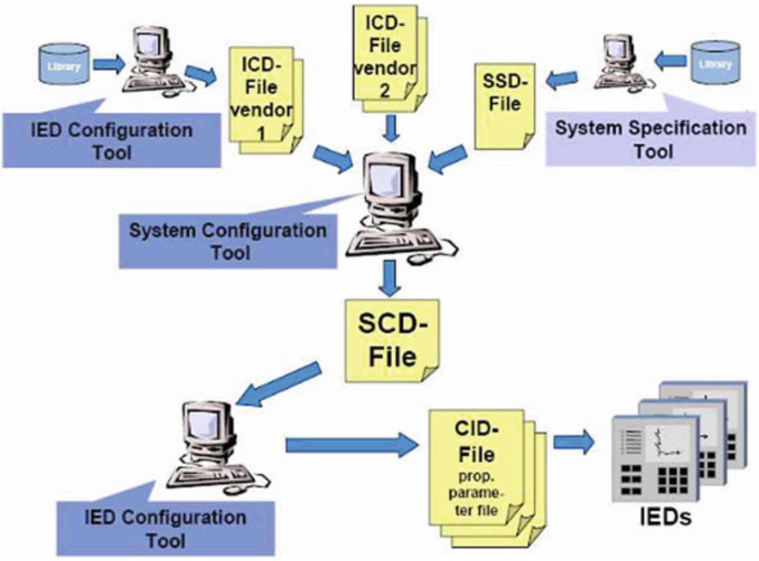


Fig. 3.6 Application of engineering tools and SCD, ICD and CID files (*Source* [4])

System Specification Description (SSD)

If a top-down engineering process is applied, the description of the system is the first step in the engineering process. Until now, this approach has not often been consistently applied. The IEC 61850 engineering process envisions the use of substation specification tools that allow the user to describe the substation design and associated functions for the substation protection and automation systems. The data exchange from such a system specification tool and other tools utilised in the process should be based on the System Specification Description files defined in IEC 61850.

These files have an SSD extension.

The SSD file describes the single-line diagram of the substation and the functional requirements represented by logical nodes. The logical nodes can be abstract in the sense that they are not allocated to specific IEDs. The SSD file defines a Substation part, Data type templates and logical node type definitions but may not have an IED section.

IED Capability Description (ICD)

The functional capacity of an IED in the substation configuration language is represented by the IED Capability Description (ICD) file. It is used for data exchange from the IED configuration tool to the system configuration tool. This ICD file describes the capabilities of an IED. Since it represents the functional capacity (i.e. before it has been configured), the IED name in this file is **TEMPLATE**. The file also includes the different logical node types as they are instantiated in the device. The .ICD file extension is for IED Capability Description. This file is required to be supplied by each manufacturer and is used for the complete system configuration. The file contains a single IED section, an optional communication section and an optional substation part which denotes the physical entities corresponding to the IED.

System Configuration Description (SCD)

The configuration of the system is represented by the System Configuration Description (SCD) file. It contains substation description section, communication configuration section and all IEDs. The IEDs in the SCD file are configured to operate within the substation protection and automation system. These files are then used to configure the individual IEDs in the system.

Configured IED Description (CID)

Derived from the SCD, the Configured IED Description (CID) file represents the entire configuration of one individual IED as it is "in service". It includes the substation specific names and addresses instead of the default ones in the ICD. It may include private content added by the IED configuration tool Instantiated IED Description (IID).

Instantiated IED Description (IID)

The Instantiated IED Description (IID) file represents the configuration of one IED but is used to re-instantiate that IED into the SCD file after the existing instance has been modified in the IED configurator tool. However, the IED configurator tool must not change any of the existing communication configurations with the other functions. The IID contains one IED section, the communication section with the IED communication parameters, the IED data type templates and, optionally, a substation section with the binding of functions (Logical Nodes) to the single-line diagram.

System Exchange Description (SED)

The System Exchange Description (SED) is a file which is to be exchanged between system configurators of different projects. It describes the interfaces of one project to be used by another project, and at re-import the additionally engineered interface connections between the projects. It is a subset of an SCD file with additional engineering rights for each IED as well as the ownership (project) of SCL data.

IED Specification Description (ISD)

Allocation of functions to generic (abstract) IEDs is part of the engineering process. The required functionality of individual IEDs can be described also using the newly defined IED Specification Description (ISD) file format, thus allowing the automation of the procurement process based on exchange of such files between the utility and its suppliers. This will support automatic selection of the IEDs that meet the requirement specification for a specific standard scheme by comparing the ISD file with the existing IED Capability Description (ICD) files. This file is intended to be included in the next edition of IEC 61850 (part 6—edition 3).

3.3.3 System Specification Tool (SST)

The role of a System Specification Tool (SST) is to support the design of an IEC 61850-based substation considering the voltage levels, bay layout and required functionality. It may also be used to specify the preferred allocation of functions in devices to be used in the substation, as well as the signal flow between them.

The SST is not intended to specify how this is completed or what actual IEDs are being used.

It allows the user to graphically construct the Single Line Diagram (SLD) specifying voltages, bay types, primary plant components, bay names and layout.

The SST is using an object-oriented approach, so the bay types and primary plant are drawn from library templates, and any modifications to the underlying template affect all bays utilising the template.

The output of the SST is a SSD file that can then be exported from the drawn Single Line Diagram and used by the system configuration tool to produce the resulting SCD file.

The SST can also be used to create hierarchical function blocks at each substation, voltage or bay level. These functions are a functional description of required application, such as Breaker Fail Protection and Breaker Management. The SST can then be used to add expected Logical Nodes (LN) and resulting signals to each function block.

The SST can also be used to specify distributed communications using GOOSE messages for relevant protection function blocks and their interactions.

3.4 Documentation [2]

Although a PACS incorporates many technology options, we must state that IEC 61850 itself is fundamentally a definition of an engineering process to specify and configure the system and participating IEDs to be able to interact in real time.

The SCL process defined in Part 6 of the standard deals with the information exchange between the different IEC 61850 tools in the form of documentation structured in an XML schema as just one small part of the entire engineering process.

While documenting the IED capabilities, IED configuration and system operation, for the purpose of use by another tool, it also needs to be stated that the IEC 61850-6 SCL files are not necessarily suitable documents for human use, but to support an efficient engineering process based on the use of SSTs and SCTs. Despite being nominally "readable" by humans, the SCL files do not necessarily provide a means for easily describing and allowing understanding of what the system is and how the system is operating as it lacks any form of user-oriented visual

Table 3.2 Different SCL files for documentation at the different stages of the development of standard schemes

	Phase	Bay	PAC devices	Plant application/ Substation	What it means
A	Standard scheme—template	G	G	G	Totally generic: SSD, ISD
B	Standard scheme—defined	S	G	G	All HW interfaces fixed SSD
C	Standard scheme—applied	S	S	G	IEDs fixed ICD, IID
D 1 2	Standard scheme: Instantiated Instantiated with small modifications	S	S	S	Everything fixed, also settings (= standard scheme applied in reality) SCD, CID

Source [2]
S = specific; *G* = generic; *B* and *C* can be one step

notation/syntax. But it is definitely a proper form of documentation when the SSTs and SCTs can visualise or export the information in the familiar user-readable formats.

The information that needs to be provided at the different stages of the development of the PACS is described in the following sections.

Table 3.2 shows the use of different SCL files for documentation at the different stages of the development of standard schemes.

3.4.1 Standard Scheme—Template

The specification documents associated with the A templates have a threefold purpose:

1. To document each of the PAC functions foreseen in the scheme template, clearly explaining the reason for its use and conceptually describing how it must work (the scheme templates being a part of the specifications as well)
2. To define the design requirements that must be taken into account in the subsequent development stages of the standardisation process—explained in Chap. 7.
3. To show the functional or operational constraints caused by the functions foreseen in the scheme templates in the following stages of the standardisation process or in their implementation in on-site installation. Reference is made to Chap. 8.

The design requirements typically cover the following aspects:

- The authorised level of functional integration (generic principles): Generally speaking, the more PAC functions are implemented in a minimum number of IEDs, the higher the level of functional integration will be. The level specified allows to achieve the desired compromise between a limitation on the number of IEDs used and the complexity of their programming files (Chaps. 7 and 8).
- Rules to be followed regarding the interface methods between the cubicle and the outside world (both on a process level and on a substation level). The two major options currently in use are traditional wiring and optical fibres or combination of both (Chap. 7).
- Characteristics of the CT circuits (1 A or 5 A).
- General design principles: number of main protections used, types of protections, the level of separation between protection and control functions, tripping and reclosing philosophy (single pole vs. 3-pole), multiple trip coils, etc. (Chap. 7)
- Substation to substation communication constraints based on the type of protection principles selected (Chap. 13).
- Constraints regarding the general layout of a cubicle: size, height, maximum authorised weight, colour, accessibility of information displayed on the front of IEDs, constraints regarding the relative position of each component, the opening direction of the door, etc. (Chap. 7)
- Rules to be followed regarding the number of auxiliary circuits to be used and their distribution between the different PAC functions.
- Generic requirements regarding test methods (Chap. 9).
- General performance requirements (maximum start time, maximum trip time, etc.).
- Generic requirements on communication architecture (e.g. star or ring topology at the substation level) (Chap. 4).
- General requirements for cabling (section, colour, etc.) (Chap. 7).
- IEC 61850 model for each function (Chap. 8).
- Basic Application Profile for each function.
- Interoperability requirements (Chap. 10).
- Cyber Security requirements (Chap. 6).
- Standards and norms to be complied with
- Other.

Note: The level of details of design constraints is user-dependent and should be carefully defined.

The functional and operational constraints resulting from the functions foreseen in the scheme templates generally relate to the following:

- The ranges of settings available for various protection functions
- Other.

The specification documents should be structured in two parts:

- A part relating general principles that apply to any standard scheme. This information should be gathered in an apart document that is referred to (these are general principles that apply to any standard scheme)
- A part specific to each scheme template.

They should also take advantage to the most extent of the modularity of the scheme components by setting up specifications for each function and by reusing them as such in all documents when possible.

The elements coming from stage A that must be included within the documentation are:

- At the drawing level: conceptual single-line diagrams, conceptual description of the PAC functions, trip matrix
- At the specifications level: the specifications resulting from the stage A of the process
- At the settings level: the settings template resulting from the stage A of the process
- At the testing level: general requirement for testing the PAC scheme (contents and tools).

3.4.2 Standard Scheme—Defined

At the end of stage B, the specifications set up during stage A for each template must be completed with the following information:

- Detailed characteristics of the primary equipment at the bay level and the secondary equipment at the substation level associated with the B template
- IEC 61850-based list of signals going through the different interfaces (cubicle and IEDs levels). The main characteristics of each signal should be also described (typical example: high logical state or low logical state in normal situation)
- Requirements for the abstract IEDs used in the different templates:
  - Types of communication channels that must be used (optical fibres, RS232/485 ports, hardwired binary inputs and binary outputs …)

  - Technical features of each communication channel (e.g. activation threshold for the binary inputs, protocol names and versions, power that can be broken by the outputs, …)
  - Number of inputs and outputs needed, taking into account the rules regarding the use of auxiliary supplies (as defined at stage A) when hardwired binary inputs and binary outputs are used
  - PAC functions (with references to their corresponding conceptual description setup at stage A) that must be implemented within the IEDs
  - Requirements resulting from the settings rules according to settings templates defined at stage A
  - Type, format and characteristics of the information that must be available through the IEDs' HMI
  - Type, format and characteristics of the internal fault recording system and internal monitoring tools (such as event lists)
  - Any other general constraints related to bay equipment that could impact the characteristics of the IEDs.
- List of the abstract IEDs used in the different templates, mixed with the corresponding conceptual drawing describing the PAC function (set up at stage A) so as to obtain the functional diagram of each template.

At the end of stage B, the drawing and specification topics set up during stage A that must be completed with the following elements:

- At the drawing level: functional diagram associated with each B template
- At the specifications level: detailed characteristics of the primary equipment at the bay level and the secondary equipment at the substation level associated with the B template, list of signals associated with various interfaces, requirements for the different abstract IEDs used
- At the testing level: specific requirements for the test equipment that needs to be used to test the interfaces in the next stages of the process.

3.4.3 Standard Scheme—Applied

The defined standard scheme from stage "B" forms the basis of the specification of the stage "C" applied standard scheme. For each defined standard scheme, there may be a suite of stage "C" templates. The "C" specification includes information such as:

- Identification of its associated stage "B" scheme template.
- Full details of the approved IEDs, including versions, and any other secondary equipment to be used for the particular application.
- The scope of application.
- Cubicle construction and installation instructions, including mounting, layout, ratings, wiring, terminations and workmanship requirements.

- IED setting guidelines.
- Testing requirement refinements, in addition to those previously established at stage "B", arising from the actual functions in the approved IEDs.

The resulting set of so-called C templates constitutes the starting point for stage "D" of the standardisation process (Standard Scheme—Instantiated) detailed in the next chapter.

The standard applied scheme documentation shall basically consist of:

- Applied Single line diagram.
- Trip and signalling matrix.
- Approved IED types, versions and ordering codes.
- IED protection and control function diagrams.
- IED input/output lists, including hardwired or protocol-based alarms.
- IED setting and programmable scheme logic files.
- IED settings template and guidelines.
- Secondary equipment materials lists.
- Triggers to disturbance recorder.
- Cubicle wiring and layout diagrams.
- Bay wiring tables and cable schedules.
- Construction and installation instructions and procedures.
- IED and scheme test procedures/protocols.

3.4.4 Standard Scheme—Instantiated

The standard scheme that is designed in stage "C" is used to define the site-specific implementation. For each bay/feeder, the appropriate applied standard scheme needs to be chosen. If the applied scheme can be based on a "C" template without any modifications, a D1 standard scheme will result.

The specification includes information like:

- Scheme number
- Bay identifiers such as substation naming, voltage level and numbering
- Bay specific parameters used to determine the scheme setting
- Cubicle numbering
- Interface specific identifier (cores, cabling, tags)
- Other site-specific information.

In order to create a "D2" variation of the standard scheme, it is necessary to apply the standards in an "intelligent" manner. This will depend to a great extent on the level of variation from the standard scheme and the experience of the protection engineer applying it.

In the specification, scheme parameters that define any variation from the standard scheme, such as primary equipment, field cabinets, auxiliary system (such as batteries, AC/DC system, diesel generator, auxiliary transformer and local distribution), control and protection, communications, HMI and cabling, must be included. From that, an informed decision can be done on which of “C” standard scheme can be used as a basis for the “D2” variation.

The copy and paste “D1” based on the standard stage “C” documentation should be used as a basis based on the scheme identifiers and parameters from the specification. Each cubicle/equipment shall have a unique and complete set of documentation as defined in stage “C”, namely interface and wiring diagrams, layout, part list, etc.

The documentation of the in-service scheme needs to have a revision control according to the user’s philosophy and practice.

For the standard scheme “D2”, any additional documentation related to the variation should be included.

It is important to use formal procedure for quality assurance and acceptance of documentation.

3.5 End-to-End Users Groups

IEC 61850 has been developed for more than a quarter of a century, creating a completely different environment for the engineering and implementation of PACS. As a result, it is a living standard that is evolving with the changing electric power industry.

To provide feedback and support the identification of gaps or issues with its implementation, the industry created users group whose goal is to provide such input and help with the definition of the requirements for future development.

3.5.1 UCA International Users Group

The UCA® International Users Group (UCAIug) is a not-for-profit corporation consisting of utility user and supplier companies that is dedicated to promoting the integration and interoperability of electric/gas/water utility systems through the use of international standards-based technology. It is a User Group for IEC 61850, the Common Information Model (CIM per IEC 61970, IEC 61968 and IEC 62325) and the Open Field Message Bus (OpenFMB per NAESB standards).

UCA IUG Mission: To enable utility integration through the deployment of open standards by providing a forum in which various stakeholders in the utility industry can work cooperatively together as members of a common organisation to:

- Influence, select and/or endorse open and public standards appropriate to the utility market based upon the needs of the membership.
- Specify, develop and/or accredit product/system-testing programmes that facilitate the field interoperability of products and systems based upon these standards.

- Implement educational and promotional activities that increase awareness and deployment of these standards in the utility industry.

The focus of UCAIug is to assist users and vendors in the deployment of standards for real-time applications in the electric utility industry. The users group does not write standards and shall, where appropriate, work closely with those standards bodies that have primary responsibility for the completion of standards (notably IEC TC 57: Power Systems Management and Associated Information Exchange).

3.5.2 ENTSO-E

ENTSO-E, the European Network of Transmission System Operators, represents 42 electricity transmission system operators (TSOs) from 35 countries across Europe, thus extending beyond EU borders.

ENTSO-E promotes closer cooperation across Europe's TSOs to support the implementation of EU energy policy and achieve Europe's energy and climate policy objectives, which are changing the very nature of the electric power system.

To support the implementation of IEC 61850 by its members, ENTSO-E created a task force of its members with the task to identify gaps and issues related to the implementation of the standard and provide feedback to IEC TC 57 WG 10 for consideration.

3.5.3 IEC TC 57 WG 10 IEC 61850 User Feedback Task Force

The IEC TC 57 WG 10 IEC 61850 User Feedback Task Force was created initially to address the issues identified by ENTSO-E.

It meets at the IEC TC 57 WG 10 meetings and provides comments resolution to the received feedback.

3.5.4 IEEE PES PSRCC IEC 61850 User Feedback Task Force

The IEEE PES (Power and Energy Society) PSRCC (Power System Relaying and Control Committee) IEC 61850 User Feedback Task Force was created to address the issues identified by mostly North American utilities.

It meets at the IEEE PES PSRCC and provides comments to be considered by The IEC TC 57 WG 10 IEC 61850 User Feedback Task Force.

3.5.5 IEC 61400 USE61400-25—Wind User Group

The mission of the IEC 61400-25 user group (USE61400-25) is to support the use of the IEC 61400-25 standard series for wind power plant communication. The vision is to add value for the users, share information and documents of relevance for use of IEC 61400-25 and to provide a discussion forum for resolution of technical issues. USE61400-25 allows users to give feedback to IEC 61400-25 maintenance team, and the group management team coordinates activities with related user groups and organisation.

References

1. CIGRE Technical Brochure 329—Guidelines for Specification and Evaluation of Substation Automation Systems. Working Group B5.18 (2007). https://e-cigre.org/publication/329-guidelines-for-specification-and-evaluation-of-substation-automation-systems
2. CIGRE Technical Brochure 548—Implications & Benefits of Standardised Protection & Control Schemes. Working Group B5.27 (2013). https://e-cigre.org/publication/584-implications-and-benefits-of-standardised-protection-and-control-schemes
3. CIGRE Technical Brochure 760—Test strategy for Protection, Automation and Control (PAC) functions in a fully digital substation based on IEC 61850 applications. Working Group B5.53 (2019). https://e-cigre.org/publication/760-test-strategy-for-protection-automation-and-control-pac-functions-in-a-fully-digital-substation-based-on-iec-61850-applications
4. CIGRE Technical Brochure 466—Engineering Guidelines for IEC 61850 Based Digital SAS. Working Group B5.12 (2011). https://e-cigre.org/publication/466-engineering-guidelines-for-iec-61850-based-digital-sas

4 IEC 61850 Communication Architectures and Services

Rannveig S. J. Løken

Abstract

This chapter introduces the IEC 61850 architectures and services. The Station bus and Process bus in the Protection, Automation and Control System are explained. Architectures like RPR and HSR are described as well as services related to GOOSE, MMS and SV.

Keywords

Station bus • Process bus • Architecture • PRP • HSR • GOOSE • MMS • SV • Latency

IEC 61850 [1] is not a communication protocol standard but is a platform for the engineering of the data interchange, data modelling, configuration definition and system and project management. The way the data is transported and delivered is open for any implementation. The way the data is available is open for different applications, but seeking for a standard model for well-known related data. The way the data is mapped for transportation and delivery uses the concept of services. Different services have different features, some providing efficient low-latency delivery, while others provide more secure but latency-added interchange in both directions: one better for protection and interlock applications and others better for SCADA.

R. S. J. Løken (✉)
Statnett, Oslo, Norway
e-mail: Rannveig.loken@statnett.no

P. Bishop and N.-K. C. Nair (eds.), *IEC 61850 Principles and Applications to Electric Power Systems*, CIGRE Green Books, https://doi.org/10.1007/978-3-031-24567-1_4

4.1 Protection Automation and Control Systems Communication Architecture

Digital technology and the evolution of communication have significantly changed the substation communication and protection technology. Modern IED's and serial-type Station bus communication and later IP-based IEC 61850-Ethernet communication have been the main technology drivers.

Protection, Automation and Control Systems (PACS) can be described as three levels of devices:

1. Station level and functions related to the overall facility and the provision of the communication interface to the Grid Control Centre
2. Bay level and functions related to a specific part of the facility, e.g. the busbar itself, a transformer, an incomer bay, an outgoing feeder, etc.
3. Process level as the primary equipment including the transformer, instrument transformers/sensors, switchgear, reactive plant, etc.

   IEC 61850-2 [2] defines process-level functions as:

   "all functions interfacing to the process, i.e. binary and analogue input/output functions like data acquisition (including sampling) and issuing of commands"

   In this respect, the note to this definition states:

   "The process level functions may be implemented in the bay level IEDs together with the bay level functions if no Process bus is applied. If a Process bus is applied the process level functions are implemented in process level IEDs".

The PACS LAN provides interconnection between these three levels in order to exchange different types of signals for specific purposes.

According to IEC 61850-7-1 [3], the sample substation architecture as shown in Fig. 4.1 focuses on the support of PACS functions and data exchange.

(1) IEC 61850-9-2-based sampled value exchange,
(2) fast exchange of I/O data for protection and control,
(3) IEC 61850-8-1 GOOSE,
(4) engineering and configuration,
(5) IEC 61850-8-1 MMS-based client/server—monitoring and supervision,
(6) IEC 61850-8-1 MMS-based client/server—control centre communication,
(7) IEC 61850-9-3 (IEEE 1588) time synchronisation.

Figure 4.1 depicts the reference communication architecture for PACS as defined in the IEC 61850 standard [1]. Specifically, the figure illustrates the levels where Station bus and Process bus communication networks are used.

Normally, there is communication to the Control Centre from a Gateway or RTU from the Station bus level and also a connection to the HMI and Engineering system in addition to asset management system.

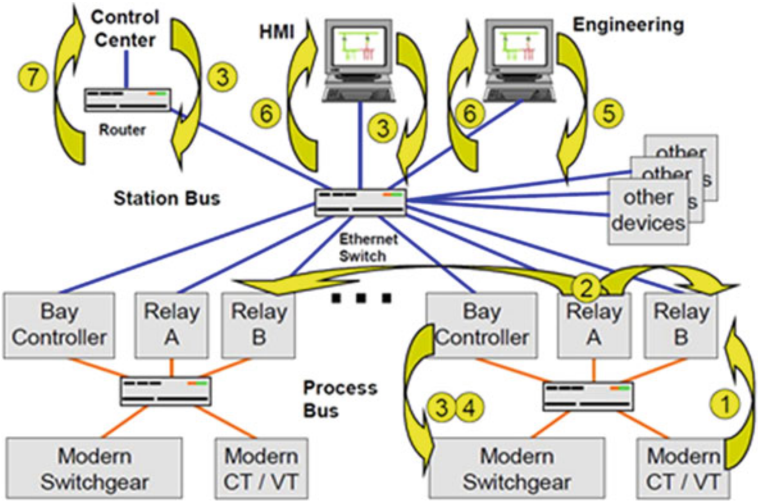


Fig. 4.1 Example of an PACS architecture, (IEC 61850-7-1, Figure 2) [3]

The two main interfaces are the Station bus and the Process bus (in Fig. 4.2, from IEC 61850-9, Figure 9, [4]). IEC 61850-5 [5] uses the terms “Station bus” and “Process bus” with no precise definition. In reality, these two buses are not specific physical entities, i.e. any particular segment of LAN cabling or LAN switches could be carrying both Station bus and Process bus-related signals. The common understanding is:

- The Station bus interconnects the whole substation and provides connectivity between central management and the individual bays. It also connects the protection and control devices within a bay, the different bays among themselves and the bays with the SCADA or grid control Gateway. The Station bus may connect up to hundreds of IEDs. In large networks, the Station bus is segmented, but all segments come together at the supervisory level. Several physically distinct Station buses are often used, e.g. one per voltage level, with or without horizontal connection. The Station bus typically carries GOOSE (Layer 2 multicast) traffic and TCP/UDP (unicast) traffic (MMS, SNTP, SNMP, FTP, etc.). The Station bus is expected to provide soft real-time response. Some jitter in delivery time is thus acceptable.
- The Process bus is specifically the part of the substation LAN that connects to the process equipment, i.e. the connections to the primary plant as switchgear, transformers, reactive plant and even IEDs associated with yard lighting, physical security, etc. It carries all forms of messages as GOOSE and MMS to/from the process devices as well as sampled values from the process devices. The Process bus in fact may appear in a “virtual” sense at the station-level equipment such as the station HMI, station gateway and station condition monitoring

devices. The Process bus topology may be different to the Station bus topology in order to service particular performance needs, the Process bus LAN can be physically segregated from the Station bus LAN, and hence, the Bay IEDs may need independent Station bus and Process bus LAN ports. As the Process bus carries essential real-time signals related to the primary power system as required for protection, automation and metering functions, the Process bus in particular has stringent real-time response requirements, i.e. the transmission guarantees a worst-case delivery time. How to meet these requirements is not in the scope of IEC 61850 [1] and depends on architecture and equipment chosen by the user and/or the system integrator.

Figure 4.2 shows a typical structure, the leftmost bay being equipped with a Process bus, attached to a Process I/O for Analogue Values (PIA) and a Process I/O for Binary Values (PIB). While it is possible to fit Station bus and Process bus into one network structure, it is prudent to separate them for various reasons, e.g. to reduce the Station bus load due to SV traffic or to avoid introducing single points of failure when coupling tightly Process bus and Station bus.

A network usually includes links with different speeds. For instance it makes sense to connect end nodes to bridges with cheaper 100 Mbit/s links and bridges among themselves (trunk links) with 1 Gbit/s links. The distance that can be covered decreases with increasing data rate since the product of bandwidth, and

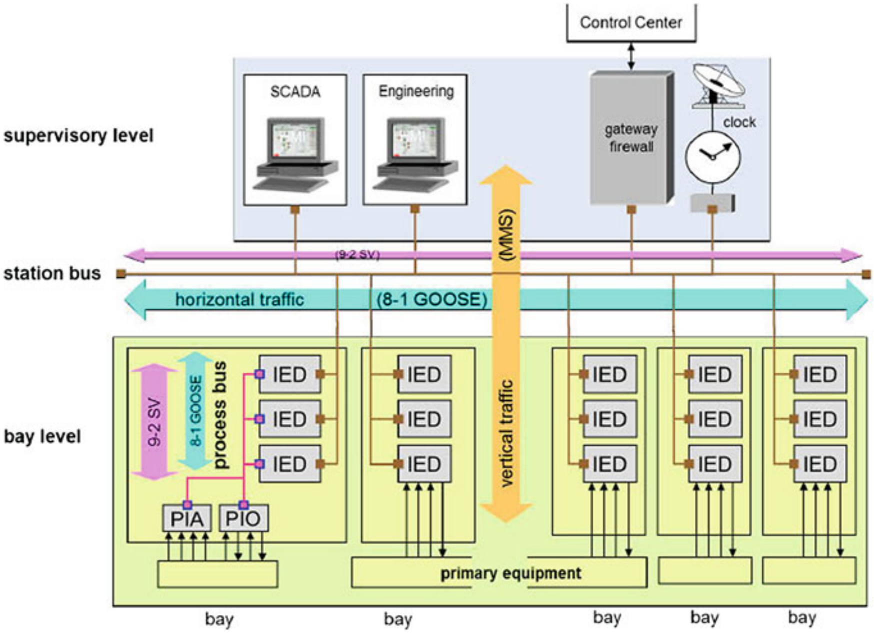


Fig. 4.2 Station bus, Process bus and traffic example (CIGRE IEC 61850-9-2:2011, Figure 9)

distance is a fundamental limit of each medium. IEC 61850 [1] considers different physical layers (copper and fibre) and can be mapped to several bit rates (in particular 100 Mbit/s, 1 Gbit/s).

4.2 Network Architecture

A network is formed with different participants, the ones injecting and retrieving data from or to the physical communication media and the ones providing different paths for data transportation using one or more physical interconnections.

Physical interconnections impose data transportation restrictions, like interconnection lost due to infinite loops. At Layer 2, there are a number of specialised protocols to control data transportation paths, dynamically disabling and enabling them according with the number of interconnections present.

The number of interconnections paths for data transmissions increases network availability for physical aspects and provides choices for media control protocols for data transportation, increasing, in theory, the availability of data transportation from one participant to another.

Physical media control protocols, at Layer 2, react on new interconnections and after a path loss. Rapid Spanning Tree Protocol (RSTP) for example calculates the new interconnections and what path should be able to transport data, in order to avoid infinite loops; in the process, data transportation is stopped until the new path is available. The time required for RSTP to re-establish the data transportation depends on the number of participants and paths present in the new network. Some applications like SCADA have mechanisms provided by Layer 4 to recover data transmission, resuming from the last unconfirmed data delivery, so this network unavailability produces no effects in operation, behaviour and low-performance impacts.

For high-performance applications like protection and control, RSTP path recovery process could impact in the behaviour and security, especially if participants are not configured using the recommendations of IEC 62439-1 [6] standard.

For these reasons, the number of participants and interconnections between them, in the network, is very important. In the following sub-sections, a number of common network architectures are discussed.

The streaming of sampled values over the substation communication network is identified as one of the most important factors to be considered in the design process. Redundant communications have been considered to improve their reliability from the early digital substation projects and are becoming a common feature of digital Protection, Automation and Control System of today. What makes a more challenging case is the combined traffic of sampled values streams for protection, monitoring and control applications (80 samples/cycle) and power quality/transient recording (256 samples/cycle) streams. The use of these sampled values streams by protection and recording applications and its impact on the design of the communications network combined with the worst-case scenario of maintenance testing of a bus differential protection needs to be analysed.

The technical report IEC 61850-90-4 TR [7]—Communication networks and systems for power utility automation—Part 4: Network engineering guidelines for substations [appendix A] is a very useful document that should be used in the design of digital PACS. It covers many aspects of the communications in digital substations, including the use of redundant communications based on PRP and HSR.

As inter-device interfaces in the substation migrate to all-digital communications, the availability and dynamic performance of the communication networks become critical. Solutions to the availability challenge are presented in the IEC 62439-3 [8] standard on: Industrial communication networks—High availability automation networks—Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR); the two solutions are described below.

Is important to analyse the current and future impacts on choosing one or other architecture, including the required protocol for high availability and performance applications, as described in Chap. 7.

4.2.1 Single Ring

In this kind of networks, LAN switches are interconnected to one port a time until the last one is connected to the first. Network capable devices, like protection relays, metres, bay controllers and other IEDs, are connected to the LAN switches using at least one port.

Devices can be connected using two redundant ports; if a failure on the active one occurs, the other takes over. Just one port is actively transmitting data at a given time. Refer Chap. 7 for a guidance on connection methods.

4.2.1.1 Rapid Spanning Tree Protocol (RSTP)

IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) is very versatile and works on virtually any configuration of networks. In order to avoid long down times, due to a network configuration change, due to a link fail or adding new LAN switches, IEC 62439-1 [6] standard establishes a method for recovery time calculation.

Experience that shows up RSTP works well on single ring network configurations, setting the ports dedicated to device connection as “EDGE” ports in order to ignore them at transmission data recovery. It is recommended for SCADA, Protection, Automation and Control System applications, if no SV or tripping transmission by GOOSE message is required.

The number of LAN switches connected in the ring pushes up recovery times, but again, this is not an issue on systems without trips or SV crossing the network.

4.2.1.2 Media Redundancy Protocol (MRP)

Media Redundancy Protocol (MRP) is defined at IEC 62439-2 standard [9]. It is specialised on single ring configurations, with a very low recovery time for a large number of LAN switches in the network. It is recommended for SCADA, Protection, Automation and Control System applications, including trips transmission using GOOSE messages, because the time delay on fails can be considered low enough.

It is desirable to take a deep analysis on this protocol's recovery performance and check if it meets requirements of the user on trip time transmission under fail conditions, considering traditional methods currently in use and the natural delays provided by intermediate devices like auxiliary relays. It is more important to consider the total time at worst case and if that will impact the power system.

In order to implement a MRP network, LAN switches connected in the ring must support the MRP.

4.2.1.3 High-availability Seamless Redundancy (HSR)

High-availability seamless redundancy (HSR) is specified in IEC 62439-3 Clause 5 (appendix A) [8] and provides seamless failover. This particular network configuration has no LAN switches, and reducing the number of participants in the network simplifies installation and lower costs. An HSR network requires all devices to support this protocol through communications ports. No other device can be connected to the network, unless a proxy one is used, to add new no-HSR devices, but they belong to the proxy device, reducing the overall reliability of the connection.

Nodes in HSR have (at least) two ports, and the nodes are daisy-chained, with each one node connected to two neighbour nodes. The last node being connected to the first node and closing the line to a physical ring structure (see Fig. 4.3). HSR uses nodes similar to PRP nodes with two network interfaces (DANH). A node must be able to forward frames from port to port at wire speed, which requires a cut-through bridge in each node and therefore a hardware implementation.

The throughput of the communication links must be determined considering the impact of the normal and testing traffic as part of the engineering of a hybrid system with a centralised disturbance recording system, which especially in the case of HSR-based implementations may require 1 Gb/s communications.

HSR is recommended for SCADA, protection and control applications, including trips transmission using GOOSE messages, because the time delay on fails can be considered low enough.

4.2.2 Two Rings

A two-ring network configuration means two parallel single rings as described above. A two ring conformed using the same LAN switches is not considered.

Both rings are independent each other, so any fail on any LAN switch or link just affects one of the rings.

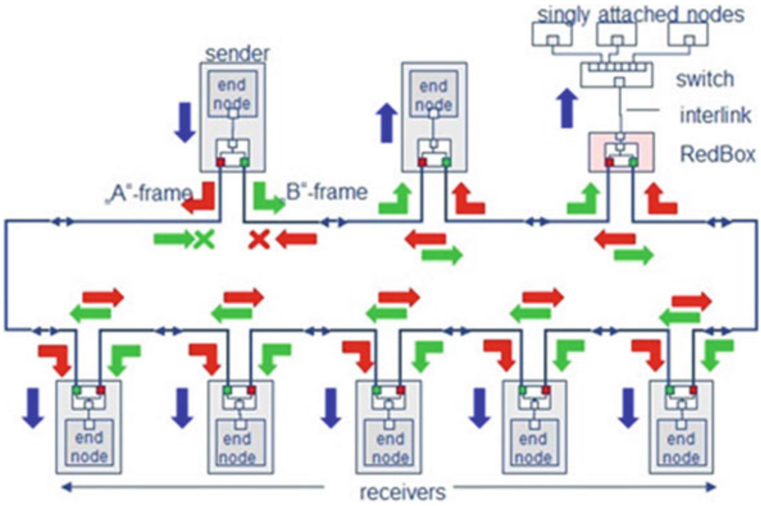


Fig. 4.3 High-availability seamless ring (HSR)

4.2.2.1 Parallel Redundancy Protocol (PRP)

Parallel Redundancy Protocol (PRP) is specified in IEC 62439-3, Clause 4 [8] as a protocol that offers seamless failover, based on complete duplication of the LAN. Both LANs operate in parallel with a source node duplicating the frames to send and the destination nodes discarding the duplicates on the base of their source and of a sequence number appended to the frame's payload. To achieve this, a PRP node is a doubly attached node (DANP) with two ports, one for each redundant LAN.

There are two independent Ethernet networks, and each directly attached device must provide two communication ports to connect to each of the independent networks. When a device sends a message, it is emitted out of both ports of the device at (almost) the same time. Each message transits each independent network. The receiving device must also have two receiving ports—allowing the receiver to receive both messages and to discard the redundant message. Clearly, failure of a component in one of the two networks allows the message to still be received without any additional delay. The architecture can be seen in Fig. 4.4. PRP provides optimal performance for device-to-device communication in the substation.

PRP is recommended for SCADA, Protection, Automation and Control System applications, including trips transmission using GOOSE messages, because the time delay is expected to be zero.

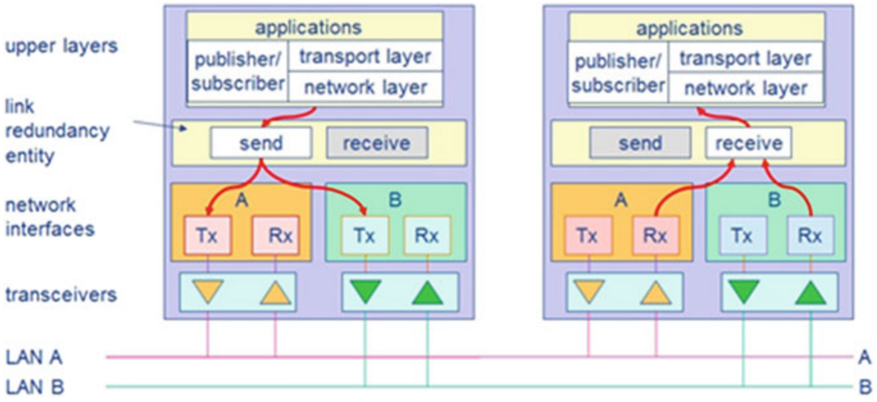


Fig. 4.4 PRP architecture

4.2.2.2 Mesh

A mesh network means multiple physical interconnections between LAN switches in the network. Devices can be connected with one or two ports. This kind of network means many paths for data transmission between participants. Two ring formed by the same LAN switches is considered a mesh network because of sharing the same issues.

At present, the most used protocol for this kind of networks is RSTP. The problem is the recovery time involved, when a LAN switch or a link fails, the high number of physical interconnections makes it impossible to deterministically calculate the total down time based on IEC 62439-1 [6], so it is not recommended to be used on IEC 61850 [1] Protection, Automation and Control System.

4.2.2.3 Software-defined Networks (SDN)

Software-defined networks (SDNs) provide a way to design the way a LAN switch should response on specific fail conditions. This is useful for mesh configuration networks, where RSTP is substituted by an engineered recovery process, designed to reduce the total down time.

SDN is recommended for SCADA, Protection, Automation and Control System applications, without trips transmission using GOOSE message, unless the design has been proven to offer a low enough down time, accordingly with the power system stability and security standards, and the calculated time is considered deterministic, in range secure for the installation and the power system. This can be archived by using a well-known design and tested LAN switches.

4.3 Services Mapped to Concrete Communication Protocols

The services defined in IEC 61850-7-2 [10] are called abstract services. Abstract means that only those aspects that are required to describe the required actions

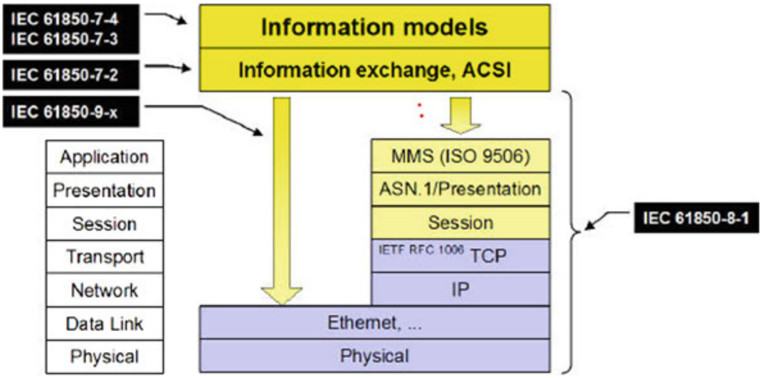


Fig. 4.5 Example of communication mapping (IEC 61850-7-1, Figure 8) [3]

on the receiving and sending side of a service request are defined in IEC 61850-7-2 [10]. They are based on the functional requirements in IEC 61850-5 [5]. The semantic of the service models with their attributes and the semantic of the services that operate on these attributes (including the parameters that are carried with the service requests and responses) are defined in IEC 61850-7-2 [10].

The specific syntax (format) and especially the encoding of the messages that carry the service parameters of a service and how these are passed through a network are defined in a specific communication service mapping (SCSM). One SCSM—IEC 61850-8-1 [11]—is the mapping of the services to MMS (ISO 9506-1 and ISO 9506-2) [12] and other provisions like TCP/IP and Ethernet (see Fig. 4.5), and another is IEC 61850-9-2 [13]—the direct mapping on Ethernet.

4.4 General Requirements for Services

IEC 61850 [1] services are independent from communication protocols and media; but in order to materialise applications, one or more protocols and specific media had to be chosen in order to provide interoperability between actors in a system.

IEC 61850 part 8-1 [11] has chosen a well-known ISO/IEC 8802-3 network [14], known as Ethernet, providing features for data transportation and delivery producing networks with several properties. Some of the aspects to study are:

1. Redundancy
2. Latency
3. Transient immunity

While ISO/IEC 8802-3 [14] is the prime media for transportation, IEC 61850 [1] is important to just consider that the standard is open to define more medias in future.

ISO/IEC 8802-3 [14] allows several ways to interconnect network participants, feature providing one or more paths for data transportation. Depending on the network interconnections, several considerations should be taken in account, because they impact to redundancy and latency. For example one of the simplest network interconnections providing redundancy and good response on network recovery time for data acquisition is a single ring using RSTP.

For details on how to select a LAN switch, refer Chap. 7.

4.4.1 Redundancy Implementation for Networks

In power utility applications, it is common to use (N-1) criteria for redundancy. It means that the system shall be tolerant to a single point of failure. This criterion is often applied selectively for the network and communication equipment. Redundancy can be subdivided into hardware redundancy and network redundancy.

Hardware redundancy is a duplication of selected devices or selected components and can be realised at the module (component) level and at the device level in these devices. Typical example for module-level redundancy is power supply redundancy. An example of equipment-level redundancy is router redundancy with Virtual Router Redundancy Protocol (VRRP).

Network redundancy is the ability of the network architecture to be resilient to failures. It is realised by redundancy protocols. Redundancy protocols implement mechanisms for fast recovery upon failures, avoiding loops and ensuring efficient and optimal data transfer through shortest communications paths. There is no “best” network topology and no “best” redundancy protocol. They all have strengths and weaknesses, and the correct choice for a given application depends on many factors.

Network redundancy protocols or network protection schemes ensure resilience to failures as redundant communications paths are available. However, redundancy protocols are characterised by failover or recovery time which is the period when the data communication is not available as the switchover to the alternative path is being performed after failure link or device has been detected.

Each utility application is characterised by its availability and maximum tolerated outage or down time. For critical Protection, Automation and Control System applications, the requirements are extreme in terms of latency and packet loss. Tripping information shall have a latency less than 4–6 ms, and no packet loss is accepted. Protection, Automation and Control System engineers are still reluctant to migrate such applications to IP or Ethernet technology. Availability requirements have direct impact on the redundancy protocol that should be used.

Redundancy means a way to provide at least two paths to accomplish data transportation, using a hot/standby or hot/hot configuration.

Hot/standby is a method where the data is transported through a path of, at least, two of them available; while other, or more, path will only be available for transportation if the path in use fails.

Hot/hot redundancy is a method where the media provides, at least, two paths for transportation, and both, or all, are effectively used to transmitting the desirable data.

The choice of the type of redundancy depends on the application and impact to system operation and monitoring locally or other systems, like electrical transmission networks.

ISO/IEC 8802-3 [14] provides a link protocol, for data transportation, using frames and headers. Headers are used to implement several types of protocols on top of Ethernet, one of them is network operation related to implement redundancy, transportation quota and priority. IEC 61850 [1] systems commonly can use several Ethernet compatible redundancy protocols in like RSTP, PRP, MRP or HSR, all of them specified at IEC 62439 standard series [15].

The protocols for redundancy can have an impact on the transportation nodes, called Ethernet switches in ISO/IEC 8802-3 [14] networks, related to allowed nodes interconnections, number of them and network latency, along a limitation on the kind of node to use, because not all support all redundancy protocols above.

The value of the protected equipment for the operation of the grid dictates the level of redundancy to be observed. A usual requirement is the avoidance of any single point of failure, which implies the introduction of redundancy. Guidance is given in Clauses 7.2 and 13.1. (IEC 61850-9 [4]).

4.4.2 Latency Implications for Networks

The communications process (CP) of the sending IED accepts the change of state of a logical variable into the data application function which next encodes a message, coordinates with the protocol stack and then egresses the digital message out the physical interface (PHY). The communications process of the receiving IED ingresses the message through the physical interface, coordinates with the protocol stack, decodes the message, and the data application creates the associated change of state of a logical variable.

Some of the individual and combined latencies include various combinations of communications devices between the IEDs such as multiplexers, switches, routers, WAN devices, fibre and radios.

Figure 4.6 illustrated several “latencies” identified as letters of the alphabet and one identified by the word “latency” (IEEE standard 1646 [16], IEEE PSRC WG H41 [17]). The component labelled “latency” included processes outside of the scope of “aspects of the act of communicating protection signals and protection signal digital messages”.

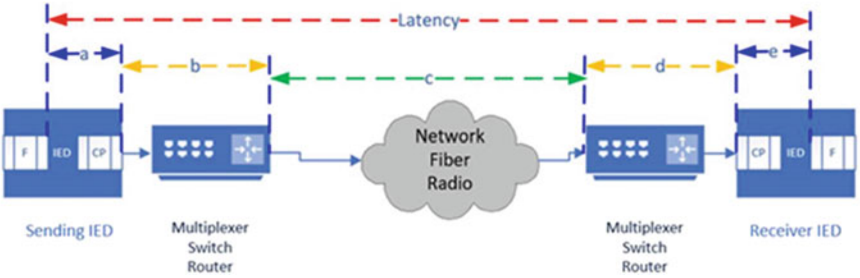


Fig. 4.6 Communications operations latency model

1. Latency emulates sender contact closure to receiver initiate action
2. “a” and “e” are the latency for sending and receiver IED communication processing (message formatting, buffer, etc.)
3. “b” and “d” are the latency for local communication equipment
4. “c” network latency over selected communication equipment and medium

Operational latency is the time delay between an input (cause) and the desired output (effect). Latency can be defined as a time delay or a duration of time. Latency measurement is a duration of time defined as the numerical difference between the timestamp of the duration start and the duration stop. Operational technologies manage, monitor and control industrial operations with a focus on the physical devices and processes they use. Operational latency is the combined time delays between an input (cause) and the desired output (effect). Operational latency can be defined as the sum of time durations or latencies of operations within a workflow. Jitter is the latency variance. Network latency is the time between the source device publishing a message onto the network and the destination device receiving the message from the network. Network jitter is the variance of the network delivery operational latency among numerous message deliveries. Round-trip time has numerous definitions. The use of this term is in general not adequate and operational process times that, or include a round-trip, require more specific definition.

Table 4.1 shows typical delay time for different functions used in an IEC 61850 PACS, e.g. protection, control and management.

Note there is not a maximum delay specified for PTP. The PTP network directly calculates and compensates for the delay over each possible path, so by definition, the protocol itself defines the fastest path between the devices.

4.4.3 Transient Immunity for Networks

Communications channels provide a limited immunity for external influences. Electric-based transmissions using wires have an intrinsic weakness to transients,

Table 4.1 Typical delay time for different functions used in an IEC 61850 PACS

Function type/Message		Interface (Table 1)	Protocol	Max Delay (ms)	Bandwith	Priority	Application
1A. Trip	GOOSE	3, 8	L2 Multicast	3	Low	High	Protection
1B Other	GOOSE	3, 8	L2 Multicast	10..100	Low	Medium High	Protection
2. Medium Speed	MMS	6	IP/TCP	<100	Low	Medium Low	Control
3. Low Speed	MMS	6	IP/TCP	<500	Low	Medium Low	Control
4. Raw Data	SV	4	L2 Multicast	4	High	High	Process Bus
5. File Transfer	MMS	6, 7	IP/TCP/FTP	>1000	Medium	Low	Management
6. Time Sync	Time Sync		IP (SNTP) L2 (PTP)		Low	Medium High	General phasors, SVs
7. Command	MMS	6	IP		Low	Medium Low	Control

especially if the environment exposes high frequency or powerful electromagnetic phenomena, such as the ones present in high-voltage installations.

While examination of electromagnetic phenomena is out of the scope of this book, it is sufficient to note that IEC 61850-3 [18] standard has a set of requirements for devices to be used in different environments.

Getting back to communications, the network media should be designed to accept external influences without affecting the transmitted data in a way that can produce misoperations or misbehaviour.

As mentioned before, the most common media for ISO/IEC 8802-3 [14] networks are wires and optical fibres.

Wire can be a set of twisted pairs, with or without shield. For Ethernet, the most common type is called UTP. In order to archive higher data transfer speeds, wires require more protection against electromagnetic interference, which can be achieved by shielding. In high-voltage installations, it is recommended to limit the length of wired communication media in order to reduce the risk of excessive affectations.

For large distances interconnection, media should provide high protection or immunity to external influences. It is recommended to use fibre optics for this application in high-voltage installations. Fibre optics is especially good to cover large distance measured in kilometres, but requires special fibre characteristics and a suitable transmitter and receiver in order to archive data transmission.

4.5 Implementation of Services Related to IEC 61850

The communication requirements for utilities (listed in IEC 61850-5 [5]) are met by the profiles shown in Fig. 4.7.

The message types and performance classes specified in IEC 61850-5 [5] are mapped as shown in Fig. 4.7:

- Type 1 (fast messages)
- Type 1A (trip)
- Type 2 (medium-speed messages)
- Type 3 (low-speed messages)
- Type 4 (raw data messages)
- Type 5 (file transfer functions)
- Type 6 (time synchronisation messages)

Messages of Type 1 and Type 1A are mapped to the same Ether type. Messages of Types 2, 3 and 5 require message-oriented services.

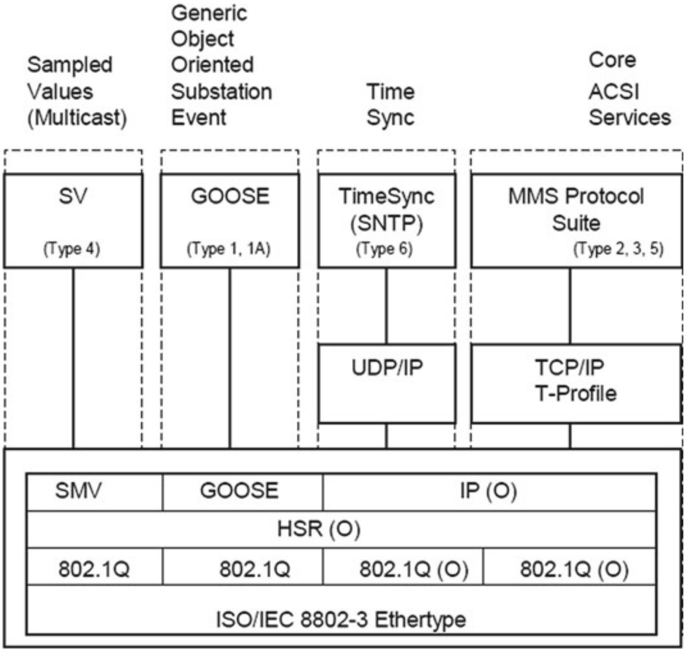


Fig. 4.7 Overview of functionality and profiles (IEC 61850-8-1, Figure 1) [5]

4.6 Available Services

Services are defined in IEC 61850 [1] in a way they can be implemented on different communication media and protocols; for this reason, they are called abstract in IEC 61850 Part 7-2 [10].

4.6.1 Services and Open Systems Interconnection

ISO/IEC 7498-1 standard [19] defines a basic open system interconnection model. The model is based on layers providing different functionalities for data transport between systems. Each layer has a specific position, and if it exists in the implementation, it works as a path for data transmission between layers. Once two systems have established communication with each other, using Layers 1, 2, 3 and 7 of the model, the data should start from the application at Layer 7, delivering it to Layer 3 allowing to transit a network, then the data is delivered to Layer 2 for media control and finally to Layer 1 for physical access to the media, in one direction; at the other end, the process for data delivering is inverted, crossing from Layer 1 to 2, then Layer 3 and finally to the application at Layer 7.

Implementing the open system interconnection model implies to select the layers to use, based on the required functionalities and data delivery performance. Functionality goes from access to different networks (Layer 3), data transportation control with connection or connection less (Layer 4), establishing a session between systems (Layer 5), data adaptation for transportation (Layer 6) and the application (Layer 7) using the communication stack implementation.

The more layers in use, the more time is required to transport data from one system to another. The implementation should consider this in order to select the required functionalities without performance penalty.

IEC 61850 [1] services are required to provide session, transport control, network, media control and physical media access for SCADA applications in order to provide security and data consistency, but low requirements on performance compared with other applications services.

High-performance applications, like protection and control and IEC 61850 [1] application services, require access directly to the media control (Layer 2) and physical media (Layer 1), removing functionalities like access to networks outside the local one.

4.6.2 SCADA-related Services

IEC 61850-7-2 [10] defines a set of services and its behaviour related to SCADA. There is a model for two-party application association, to implement a client–server approach, for both confirmed and unconfirmed data transfers. Servers providing this service require association requests from clients in order to transmit data. A release association service is also provided. The MMS protocol represents an implementation of these services. Its features are described below.

4.6.2.1 Manufacturing Message Specification—MMS

MMS traffic defined in IEC 61850-8.1 [11] allows an MMS client such as the SCADA, an OPC server or a gateway, to access all IED objects on the same level. MMS is based on IP (layer 3).

This traffic can flow both on the Station bus and on the Process bus. Not all Process bus IEDs are required to support MMS (IEC 61850-9 [4]).

The MMS protocol is a client–server protocol operating at the network layer (Layer 3). Therefore, it operates with IP addresses and can cross routers. In one operating mode, the client (generally the SCADA or gateway) sends a request for a specific data item to an IED that has an MMS server, identified by its IP address. The server responds with the requested data in a response message to the IP address of the client. In another mode, the client can instruct the server to send a response spontaneously upon occurrence of an event (Fig. 4.8).

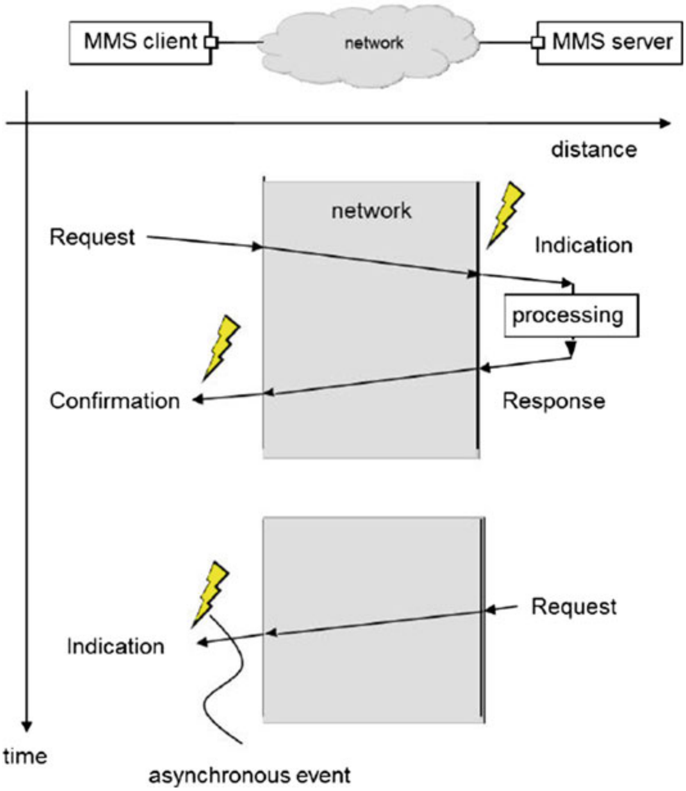


Fig. 4.8 MMS protocol

To ensure that no event is lost, MMS relies on the TCP for error detection and recovery. An MMS server can support a number of clients simultaneously, but each client is treated individually Fig. 4.8.

4.6.3 Protection and Control Services

IEC 61850 [1] provides a set of services to perform high-speed data interchange between devices related to protection and control schemes.

For protection and control-related services, IEC 61850 defines basically two protocols:

- Part 8-1: Generic Object-Oriented System Event—GOOSE [11]
- Part 9-2: Sampled Values—SV [13].

GOOSE and SV are specialist protocols for the operation of the protection system.

Protection applications require low-latency high-speed data transport and no confirmation, when a communication protocol is in use like GOOSE. Trip signals will be transported to devices performing the actual trip on circuit breakers.

Control applications can require signals to secure operations, e.g. interlocking associated to open and close requests of circuit breakers and disconnectors. Signals for control applications should be transported at high speed, but require less priority than the protection ones. Also, control applications need to send commands to devices interfacing primary equipment disconnecting devices. It is important to distinguish between control commands sent as part of SCADA and the ones related to interlocking. The former requires less priority in network communications transportation, confirmation, and they have a large stack to traverse in order to provide other features like security, data integrity and network traverse capability.

For this kind of services, IEC 61850-7-2 [10] provides a multicast application association model. Data is sent to the network by the server and received by clients, in this case known as subscriber. GOOSE protocol is the choice in IEC 61850 [1], providing multicast and high-speed transmission and fast reception processing by server (publisher) and client (subscriber).

4.6.3.1 Generic Object-Oriented Station Event (GOOSE)

GOOSE traffic defined in IEC 61850-8.1 [11] allows IEDs to exchange data “horizontally” between the bays or “vertically” between process level and bay level, especially for the status signals and tripping signals and sometimes for interlocking and measurement. This traffic flows normally over the Station bus or the Process bus (IEC 61850-9 [4]).

GOOSE messages are exchanged at Layer 2 (link layer), taking advantage of the multicast functionality provided by Ethernet. The GOOSE communication consists of an event-driven transmission and of a relatively slow cyclic part.

Upon occurrence of a preconfigured event condition, an IED sends a GOOSE message carrying the variable values to be communicated for that event. Since they are multicast, GOOSE messages are not acknowledged by the destination. To overcome transient errors, the same GOOSE message is retransmitted several times in a row, at interval T1, then T2, then T3 (application specific). To assess the presence of the source, GOOSE messages are retransmitted at low rate T0 as Fig. 4.9 shows. Since GOOSE messages operate at Layer 2, they do not leave the LAN and cannot cross routers.

GOOSE operates on the publisher/subscriber principle. The new value received is supposed to replace the former value, as opposed to being queued if the old value could not be processed in time. However, overwriting is not prescribed, so queuing is also used.

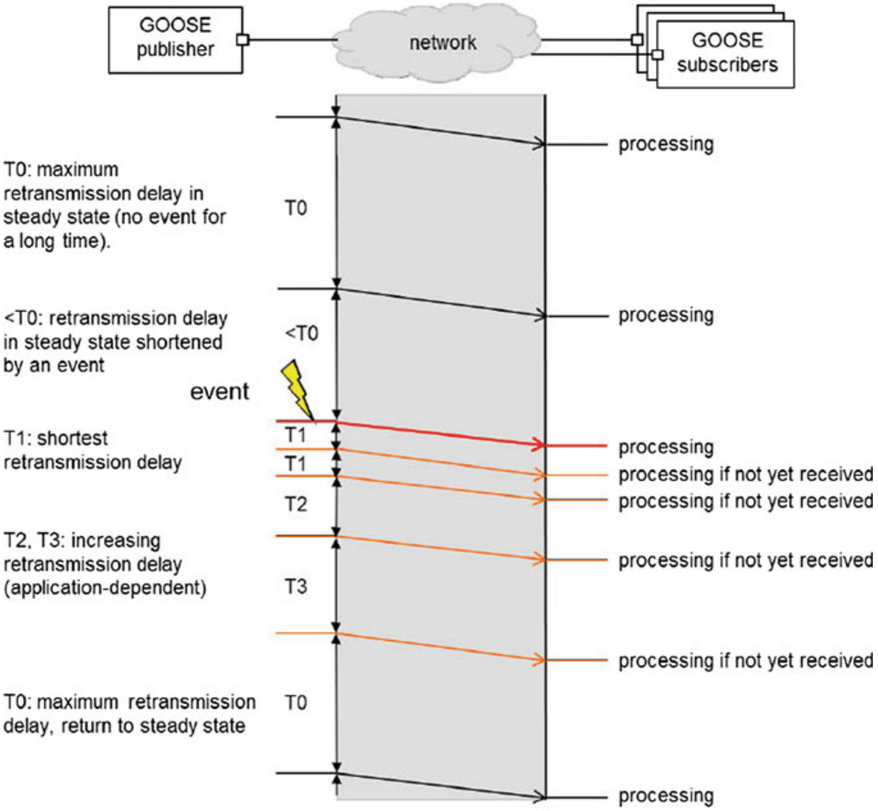

GOOSE publisher
network
GOOSE subscribers
processing
T0: maximum retransmission delay in steady state (no event for a long time).
T0
processing
<T0: retransmission delay in steady state shortened by an event
<T0
event
T1: shortest retransmission delay
T1
T1
T2
processing
processing if not yet received
processing if not yet received
T2, T3: increasing retransmission delay (application-dependent)
T3
processing if not yet received
processing if not yet received
T0: maximum retransmission delay, return to steady state
T0
processing

Fig. 4.9 GOOSE protocol

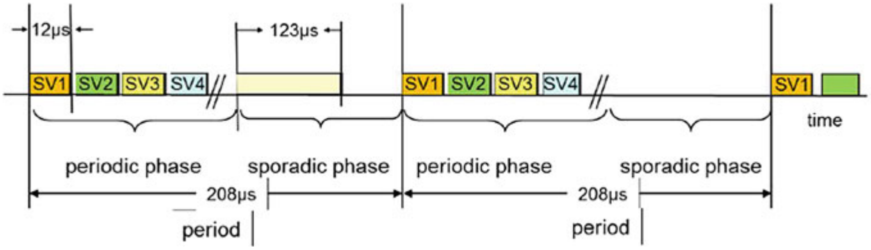


Fig. 4.10 Example of SV traffic (4800 samples per second)

4.6.3.2 Sample Value (SV)

SV traffic defined in IEC 61850-9-2 [13] carries voltage and current samples. This traffic flows normally on the Process bus but can also flow over the Station bus for instance for busbar protection and phasors (IEC 61850-9 [4]).

The sampled values protocol (specified in IEC 61850-9-2 [13]) is mainly used to transmit analogue values (current and voltage) from the sensors to the IEDs. The SV protocol, like GOOSE, uses Layer 2 multicast, and messages are identified by their MAC addresses and an identifier in the message body. Like for GOOSE, there is no retransmission protocol: a lost sample is overwritten by the next successful one. The SV messages, unlike GOOSE, are transmitted purely cyclically and with a small period. The UCA 61859-9-2LE implementation guide [20] prescribes a period of 250 µs in a 50 Hz grid, respectively, and 208.3 µs in a 60 Hz grid. Therefore, the SV messages are kept small. With a typical size of 160 octets, an SV message takes some 12 µs at 100 Mbit/s, and time in the period should accommodate a maximum size FTP message of 123 µs at 100 Mbit/s, thus limiting the number of attached SV senders on a bus. To avoid spurious jamming, all SV sources on the same bus should operate at the same period and preferably implement a time division multiplex scheme such as Fig. 4.10 shows. IEC 61869-9 [21] defining the profile for MU is published and provides backward compatibility with the UCA 61859-9-2LE profile [20].

4.6.3.3 Time Synchronisation Services

Time synchronisation is a service required for specific applications, like event sequence analysis, metering for energy commercialisation and samples alignment. Please see further description in Chap. 5.

Neither MMS nor GOOSE specifically relies on synchronised year/month/day/hour/minute/second timestamp across the network in order to work. In the same way as old electro-mechanical relays had no concept of time, protection systems will operate correctly even if devices are operating with a different year time reference. However, for some SV applications, each merging unit (the publisher of the SV message) must have accurate synchronisation coherency of the start of each one-second window; however, the year/month/day/hour/minute is essentially irrelevant. In small networks, IRIG-B/1 pulse per second may achieve close to one microsecond coherency. However, and in practice, SV really needs time synchronisation via IEEE 1588 PTP (v2) with specific substation profile defined in IEC 61850-9-3 [22]. This also means that the network switches must also be chosen as IEEE 1588 transparent clock capability; i.e. older networks pre-2010 may need to have old switches replaced, but certainly, it would be wise to procure any new switches with this capability to avoid replacement in future.

4.7 Example of Communication Network

In Chap. 12, some examples which use HSR architectures and PRP architecture for Process bus-based Protection, Automation and Control System are presented.

4.7.1 Communication Networks for Protection, Automation and Control System (PACS) with Process Bus [23]

The design of the communication networks in Protection, Automation and Control System (PACS) with Process bus based on the IEC 61850 [1] peer-to-peer and client–server services has to be taken into account several factors, such as:

- Functionality of the substation Protection, Automation and Control System
- Importance of the substation as a component of the electric power grid
- Sampling rates and protocol used for the sampled values
- Requirements for fault clearing times
- Protection, automation and control philosophy
- Communication system architecture can be
  - Distributed
  - Centralised
  - Hybrid

Today, most of the Protection, Automation and Control System with Process bus has a hybrid architecture, meaning that the Protection, Automation and Control System at the bay level is performed by multifunctional intelligent electronic devices (IEDs) communicating with the process interface devices, while some of the functions (interlocking, disturbance and event recording) are centralised.

Figure 4.11 shows a simplified block diagram of a Protection, Automation and Control System with Process bus with hybrid system architecture. The PACS functions are distributed between the IEDs, and some can even be implemented locally in the process interface units (PIUs). The disturbance recording is implemented in a centralised recorder connected to the Process bus.

We should not forget that the station and Process buses are not necessarily physical components and can be implemented on the same Ethernet network.

Communication of the sampled values was initially based on the UCAIug guideline document known as “IEC 61850-9-2 LE” [24] in order to provide some guidance to the vendors on the "appropriate" parameters for interoperability. However in 2016, IEC 61869-9 [21]: Instrument Transformers—Part 9: Digital interface for instrument transformers was published as International Standard describing the profile for SV interface, effectively replacing UCAIug "LE" guide but also introducing various changes to the parameters, e.g. samples per second instead of samples per cycle.

UCAIug "IEC 61850-9-2 LE" [24] defines for protection and control applications a sampling rate of 80 samples/cycle at the nominal system frequency. The digital output publishing rate is 4000 frames per second at 50 Hz and 4800 frames/sec at 60 Hz with one application service data unit (ASDU) per frame. For power quality monitoring and disturbance recording, the sampling rate is 256 samples/cycle at the nominal system frequency with 8 ASDUs per frame.

The IEC 61869–9 [21] standard defines requirements for digital communications of instrument transformer measurements. It is based on the IEC 61850 series [1], UCA international users group document implementation guideline for digital interface to instrument transformers using IEC 61850-9-2 [25] and the relevant parts of IEC 60044-8 [26] that are replaced by this standard. It includes additional improvements including the IEC 61588 [27] network-based time synchronisation. It defines two preferred sampling rates:

- 4800 Hz for general measuring and protection applications, regardless of the power system frequency
- 14,400 Hz for power quality and metering applications, regardless of the power system frequency

In both cases, the digital output publishing rate is 2400 frames per second with the number of application service data unit (ASDU) in the first case being 2 and in the second 6 per frame.

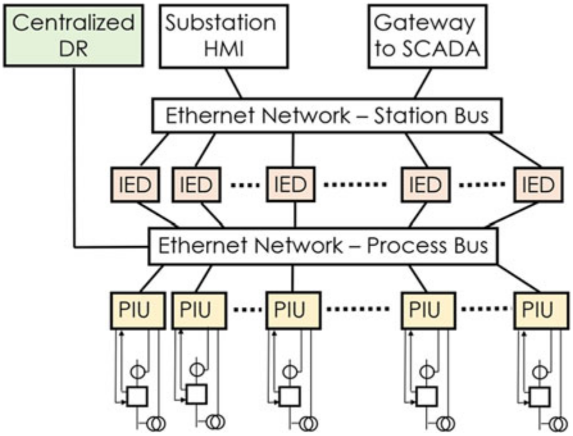


Fig. 4.11 Simplified block diagram of Protection, Automation and Control System (PACS) with Process bus with hybrid architecture

As a result of the transition to IEC 6186-9 [21], the traffic on the communications network will be reduced in half, but the size of the frames will increase. This needs to be taken into consideration in the design of the communications architecture.

The use of centralised disturbance recording means that streams of sampled values from all merging units or process interface units in the substation need to reach the central disturbance recorder. This will require careful analysis, especially for the use of ring topology and the impact of the additional traffic published by the test system during maintenance testing.

Considering the criticality of the operation of protection and control functions based on sampled values and Generic Object-Oriented Substation Event (GOOSE) messages, it is clear that the design of the communications network may have a significant impact on the performance of the system. Some of the criteria are related to reducing the latency of messages, while others have to do with the impact of failure of communication network components on protection and control.

4.7.2 Future Protection, Automation and Control System Communication Architectures [28]

There is ongoing work in the industry to define and evaluate the concept of protection and control of the whole substation as integrated in a limited number of devices (CIGRE Brochure 629, Coordination of Protection and Automation for Future Networks [28]). Those devices would have similar functionality and are redundant. There are already some installations in service based on this concept.

The idea of the architecture is to leave the bay-level system IED's out and this way to minimise the number of IED's. In station level, there are two or more central computer units which contain all protection and control functions. Station-level computers have Ethernet connections networked to current, voltage and binary interface modules. These modules are located in the switchgears, next to instrument transformers and switching devices or even in the control house (when optical sensors are used). The advantages of this solution are less hardware and wiring costs, less maintenance and testing objects and flexible functionality at the station level. Reliability and maintenance issues will have to be addressed; however, other industries (like aeronautics) have already developed solutions which can be considered.

The industry will define requirements for the architecture of the future PACS system. It is too early to say whether one single architecture or several different architectures will emerge. Possible future PACS architectures are shown in Figs. 4.12 and 4.13.

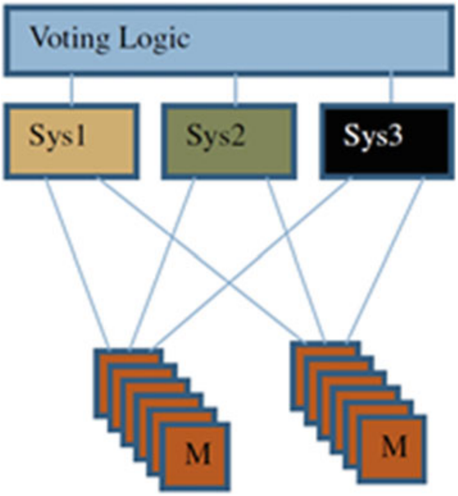


Fig. 4.12 Possible PACS architecture based on independent PACS subsystems with voting logic

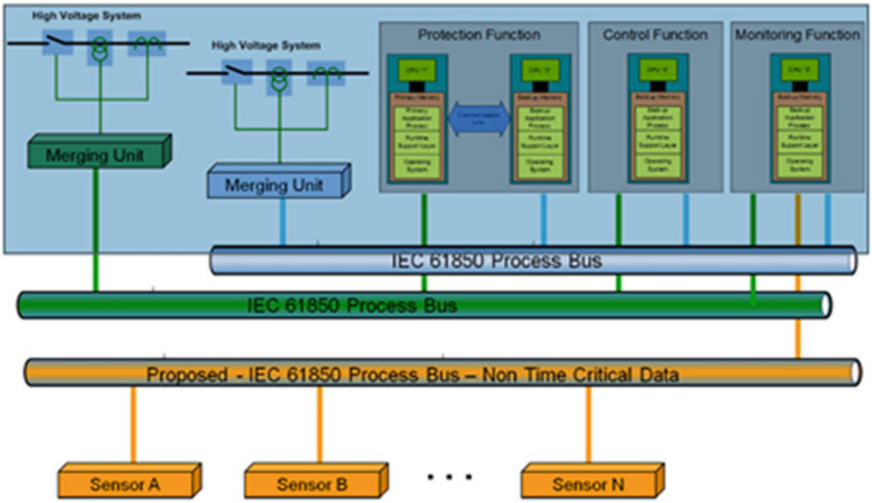


Fig. 4.13 Possible PACS architecture based on redundant Process bus and a third Process bus for non-critical data

4.7.2.1 Decentralised Protection, Automation and Control Systems

Protection, Automation and Control Systems with Process bus can provide solutions to the new power system functional requirements concerning protection, grid operation, power quality and enhanced equipment monitoring.

The dispatching and control functionalities offered by the digital technology will have to be significantly increased in order to integrate distributed energy resources (DER), which are highly intermittent into the system as well as to support operations of transmission and distribution grids.

A possible solution to the above-mentioned issues could come from a decentralised approach to network control, in normal and emergency conditions.

For example innovative applications for a decentralised active and reactive power control in a portion of the HV network are being developed. These applications include the voltage control, management of the power flows and the islanding operations.

4.7.2.2 Communication Interface with Customers

It is expected that in future, networks load will be used as a dispatchable energy resource. To that end, communication into the homes and industrial sites will be required. Media options for these interfaces include:

- Fibre—exists in many markets around the world for in-home Internet, TV, phone and security. Future trend is to advantage this infrastructure. Drawback is lack of control by the utility and subsequently, adoption issues.
- Utility-owned "private" cell technology—could be bridged to commercial cell system during emergencies or failures.
- Commercial cell technology—low-cost interfaces can be developed and can provide complete bidirectional communications. Drawbacks include cost of usage, coverage area, lack of multicast and performance.
- Utility-owned infrastructure—this option is being facilitated by the national allocation of utility-dedicated spectrum (e.g.—Canada) as well as new implementations in existing non-licenced spectrums (e.g.—900 MHz ISM band in the US). Coverage is implemented as desired, performance augmented, and multicast is enabled. Drawback is the installation costs.

References

1. IEC 61850 Communication networks and systems for power utility automation, full standard, https://webstore.iec.ch/publication
2. IEC 61850-2:2019 Communication networks and systems for power utility automation-Part 2: Glossary, IEC TS 61850–2:2019, "Copyright © 2011 IEC Geneva, Switzerland. www.iec.ch" | IEC Webstore
3. IEC 61850-7-1:2011 Communication networks and systems for power utility automation-Part 7-1: Basic communication structure—prinsiples and models, IEC 61850-7-1:2011+AMD1:2020 CSV, "Copyright © 2011 IEC Geneva, Switzerland. www.iec.ch" | IEC Webstore
4. IEC 61850-9: 2011 Communication networks and systems for power utility automation-IEC 61850:2022 SER, "Copyright © 2011 IEC Geneva, Switzerland. www.iec.ch" | IEC Webstore | LVDC
5. IEC 61850-5: 2013 Communication networks and systems for power utility automation—Part 5: Communication requirements for functions and device models, IEC 61850-5:2013, "Copyright © 2013 IEC Geneva, Switzerland. www.iec.ch" | IEC Webstore | LVDC

6. IEC 62439-1: 2010 Industrial communication network—high availability automation networks—Part 1: General consepts and calculation methods, IEC 62439–1:2010+AMD1:2012+AMD2:2016 CSV, "Copyright © 2010 IEC Geneva, Switzerland. www.iec.ch" | IEC Webstore | smart manufacturing, industrie 4.0, industry 4.0
7. IEC 61850-90-4 T: 2020 Communication networks and systems for power utility automation, Part 90-4: Network engineering guidelines, IEC TR 61850–90–4:2020, "Copyright © 2020 IEC Geneva, Switzerland. www.iec.ch" | IEC Webstore
8. IEC 62439-3: 2021 Industrial communication network—High availability automation networks—Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR), IEC 62439-3:2021, "Copyright © 2021 IEC Geneva, Switzerland. www.iec.ch" | IEC Webstore
9. IEC 62439-2: 2021 Industrial communication network—High availability automation networks—Part 2: Media Redundancy Protocol (MRP), IEC 62439–2:2021, "Copyright © 2011 IEC Geneva, Switzerland. www.iec.ch", "Copyright © 2021 IEC Geneva, Switzerland. www.iec.ch" | IEC Webstore
10. IEC 61850-7-2: 2010 Communication networks and systems for power utility automation, Part 7-2: Basic information and communication structure - Abstract structure—Abstract communication service interface (ACSI), IEC 61850–7–2:2010, "Copyright © 2010 IEC Geneva, Switzerland. www.iec.ch" | IEC Webstore | LVDC
11. IEC 61850-8-1: 2011 Communication networks and systems for power utility automation, Part 8-1: Specific communication service mapping (SCSM)—Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3, IEC 61850-8-1:2011+AMD1:2020 CSV, "Copyright © 2021 IEC Geneva, Switzerland. www.iec.ch" | IEC Webstore | LVDC
12. ISO 9506-1: 2003 Industrial automation system—Manufacturing Message Spesification—Part 1 Service definition, ISO—ISO 9506-1:2003—Industrial automation systems—Manufacturing Message Specification—Part 1: Service definition and ISO 9506-2: 2003 Industrial automation system—Manufacturing Message Spesification—Part 2: Protocol Spesification, ISO—ISO 9506-2:2003—Industrial automation systems—Manufacturing Message Specification—Part 2: Protocol specification
13. IEC 61850-9-2: 2011 Communication networks and systems for power utility automation—Part 9-2: Specific communication sercie mapping (SCSM)—Sampled values over ISO/IEC 8802-3, IEC 61850-9-2:2011+AMD1:2020 CSV, "Copyright © 2021 IEC Geneva, Switzerland. www.iec.ch" | IEC Webstore | cyber security, smart city, LVDC
14. ISO/IEC 8802-3: 2014, Withdrawn, Standard for Ethernet, ISO/IEC/IEEE 8802-3:2014 | IEC Webstore
15. IEC 62439: 2010 full standard, Industrial communication network—High avaikability automation networks, IEC 62439-1:2010+AMD1:2012+AMD2:2016 CSV | IEC Webstore | smart manufacturing, industrie 4.0, industry 4.0, e-cigre > Publication > Test Systems Consideration in the Design of Communications Networks for Digital Substations
16. IEEE 1646: 2004—IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation, IEEE 1646-2004—IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation
17. IEEE PSRC WG H41 Revision of IEEE 1646 Communication Delivery Time Performance Requirements, Relaying Communications Subcommittee—IEEE PSRC (pes-psrc.org)
18. IEC 61850-3: 2013 Communication networks and systems for power utility automation-Part 3 General requirements, IEC 61850–3:2013, "Copyright © 2021 IEC Geneva, Switzerland. www.iec.ch" | IEC Webstore | LVDC
19. ISO/IEC 7498-1: 1994 Information technology- Open System Interconnection- Basic Reference Moddel: The Basic Model, ISO/IEC 7498–1:1994 | IEC Webstore
20. UCA 61859-9-2LE implementation guide, Home—UCAIug
21. IEC 61869-9: 2016 Instrument transformers—Part 9: Digital interface for instrument transformers, IEC 61869-9:2016 | IEC Webstore | LVDC

22. IEC 61850-9-3: 2016 Communication networks and systems for power utility automation, Part 9-3: Precision time protocol profile for power utility automation, IEC/IEEE 61850-9-3:2016 | IEC Webstore | LVDC
23. CIGRE session 2020, paper B5-205, Test system considerations in the Design of Communications Network for Digital Substations, e-cigre > Publication > Test Systems Consideration in the Design of Communications Networks for Digital Substations
24. IEC 61850-9-2 LE: 2011 Communication networks and systems for power utility automation, Part 9-2 Spesific communication service mapping (SCSM)—Sample values over ISO/IEC 8802-3, IEC 61850-9-2:2011+AMD1:2020 CSV, "Copyright © 2011 IEC Geneva, Switzerland. www.iec.ch" | IEC Webstore | cyber security, smart city, LVDC
25. IEC 61850-9-2: 2011 Communication networks and systems for power utility automation, Part 9-2 Spesific communication service mapping (SCSM)—Sample values over ISO/IEC 8802-3, IEC 61850-9-2:2011+AMD1:2020 CSV, "Copyright © 2011 IEC Geneva, Switzerland. www.iec.ch" | IEC Webstore | cyber security, smart city, LVDC
26. IEC 60044-8: 2002 Instrument transformers—Part 8 Electronic current transformers, IEC 60044-8:2002 | IEC Webstore
27. IEC 61588: 2021 Precision Clock Synchronisation Protocol for Networked Measurement and Control Systems, IEC 61588:2021 | IEC Webstore
28. CIGRE Technical brochure 629, Coordination of Protection and Automation for Future Network, 2015, e-cigre > Publication > Coordination of Protection and Automation for Future Networks

5 Time Synchronisation for IEC 61850 Systems

Richard Hunt, Calum Dalmeny, and Marcel Geor

Abstract

This chapter defines the time synchronisation requirements for IEC 61850 systems. This includes accuracy requirements for different applications and classes of data, the uses of time in the IEC 61850 model, and indicating the accuracy of time synchronisation. The chapter also discusses the commonly available global primary reference sources used for time synchronisation, the use of IEC 61588 Precision Time Protocol (PTP) as the preferred time synchronisation as the preferred methods, legacy time synchronisation methods that may be used in limited circumstances, and the considerations for successfully applying PTP over the network architectures described in Chap. 4. The chapter also covers time synchronisation redundancy to ensure that IEC 61850 systems remain available, some case studies showing practical implementations of time synchronisation in operating substations, and discusses performance testing of time synchronisation systems.

Keywords

Time synchronisation • PTP • IEC 61850

The design of any substation automation system needs to incorporate appropriate time synchronisation for either or both of:

R. Hunt (✉)
Quanta Technology, Raleigh, NC, USA
e-mail: RHunt@quanta-technology.com

C. Dalmeny
Chronos Technology, Lydbrook, UK
e-mail: calum.Dalmeny@chronos.uk

M. Geor
Microchip Technology Inc., Lower Hutt, New Zealand
e-mail: Marcel.Geor@microchip.com

P. Bishop and N.-K. C. Nair (eds.), *IEC 61850 Principles and Applications to Electric Power Systems*, CIGRE Green Books, https://doi.org/10.1007/978-3-031-24567-1_5

- Fault and incident analysis
- Correct automation system operation

When we consider wire-based systems prior to the advent of communication systems, protection devices had no “understanding” of time as they were electromechanical or electronic devices with no time reference—the “synchronisation” was simply because of the analogue quantities the devices were presented with from the primary power system. In other words, the protection system could operate perfectly with no time synchronisation signal presented to the device.

However, at the SCADA level, time stamping of events became critical in order to provide a reasonably accurate Sequence Of Events (SOE) log mostly used in the event analysis of what happened in what order. This forensic activity has allowed the cause of events to be more accurately determined, and even the performance of equipment and devices to be assessed for maintenance purposes. As the SCADA system received the event signal as wire-based contact inputs to the Remote Terminal Unit (RTU) or Bay Control Unit (BCU), the time stamp was assigned by those devices, not the protection device itself. This time synchronisation needed to achieve two factors:

1. accuracy to actual time, i.e. every device knows the same time as Year/Month/Day/Hour/Minute/Second/Millisecond
2. resolution of time stamps to be initially 10 ms in the 1980’s, and then down to 1 ms resolution as commonly required today.

The advent of communication facilities to relays in the mid-1980s provided the opportunity for the relays to time stamp the events “at source” with the same two factors of accuracy and resolution which was generally achieved by the use of the IRIG-B signal of actual time or at least one pulse per second signal to maintain the relay’s internal clock accuracy.

With the implementation of IEC 61850 systems, even today some systems just use MMS and/or GOOSE implementation. In such applications, the two-factor requirement stated above for time synchronisation has not changed.

- Sequence of events generally only need one millisecond resolution for event time stamps reported in MMS messages
- Protection functions have no reliance on “knowing” the actual time in order to operate correctly.

As such “conventional” time synchronisation methods (IRIG-B/1PPS, NTP, SNTP) have been totally acceptable.

However, IEC 61850 introduced a third communications based function—the measurement of analogue quantities which are distributed on the LAN/WAN as IEC 61850-9-2 [1] Sampled Values. There are some 22 analogue quantities defined in IEC 61850-7-4 [2] which may be distributed as Sampled Values. Some of those signals may be “in-frequent” as say once per day samples, while others such as current and voltage sensors may need to report the instantaneous value at 4800 samples per second or higher.

The nature of protection devices may vary from just using a single Sampled Value (SV) stream as say the current on a particular feeder to requiring two or more different SV sources such as a voltage and current, or multiple currents.

If there is only one SV stream required for the device, e.g. a simple overcurrent protection device, the protection function needs no higher level of time synchronisation as it is only required for protection event analysis.

However, if the device requires two or more SV streams for any function, more stringent time synchronisation is required so that the source merging units are synchronised to within one microsecond between each other. A device may require two or more SV streams for the purpose of just providing power-type measurements using one voltage and one current, impedance or power-type protection such as distance or reverse power, or perhaps differential functions with two or more currents for transformers, busbars, lines or even motors. Coherency is a more stringent requirement than just resolution—it relates to all devices knowing the exact same time at the microsecond level so that each one-second window starts at precisely the same instant within one microsecond of each other. This chapter therefore discusses the requirement for time synchronisation particularly related to systems which have implemented analogue quantity measurements.

5.1 Timing Requirements

In an IEC 61850-based substation, a specific protection and control application likely requires the use of electric power system parameters measured in different physical locations. These measured parameters must be time synchronised to a common time reference with sufficient accuracy to ensure correct performance of the application. It is clear that every application in the substation, not just PAC applications, needs some level of time synchronisation, including telecommunications, revenue metering, synchrophasor applications, and travelling wave applications. All have specific requirements for the precision of measurement are shown in Table 5.1. All these applications also have specific requirements for the availability and reliability of time synchronisation [3].

IEC 61850-based substations may use the timing signals from a global navigation satellite system (GNSS) to synchronise local time servers or clocks. The time synchronisation system must be reliable in all operating scenarios, making time synchronisation part of the PAC engineering process. Many issues must be addressed such as the selection of GNSS system including satellite availability, redundancy of time servers, the definition of minimum holdover times, the desired accuracy, the security of the signal, and maintenance.

Table 5.1 Principal substation services

Service	Description	Precision
SCADA	Supervision, control and data acquisition	1 ms
Control bays	Remote terminal units (RTUs) and distributed bay control units	1 ms
Digital relays	Protection relays	1 ms
Energy billing	Revenue meters	1 s
Operational measurement	Multimeters	1 s
Merging units	Standalone merging units (SAMUs)	1 μs
Synchrophasor	Phasor measurement units (PMUs)	1 μs
Fault analysis	Digital fault recorders	1 ms
Fault localisation	Travelling wave fault location (TWFL)	100 ns

5.1.1 Time-Related Requirements in IEC 61850

Measured parameters in IEC 61850 are shared as data objects. One of the mandatory data attributes of data objects is the attribute ***t***, time. This attribute ***t*** is the time tagging or age of the related data and will reflect the most recent event associated with the data object. Time tagging is therefore associated with the publisher of the data. Refer Fig. 5.1.

Subscribers to data must be able to process these time tags correctly. This means IEC 61850 sets some common time-related requirements for data [4]:

- Accuracy—depending on the application, different time accuracy is required.
- The time stamp shall be based on an existing time standard.
- The time model shall be able to track leap seconds and provide enough information to allow the user to perform delta time calculation for events crossing the leap second boundary.
- The time stamp model shall contain sufficient information that would allow the client to compute a date and time without additional information such as the number of leap seconds from the beginning of time.
- The time stamp shall be easily derived from commercially available time sources.
- The overall time model shall include information to allow computation of local time.
- The time model shall allow for ½ hour offsets for local time.
- The time model shall indicate whether daylight savings is in effect or not.
- The format shall last at least 100 years.
- The time stamp format shall be compact and easily machine manipulated.

These basic time requirements are system requirements, but the devices that comprise the system should support these requirements.

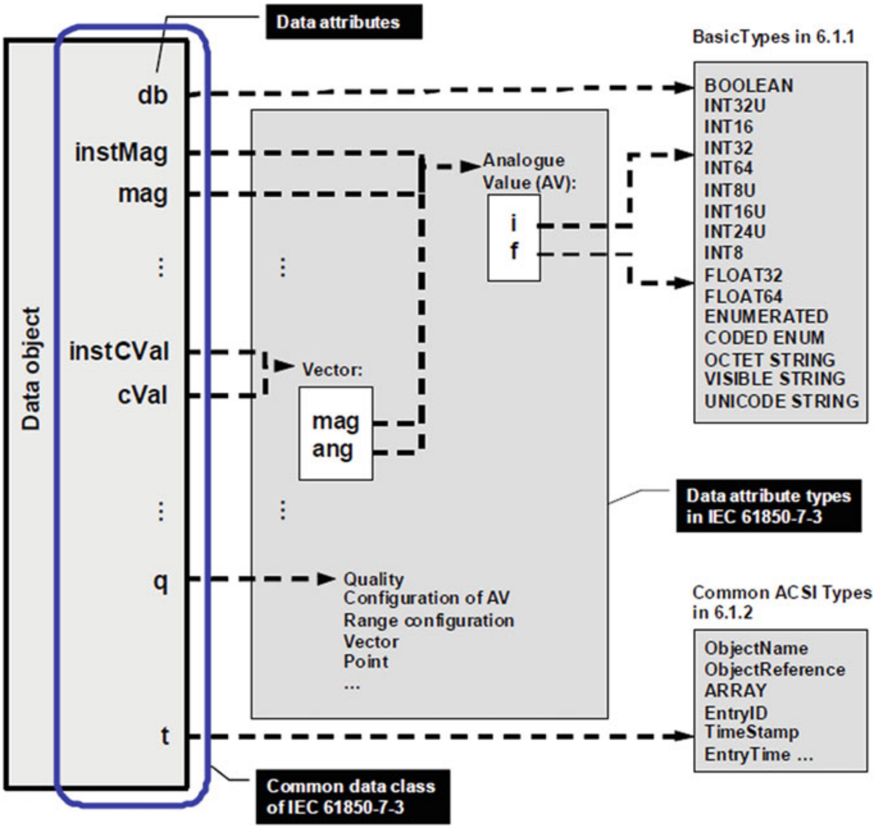


Fig. 5.1 Time as a data attribute (*Source* IEC 61850-7-2 Fig. 18)

Time tagging of data is based on the event time: the time the data last changed state. IEC 61850-5 defines how to determine the time tagging for three general events:

- If an event is defined as result of computation (internal or calculated event) allocation of time (time tagging) shall be done immediately within the time resolution of the clock. No special measures are needed.
- If an event is defined as change of a binary input, the delay of the debouncing procedure of the input contact has to be considered. The event time shall be locally corrected.
- If an event is defined as change of an analogue input, the delay of the filtering procedure of the input circuit has to be considered. The event time shall be locally corrected.

This strong event time definition ensures that the processing of the time stamp becomes independent from the communications system latency and does not require correction by the receiving function.

5.1.2 Time in the IEC 61850 Model

As stated, time tagging is managed through the time ***t*** data attribute in each published data object, the basic attribute of time tagging. This ***t*** data attribute is mandatory in all data objects. Beyond this, IEC 61850 also includes some other time-related data attributes and data classes.

The<<TimeStamp>>type represents a UTC time with the epoch of midnight (00:00:00) of 1970-01-01 specified.

Another time-related attribute in the model is <<FractionOfSecond>> representing the fraction of the current second when the value of the<<TimeStamp>>has been determined.

The<<TimeQuality>>is an attribute in the object models that provides information about the time source of the sending device and includes information about:

- <<LeapSecondsKnown>>
- <<ClockFailure>>
- <<ClockNotSynchronised>>
- <<TimeAccuracy>>

The information in the <<TimeQuality>> attribute is used by the receiving device to determine the suitability of using the data contained in the message in associated applications.

5.1.3 Time Synchronisation Concept

Devices in a substation must be synchronised to a common time standard. The general concept of time synchronisation and accuracy is shown in the simple block diagram of Fig. 5.2.

The common time standard is the external Global Primary Reference: one of the GNSS systems available that use a defined existing standard to provide the

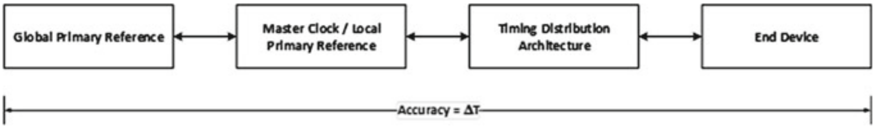

Global Primary Reference
Master Clock / Local Primary Reference
Timing Distribution Architecture
End Device
Accuracy = ΔT

Fig. 5.2 Time synchronisation block diagram

time reference. The master clock/local primary reference is a clock or time server located in the substation, normally synchronised to the Global Primary Reference. The clocks in end devices are synchronised to the master clock through the timing distribution architecture in the substation, which may be through an analogue or digital communications network. The accuracy of time synchronisation is defined as the difference in time between the global primary reference and the end device.

5.1.4 Time Synchronisation Accuracy Classes

Different functions and applications in the substation have different requirements for the accuracy of time synchronisation. IEC 61850-5 defines time synchronisation classes from the least accurate to the most accurate as in Table 5.2 of IEC 61850-5, repeated as Table 5.2 here.

This table sets accuracy classes intended to meet different levels of performance requirements. More practical is to map the accuracy requirements for different applications in the substation to the time synchronisation accuracy classes. This is shown in Table 5.3 of IEC 61850-5, shown (and modified) here as Table 5.3, remapping the Services of Table 5.1 to illustrate application-based time synchronisation requirements.

Table 5.2 IEC 61850-5 [4] Table 2 Time synchronisation classes for IED synchronisation

Time synchronisation class	Accuracy [us]	Phase angle accuracy for 50 Hz [°]	Phase angle accuracy for 60 Hz [°]	Fault location accuracy[b] [%]
[a]TL	>10,000	>180	>216	n.a.
T0	10,000	180	216	n.a.
T1	1000	18	21.6	7.909
T2	100	1.8	2.2	0.780
T3	25	0.5	0.5	0.195
T4	4	0.1	0.1	0.031
T5	1	0.02	0.02	0.008

[a] TL stands for time synchronisation “low”

[b] Only considering the quotient of voltage and current with the time jitter of the given accuracy. Since details in the fault location algorithms are not considered this column indicates only some reasons for requiring certain time synchronisation classes to reach a requested accuracy of the fault location. Reference for 100% is the full line length

Source modified version of IEC 61850-5 [4] Table 2

Table 5.3 Based on IEC 61850-5 Table 3 application of time synchronisation classes for time tagging or sampling

Time synchronisation class	Accuracy [ms] synchronisation error	Application	Service
TL	>10,000	Low time synchronisation accuracy—miscellaneous	Energy billing, operational measurement
T0	10,000	Time tagging of events with an accuracy of 10 ms	
T1	1000	Time tagging of events with an accuracy of 1 ms. SCADA, RTUs, and Distributed Bay Control Units	SCADA, Control Bays (RTUs, Bay Control Units), Digital Relays, Fault Analysis
T2	100	Time tagging of zero crossings and of data for the distributed synchrocheck. Time tags to support point on wave switching	
T3	25	Miscellaneous	
T4	4	Time tagging of samples respectively synchronised sampling	Merging Units
T5	1	High-precision time tagging of samples respectively high synchronised sampling	Phasor measurement units, travelling wave fault location

Source modified version of IEC 61850-5 [4] Table 3

5.1.5 Indicating Time Synchronisation Accuracy

Device publishing data will continue to publish this data even if the accuracy of their time synchronisation has degraded beyond their normal performance class. Therefore, the data must indicate the quality of the time tagging of the data, by providing some indication of the time synchronisation accuracy of the publishing device. Publishing devices can use information in the time synchronisation signal and their own processes to indicate time synchronisation accuracy.

The time synchronisation signal can indicate the accuracy of the clock time synchronisation against a global reference. Once an external time reference signal is lost, clocks will continue to publish time synchronisation signals based on their internal clock oscillator. Oscillators are not stable and drift over time, degrading the clock accuracy. The synchronisation signals should indicate that the server is no longer externally synchronised and how accurate the signal is. The 2016 edition of IEC 61850-9-3 [5] defines the use of the <<clockClass>> attribute of

IEC 61588 [6] to indicate to other devices the accuracy of the clock signal. The next version of IEC 61850-9-3 will use the <<clockAccuracy>> attribute of IEC 61588 to indicate accuracy of the clock signal.

Sampled Values publishers will indicate time accuracy through the <<SmpSynch>> attribute defined in IEC 61850-9-2 [1] and further defined in IEC 61869-9 [7]. Synchrophasor publishers will indicate time accuracy through the time quality portion of the FRACSEC word contained in the synchrophasor Ethernet frame defined in C37.118.2 [8].

Devices other than Sampled Values publishers can also indicate time accuracy by implementing time master supervision through the LTMS logical node. The time accuracy can be indicated through optional data objects. <<TmAcc>> indicates the number of significant bits in the Fraction of Second in the time accuracy part of the time stamp. <<TmSyn>> indicates that the device is synchronised according to IEC 61850-9-2, using an similar method to <<SmpSynch>> to indicate if the device is synchronised by a global area clock signal (<<TmSyn>> = 2), local area clock signal (<<TmSyn>> = 1), or external area clock signal (<<TmSyn>> = 0). TmSrcSet1 can set the time source to be IEC 61588 or other time sources.

5.1.6 Synchronisation

Clocks can be synchronised in three different ways:

1. time synchronisation,
2. syntonization, and
3. phase synchronisation.

IEC 61850 systems require the use of time synchronisation: all clocks must agree on the same time of day to provide accurate time tags for data. Wide-area communication networks, such as TDM, SDH, and SONET, require the use of syntonization: all clocks must operate at the same frequency so as to reduce data transmission errors. These networks do not normally require phase synchronisation, where the synchronised clocks are all in phase. The primary reference clock system used with these wide area networks is intended to provide only synchronisation. IEC 61850 systems implemented in substations need only time synchronisation.

5.2 Methods for Time Synchronisation

It is necessary to understand how to implement each step of the time synchronisation block diagram of Fig. 5.2. This includes the various global primary reference sources, some general requirements of the local master clocks, the time synchronisation methods that meet the requirements of IEC 61850 applications, the timing distribution network architectures possible based on the time synchronisation method, and how end devices perform based on their time synchronisation.

5.2.1 Global Primary Reference Sources

GNSS systems broadcast time signals from multiple satellites that are used to calculate the position of the receiver. These same time signals are used as the global primary time reference. The accuracy of this reference depends on multiple factors such are the clock precision, the satellite position and the propagation signal delay. There are multiple GNSS systems available. They use radio signals, broadcast on different frequencies, requiring different receiver antennas. They also use different global time scales, including differences in the handling of leap seconds.

5.2.1.1 Time Standards

There are three related high-precision coordinate time scales used by GNSS systems: International Atomic Time (TAI), Coordinated Universal Time (UTC), and Global Positioning System (GPS) time.

TAI is the principle realisation of terrestrial time using a weighted average of the time kept by over 400 highly accurate atomic clocks in over 50 national laboratories worldwide. The clocks are compared using radio signals and two-way satellite time and frequency transfer. TAI is an order of magnitude more stable than its best constituent clock due to the signal averaging between all the clocks. The epoch of TAI is midnight (00:00:00) of 1 January 1958. TAI does not implement leap seconds.

UTC is the primary time standard regulating clocks and time worldwide. UTC is kept to within 1 s of mean solar time at 0° longitude. UTC is defined by International Telecommunication Union Recommendation (ITU-R TF.460-6), “Standard-frequency and time-signal emissions” [9], and is based on TAI time with leap seconds added to account for the accumulated difference between TAI time and the earth’s rotation. As of 1 January 2017, UTC time is 37 s behind TAI time. The difference is based on a 10 s adjustment made on 1 January 1972, when UTC was implemented, and the 27 leap seconds that have been added since 1972.

GPS time is the atomic time scale implemented by the atomic clocks of the Global Positioning System. The epoch of GPS is midnight (00:00:00) of 6 January 1980. At this date, UTC was 19 s behind TAI time. Since GPS does not implement leap seconds, GPS is now 18 s (37–19 s) ahead of UTC time.

5.2.1.2 Global Positioning System (GPS)

The Global Positioning System (GPS) is a satellite-based radio-navigation system owned by the US government and operated by US Air Force. It is a global satellite system that provides position, navigation, and timing to a GPS receiver anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites.

The GPS Constellation requires a minimum of 24 satellites to operate worldwide. As of 2019, there are 31 operational satellites with a target of 33.

The GPS system uses the GPS time scale, and as of 1 January 2017, is 18 s ahead of UTC and 19 s behind TAI.

5.2.1.3 GLONASS

GLONASS is a space-based satellite navigation system operating as part of a radionavigation satellite service, owned by the Russian government, and operated by the Russian State Corporation for Space Activities (Roscosmos). It provides an alternative to GPS and is the second navigational system in operation with global coverage and of comparable precision. GLONASS provides real-time position and velocity determination for military and civilian users. GLONASS's orbit makes it especially suited for usage in high latitudes (north or south), where getting a GPS signal can be problematic. The constellation operates in three orbital planes, with eight evenly spaced satellites on each. A system is fully operational constellation with global coverage consisting of 24 satellites.

GLONASS time is based on UTC and is UTC time + 3 h (Moscow time). Since GLONASS is based on UTC, it implements leap seconds.

5.2.1.4 Galileo

Galileo is the GNSS created by the European Union (EU) through the European GNSS Agency (GSA).

One of the aims of Galileo is to provide an independent high-precision positioning system so European nations do not have to rely on GPS or GLONASS systems, which could be disabled or degraded by their operators at any time. The use of basic (lower-precision) Galileo services is free and open to everyone. Galileo has 24 active satellites.

Galileo uses the TAI time scale. The Galileo start epoch is defined as 13 s before 0:00:00 UTC on Sunday, 22 August 1999.

5.2.1.5 BeiDou

The BeiDou Navigation Satellite System (BDS) is a satellite navigation and time system built by China. BDS provides all-time, all-weather and high-accuracy positioning, navigation and timing services to global users.

BDS has 49 satellites in orbit, with 44 operational, between the BeiDou-2 and newer BeiDou-3 system.

BeiDou uses the UTC time scale, and therefore implements leap seconds, with an epoch of 1 January 2006 at 00:00:00.

5.2.1.6 Using Multiple GNSS Constellations

For reliability, it is attractive to use clocks that can synchronise to multiple GNSS constellations simultaneously, as each system uses different signals transmitted over different frequency bands. This requires a GNSS antenna that can receive the different signals in the different frequency bands. However, the GNSS constellations use different time scales and different implementation of leap seconds. It is incumbent on the clock to handle synchronisation between the different GNSS constellations and output the time signals correctly, especially if synchronisation to one of the constellations is lost. This capability must be proven during acceptance testing of the clock.

5.2.1.7 Using Multiple GNSS Frequencies

Each GNSS constellation transmits signals over more than one frequency band. It is also possible to have multiband receivers that synchronise to more than one frequency of each GNSS signal. This allows the clock to calculate propagation delays through the ionosphere with higher precision, resulting in better accuracy. Multiband clocks will have faster acquisition times after loss of signal and can enable advanced services such as anti-spoofing.

5.2.2 Contemporary Time Synchronisation Methods

The recommended time synchronisation method for IEC 61850 applications is IEC 61588 (Precision Time Protocol, or PTP). Existing substations will mostly use one of the common time synchronisation methods used in substations, such as one pulse per second (1 PPS), IRIG-B, and the Network Time Protocol (NTP)/Simple Network Time Protocol (SNTP), [10] but these have challenges when implementing IEC 61850-based solutions. PTP is recommended for new IEC 61850 systems as it provides T5 accuracy using packet-based time synchronisation signals over any Ethernet network.

5.2.2.1 Time Synchronisation Architecture

PTP is designed to be used over packet-based networks, using the ping-pong method of sending and receiving data frames between the master clock and end devices to measure, and compensate for, the network path delay between devices. PTP supports multiple master clocks to provide both redundancy and reliability, while permitting end devices to choose the best master clock for synchronising purposes. PTP compensates for the switching delays of network devices while measuring the total path delay so as to provide T5 accuracy and is therefore suitable for all applications.

5.2.2.2 IEC 61588 PTP

IEC 61588 Precision Clock Synchronisation Protocol for Networked Measurement and Control Systems, commonly called the “precision time protocol” (PTP), is a time synchronisation protocol that operates over packet-based networks. The advantage to PTP over NTP/SNTP is the ability to compensate time synchronisation for the switching delays of network devices, such that PTP networks can achieve T5 accuracy. PTP networks also support multiple master clocks. All clocks under PTP run a Best Master Clock Algorithm (BMCA) to choose the best clock for time synchronisation. The choice of best master clock is based on clock accuracy, clock priority, and transmission path delays. This provides reliability and accuracy in the case of clock failure, or if increased delays on a network path impact accuracy.

PTP also supports special clock types to better manage the switching devices of packet-based networks. The first of the special clock types is the “transparent clock” (TC). Ethernet switches must implement a “transparent clock” that measures the residence time of the PTP messages passing through the switch, then updates the PTP messages with this time to compensate for switch delays. The residence time is the time an Ethernet frame takes to transit the switch, which will vary with network load. This compensates for switch latency due to other network traffic and significantly improves the performance of PTP when a shared Ethernet network. This also means that PTP network traffic does not need to be prioritised over other traffic, simplifying the network design. This transparent clock requirement means that network devices must have native hardware support for PTP.

The other special clock type is the “boundary clock” (BC). A boundary clock can segment the network into separate “time zones” for reliability purposes. A boundary clock has multiple PTP ports. One of these ports synchronises to an upstream master clock. The other ports are used to synchronise downstream end devices to the boundary clock. In normal operation, the boundary clock passes time synchronisation messages from the master clock through to the end devices. If the master clock signal is lost, the boundary clock continues to synchronise all the downstream end devices to the boundary clock itself, maintaining a relative time synchronisation for this part of the substation network. Boundary clocks are most commonly implemented in network switches.

PTP is a time synchronisation standard used in all industries, not just the electrical industry. As a result, it is a very broad standard to provide the flexibility needed for timing applications in these different industries. Therefore, every industry must develop application profiles for PTP to provide standard ways to meet the requirements for the industry. The power industry has two closely related profiles for PTP: IEC 61850-9-3 (the “Utility Profile”) and IEEE C37.238 [11] (the “Power Profile”).

5.2.2.3 IEEE/IEC 61850-9-3

IEEE/IEC 61850-9-3 is a joint standard between IEEE and IEC. The standard is a PTP profile to define the options used in the bulk electric system. These options include:

- Time is transmitted using TAI; conversion to UTC, if needed, is done by slave devices.
- Peer-to-peer delay calculations are used. The delay between devices that make up every network hop is measured individually; the time compensation between the master clock and the end devices is the sum of all these individual peer delays. Accuracy is based on an average error estimate.
- Support of both transparent clocks and boundary clocks in the system is required.

- Definition of performance requirements such that any network with up to 15 cascaded switches will deliver time with better than one microsecond (T5) accuracy 99.7% of the time. The standard defines a method to calculate this network inaccuracy and sets maximum inaccuracy limits for network devices.

5.2.2.4 IEEE C37.238-2017

IEEE C37.238:2017 extends the IEC 61850-9-3 profile for some specific applications, specifically to identify the accuracy of time synchronisation of synchrophasor data. C37.238 adds:

- A custom Type Length Value (TLV) to communicate the time inaccuracy field. This field is used by phasor measurement units to determine the time accuracy of synchrophasor data, as described in the Message Time Quality of C37.118.2. All transparent clocks must support the IEEE C37.238 profile in order to update the total inaccuracy information, which is a dynamic field. Accuracy is based on a worst-case error estimate.
- Immunity to other PTP profiles on the network. C37.238-2017 uses a fixed PTP domain of 254, while other profiles are only allowed to use 0-127.
- Updated short grandmaster ID. The short grandmaster ID field now allows the use of all 16 bits. This provides compatibility for devices using IRIG-B and the IEEE Std C37.238-2011, as this field is a user-settable ID that does not change when the clocks hardware is replaced.
- Support for PTP-to-IRIG protocol converters to account for legacy systems.

Because C37.238-2017 is an extension of IEC 61850-9-3, any clock or switch that supports C37.238 will therefore support IEC 61850-9-3.

5.2.3 Legacy Time Synchronisation Methods

Though the use of PTP as the time synchronisation method is recommended for all new IEC 61850 systems, many substations will still have legacy devices requiring other time synchronisation methods. It is useful to discuss some of these methods and their ability to meet IEC 61850 timing requirements for practical application needs. 1 PPS and IRIG-B both use analogue time synchronisation signals, and therefore required a dedicated timing distribution architecture. NTP/SNTP uses packet-based time synchronisation signals and can use any Ethernet network. 1 PPS and IRIG-B can achieve T5 accuracy, and so are suitable for any application in the substation. NTP/SNTP can normally only achieve T0 accuracy and therefore should only be used for applications where basic time synchronisation is required.

5.2.3.1 Legacy Time Synchronisation Architecture

As stated, both 1 PPS and IRIG-B are analogue time synchronisation signals and require a dedicated architecture to distribute the signal. This architecture can be either electrical or fibre optic. The electric architecture is driven by an analogue output from the master clock and uses either shielded twisted pair or coaxial cable. Multiple end devices can be multidropped from the electrical cable. Great care must be taken in setting and designing the network, to ensure the clock analogue output can handle the load, to prevent propagation delays from effecting accuracy, to ensure proper electrical isolation and prevention of ground loops, and to ensure the circuit is grounded properly with an appropriately sized terminating resistor to prevent reflection of the signal. Master clocks typically have multiple analogue output ports to support multiple analogue circuits, and signal repeaters are often on circuits to manage distance and loading. Architectures using fibre-optic cable still send an analogue pulse only over fibre-optic cable. Devices can still be multidropped to multiple end devices. The use of fibre-optic cable alleviates some of the installation challenges of electrical cable. 1 PPS and IRIG-B do not support multiple master clocks, so each analogue cable is a single point of failure for time synchronisation.

NTP/SNTP is designed to be used over packet-based networks, using the ping-pong method of sending and receiving data frames between the master clock and end devices to measure, and compensate for, the network path delay between devices. NTP/SNTP supports multiple master clocks to provide both redundancy and reliability, while permitting end devices to choose the best master clock for synchronising purposes. Unlike PTP, NTP/SNTP simply measures total path delay and does not compensate for the switching delays of network devices. NTP/SNTP therefore nominally supports T1 accuracy, but in practice supports only T0.

5.2.3.2 One Pulse Per Second (1PPS)

One pulse per second (1PPS) can be used to provide an accurate synchronisation reference. Pulse is the simplest form of synchronisation, as devices are synchronised on the rising or falling edge of an accurately repeated pulse. The technical parameters to provide the performance pulse signals are pulse width, electrical level, and static space contact.

1 PPS can provide T5 accuracy, which is sufficient accuracy for all applications. However, it does not provide time of day information, so it may not be used with devices publishing synchrophasors, or with any services requiring time stamped data, such as fault location, fault analysis, or SCADA. Some devices may use a different time protocol such as IRIG-B, ASCII serial time protocols, or SNTP to provide time stamp data, while using 1 PPS to provide the on-time point. 1 PPS can be used for synchronising devices publishing SV, but is not recommended, as this requires a separate timing distribution circuit to be provided to merging units and other devices in the switchyard.

5.2.3.3 IRIG-B [12]

IRIG-B has been the most commonly used time synchronisation in substations, as IRIG-B can provide T5 accuracy, while providing information such as time of day through analogue electrical pulses. IRIG-B can be transmitted as unmodulated DC level shift pulses over electric or fibre-optic cables, or as an amplitude modulated

(AM) 1 kHz carrier over electrical cable. Unmodulated DC level shift is more accurate than AM, while AM can support longer analogue circuits. However, due to the complexity of detecting zero crossings, AM alone cannot be reliably used as the time synchronisation signal for synchrophasors to meet the 1 μs time error requirement and may require an unmodulated pulse as well.

IRIG-B has a number of options of how the time code is formatted and transmitted. The synchrophasor standards, especially IEEE Std C37.118.1-2011 [13], require additional extensions that provide information such as year, time zone offset from UTC, daylight savings time, and time quality. These time code options can lead to challenges in device interoperability and in designing the timing networks. Many end devices support only specific IRIG-B time codes and also typically support only unmodulated or modulated signals, but not both. Since only one time code and one transmission format can be used per timing circuit, multiple different analogue circuits may be required in some substations, or the use of localised conversion devices to change time codes or transmission formats.

IRIG-B will continue to be used in substations due to the installed legacy base and can provide time synchronisation for every application. IRIG-B should not be used for synchronising SV publishers, as IRIG-B requires providing a separate timing distribution circuit to merging units and other devices in the switchyard.

5.2.3.4 NTP/SNTP [10]

Network Time Protocol (NTP) and Simple Network Time Protocol (SNTP) are time synchronisation protocols that use the same time packet from a master clock message to compute accurate time. The messaging from the master clock is exactly the same for NTP and for SNTP. The difference between NTP and SNTP is how the end device does error checking and actual correction to the time data. NTP provides slightly more accuracy than SNTP, but NTP is more complex to implement, so SNTP is typically used in substation devices.

NTP/SNTP has been used in substations because it was the first widely adopted timing protocol over packet-based networks that provided reasonably accurate time synchronisation for applications such as device event logs. As the accuracy is nominally only T1, and in practice is normally T0, NTP/SNTP should only be used when required by legacy applications. For example, many Ethernet switches only use SNTP for internal time synchronisation.

5.2.4 General Requirements for the Local Master Clock

The local master clock is the interface between the global primary reference for time and the devices in the substation. There are some general high-level requirements for this master clock:

- The clock should be based on GNSS, with the ability to support timing signals from multiple global primary reference systems simultaneously.

- The clock should support PTP as the primary time synchronisation method. PTP should at a minimum implement the IEC 61850-9-3 profile. Ideally, the clock should implement the C37.238 profile, especially when synchronising phasor measurement units. When applied in substations with legacy equipment, to ensure compatibility the clock should support time synchronisation via IRIG-B, NTP/SNTP, and PTP simultaneously.
- When the clock supports IRIG-B for legacy devices, the clock should have multiple IRIG-B outputs, with the ability to support both modulated and unmodulated IRIG-B signals. The IRIG-B time code should be configurable.
- The clock should have multiple Ethernet ports for NTP/SNTP and PTP synchronisation over packet-based networks. The clock should be able to connect to a minimum of two separate networks. The PTP implementation should support both PRP and HSR high availability network recovery protocols for reliability.
- The clock oscillator should be at a minimum a TCXO—Temperature Controlled Crystal Oscillator—to provide low drift rate when operating in holdover mode.

For most substation applications, this TCXO is sufficient, and the expense of a more accurate oscillator, such as a rubidium oscillator, is not justified except for certain critical substations. OCXO oscillators may be good compromise when better performance than a TCXO is needed, as they offer excellent resilience to temperature fluctuations and good short-term stability. In addition, chip-scale atomic clocks are starting to become available, resulting in local clocks with very accurate performance at reasonable cost.

Support for IEC 61850-9-3 is very important when synchronising Sampled Value publishers. IEC 61869-9 extends the requirements for publishing SV defined in IEC 61850-9-2 by using the <<clockClass>> attribute of PTP as defined by IEC 61850-9-3 to determine the value of the <<SmpSynch>> attribute for SV data. The method of IEC 61869-9 is the only globally defined method to determine the <<SmpSynch>> attribute. Versions of IEC 61850-9-3 later than the 2016 edition will mandate the use of <<clockAccuracy>> of IEC 61588 to determine the value of the <<SmpSynch>> attribute.

Another general set of requirements for the local master clock is around cyber security. Blocking or spoofing clock signals can negatively impact applications in the substation. General requirements would be to use anti-jam antennas for connecting to GNSS and implementing spoofing detection. The clock should plan for future support for securing the actual PTP messaging over the network once the industry determines standard methods to do so.

5.2.5 Network Architecture Considerations

The main design consideration from a time synchronisation perspective should be ensuring the highest availability, maintainability, expandability, and robustness that meets the application requirements of an IEC 61850 substation. The goal should be to provide T5 accuracy to all devices and applications in normal operating circumstances, and to maintain T4 accuracy during periods where synchronisation to the global primary reference is lost. In general, this recommends PTP as the preferred solution for new substation projects due to the following benefits:

- Utilises the existing communication infrastructure of a substation automation system minimises the investment cost as no separate infrastructure for time synchronisation is required.
- Supports redundant master clocks for reliability purposes.
- Supports robust design of substation automation applications with graceful degradation and islanding of time domains through the best master clock algorithm (BMCA).
- Simplifies engineering as only simple or no configuration is required for clocks.

The use of PTP is especially recommended with SV publishers such as merging units. This ensures there is only one communications infrastructure in the switchyard to provide SV data, status and control of primary equipment, and time synchronisation.

5.2.5.1 PTP Over Networks Using PRP or HSR

Many IEC 61850 substations will implement networks using either the PRP or HSR recovery protocols for high availability networks. Both of these recovery protocols use the same basic concept of duplicating a published Ethernet frame over different network paths. The subscribing device uses the first of the frames received and discards the second. This is a challenge for PTP signals. PTP measures the round trip path delay between the master clock and the end devices, but the master clock will be receiving duplicate frames, which can lead to improper time synchronisation.

IEC 61850-9-3 requires the use of one of the time synchronisation methods described in Annex A of IEC 62439-3 [14]. The basic logic behind all the methods in the Annex is to treat the duplicate frames and paths as essentially two different PTP master clocks by implementing a modified BMCA. An end device is time synchronised through one of the duplicate paths to the master clock, but is always checking the other duplicate path to the master clock. One of the possible methods, that of a doubly attached ordinary clock, is shown in Fig. 5.3. The practical challenge is that Annex A describes multiple implementation methods, leaving the choice as to method and specific details a vendor decision. One such vendor implementation is described in [15], using the Ordinary Doubly Attached Clocks described in Annex A, but other methods and implementations are possible.

Using PTP over PRP or HSR therefore requires significant testing to prove that this time synchronisation works; and works with all devices on the network. Note that with PRP, master clocks can be connected as singly attached nodes to each of the networks, so end devices can use the normal BMCA for synchronisation.

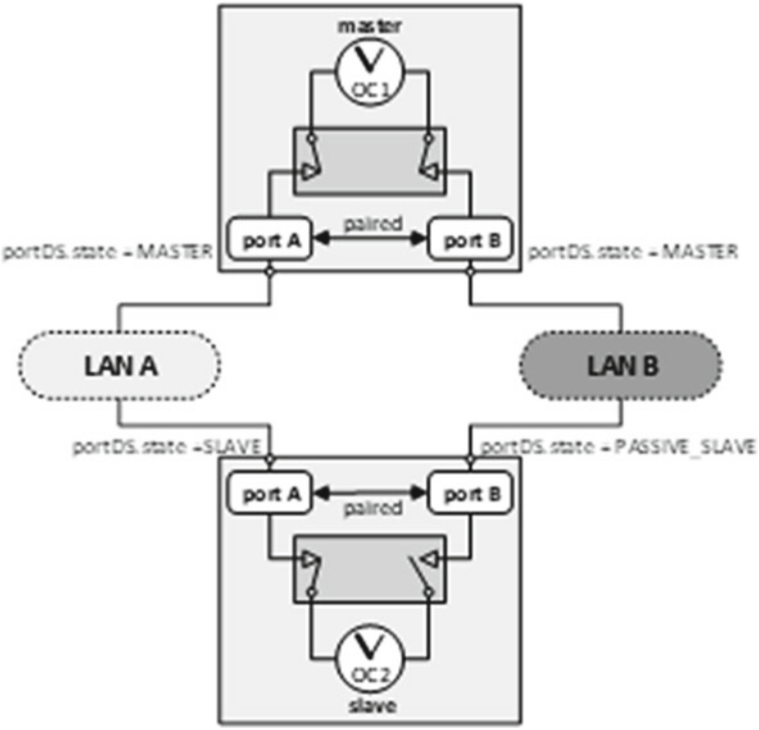


Fig. 5.3 Ordinary doubly attached clocks

5.2.5.2 Impact of Loss of Time Synchronisation

All systems in the substation that use time synchronisation can be impacted by the loss of global time synchronisation. Some functions will continue to operate with local time synchronisation, and some functions can operate without any time synchronisation. To consider specific functions in the substation operating under local time synchronisation:

- GOOSE messaging will continue to operate as normal. Time tagging of data will lose accuracy as the local clock oscillator starts to drift.
- MMS controls and services will continue to operate as normal. Time tagging of data will lose accuracy as the local clock oscillator starts to drift.
- Sequence of event data will still be captured, but time tagging of data will lose accuracy as the local clock oscillator starts to drift.
- Disturbance data will still be captured, but time tagging of data will lose accuracy as the local clock oscillator starts to drift.
- Synchrophasor data will still be published. Under C37.118.2, the Message Time Quality information will change to indicate the loss of accuracy as the local clock oscillator starts to drift.

- Sampled Values messages will still be published. The <<SmpSynch>> attribute will remain at 2 “time traceable” initially, and all protection functions will continue to operate as normal. Once the local clock accuracy degrades and time accuracy is no longer smaller than 250 ns of accuracy, the <<SmpSynch>> attribute is set to 1 “local clock”. Depending on the capability of and configuration of the protection devices, most protection functions based on Sampled Values data will continue to operate on this local time synchronisation. However, line differential protection is likely to only be available when the <<SmpSynch>> attribute in the SV messages is 2. On circumstances of total loss of a time synchronisation signals, <<SmpSynch>> will be set to 0, and all protection functions in subscribing relays requiring synchronised SV should be blocked.

Of particular note is when the global time synchronisation is re-established after a period under local time synchronisation. The performance of most functions will be unaffected, other than the accuracy of the time tagging. There is a concern over SV messages, however. If significant time synchronisation drift has occurred, the time sequence of published SV data may become disordered when global synchronisation is re-established, which can result in blocking protection functions until the time sequence is restored, or possibly result in undesirable operations of protection functions [16]. Testing of device responses is required during both acceptance testing of devices and commissioning of actual systems.

The <<SmpSynch>> attribute for SV data is important to understand to ensure protection functions work as desired. The availability of protection functions in a device will be tied to the value of the <<SmpSynch>> attribute in the SV data. To date, manufacturers of merging units have been inconsistent in how the <<SmpSynch>> attribute is set in relation to the availability of clock signals. How devices set the <<SmpSynch>> attribute, and their interaction with specific clocks, must be tested during both acceptance testing of devices and commissioning of actual systems.

This is one reason why PTP using the IEC 61850-9-3 profile is recommended. IEC 61869-9 maps the <<SmpSynch>> attribute to the <<clockClass>> attribute as defined by the 2016 edition of IEC 61850-9-3. While the SV publisher is connected to a master clock that is globally synched (9–3 clockClass = 6), the <<SmpSynch>> attribute is set to 2 “time traceable”. <<SmpSynch>> remains set to 2 if the clock loses global synchronisation, but is still within holdover accuracy (9–3 <<clockClass>> = 7). When the clock accuracy in this holdover state degrades past 250 ns, <<clockClass>> is set to 52, then it is set to 187 once accuracy exceeds 1 μs. When the <<clockClass>> is 52 or 187, T5 accuracy cannot be maintained, which mandates the <<SmpSynch>> attribute be set to 1 “local area clock”. Later versions of IEC 61850-9-3 will use the <<clockAccuracy>> attribute to determine the value of <<SmpSynch>>. <<Smpsynch>> is set to 2 if the <<clockAccuracy>> is within 250 ns, and set to 1 once accuracy is outside of 250 ns.

5.2.5.3 Boundary Clocks to Maintain SV Performance

The merging units publishing SV data subscribed to by a specific relay must be time synchronised to each other for the protection functions in the relay to function properly. As described, the <<SmpSynch>> attribute is intended for the merging units to provide an estimation of time synchronisation accuracy to the subscribing devices. A concern is a long-term failure of master clocks in the substation, leading to eventual drift of time synchronisation, and blocking of all protection functions. When using PTP, one solution to this may be to use boundary clocks resident in network switches or other devices to segment the merging units connected to a relay into an individual "time zone". Merging units are normally synchronised to the master clock through the boundary clock. If the master clock completely fails, the merging units remain synchronised to the boundary clock. In this case, <<SmpSynch>> will be set to 1, and all local protection functions should continue to operate.

5.3 Time Synchronisation Redundancy

Time synchronisation redundancy is a subject that should be considered relative to the timing requirements of the user application and the effect on the application system should timing signals be lost or significantly degraded. In other words, if the application system can still adequately function with a loss of timing, then redundancy may not be required. If the application system cannot continue to adequately function with a loss or degradation of timing, then an alternative timing source should be deployed. This process of redundancy can mitigate for hardware and software failures in the deployed timing equipment by providing identical parallel timing equipment, or it could be a different timing technology to act as a backup timing source. This type of backup timing source is useful when the primary timing source is affected by changes in the external macro layer timing system, such as for example jamming and spoofing of GNSS. The backup timing system should be selected such that the threats or failure mechanisms of the backup timing system are different to the primary timing system. For example, if GNSS is the primary timing system then the backup timing system could be a terrestrial system without the same exposure to RF jamming and space weather that can adversely affect GNSS signals.

5.3.1 GNSS

Global Navigation Satellite Systems (GNSS) have long been used as a source of timing and synchronisation, given that the satellite constellations are themselves synchronised to UTC and allows a GNSS receiver to very accurately synchronise to the satellites typically to within 50 ns accuracy relative to UTC. There are now multiple independent satellite constellations with the main ones being GPS (US), Galileo (EU), BeiDou (China) and GLONASS (Russia) meaning that there are now a large number of satellites available to cater for space segment failures of individual satellites or constellations, as described in Sect. 5.2.1 Global primary reference sources. GNSS timing systems often use packet-based timing protocols to transport timing to point of use over IP networks, with the use of IEC 61588 PTP being an increasingly popular protocol. The PTP standard defines the use of grandmaster and slave clocks, with the grandmaster clock typically synchronised to GNSS and the slave clock co-located with the user equipment.

5.3.1.1 System-Wide Grandmaster Clock Versus Local Architecture

While locating a single grandmaster to connect to all slave clocks over a network is possible, the effects of Packet Delay Variation (PDV) on the PTP packets over a full IP network can significantly impair the recovered timing performance at the slave clocks. Therefore, care should be taken with the IP network design to avoid network asymmetry, and often it yields better results to locate multiple grandmaster clocks that can serve local sectors of the network with less PDV effects. The use of multiple grandmaster clocks also provides resiliency as slave clocks can select multiple grandmaster clocks to connect to through the best master clock (BMC) algorithm. Of interest is the availability of chip-scale atomic clocks, which permit the use of local master clocks with very high accuracy at reasonable cost.

The use of GNSS does have a number of significant and well-known failure mechanisms as described in the following sections.

5.3.1.2 RF Interference

The GNSS satellites transmit low power signals, such that by the time the signals are picked up by a ground based GNSS receiver the signals are extremely weak. This means that the signal-to-noise ratio (SNR) of the received signals can be very susceptible to local RF interference that can block the reception of GNSS signals and deny the capability of the GNSS receiver to continue providing UTC aligned timing signals to the user equipment. GNSS receivers typically have low-cost Temperature Compensated Crystal Oscillators (TCXOs) as their local oscillator which will continue providing timing signals for a very short period of time following a loss of GNSS lock, and GNSS timing servers often have higher-quality Oven Crystal Oscillators (OCXOs) or even atomic Rubidium (Rb) or Cesium (Cs) atomic clocks for extended holdover periods. The level of GNSS interference is steadily increasing globally due to the extensive use of GNSS jamming equipment that is typically used in vehicles to overcome GNSS tracking systems and is either civilian or criminal in use. As such, any user equipment that is GNSS synchronised that is located near to roads or highways may be exposed to GNSS interference, although it should also be noted that RF interference from other general electronic equipment located near the GNSS receiver antenna can induce similar effects.

Therefore, if the user application needs resilient GNSS timing then the potential effects of GNSS interference should be considered and mitigated by the use of high-quality holdover oscillators or suitable backup timing systems. In the case of backup timing systems, there should be included the capability to detect GNSS interference and switch to the backup timing system and then revert when the

GNSS interference has ended. This type of interference detection capability is now being included in the equipment of various timing equipment vendors and should be tested in accordance with performance testing systems as described in Sect. 5.5.

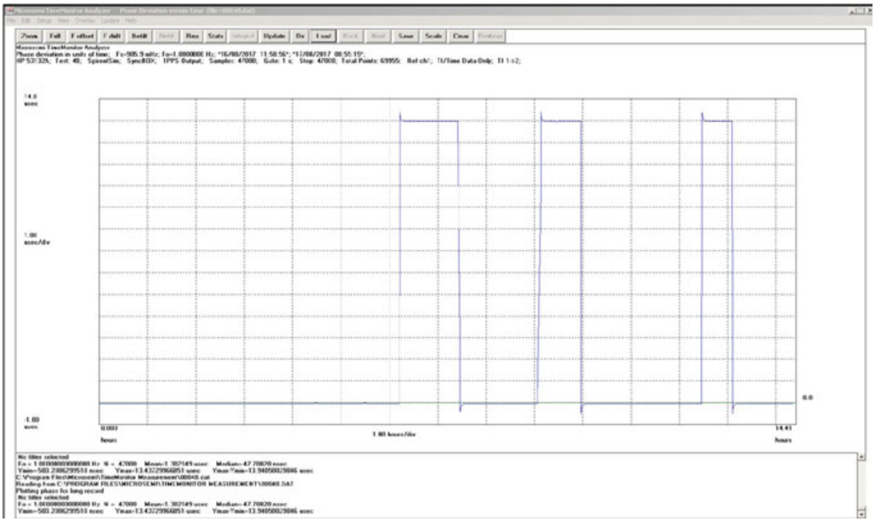
5.3.1.3 GNSS Spoofing

GNSS timing receivers lock onto the received GNSS signals and extract timing information from the signal data to synchronise their timing outputs to the GNSS satellite constellation. GNSS spoofing is a process whereby someone deliberately transmits fake GNSS signals with incorrect timing or positional data from a location close to the GNSS receiver with a view of trying to fool or "spoof" the GNSS receiver into locking onto these fake GNSS signals. If a GNSS timing receiver locks onto the spoofed signals, then the receiver may simply follow whatever timing errors have been deliberately introduced into the fake signals and will have the effect of making the receiver timing signals follow these errors. GNSS spoofing has been known about for a number of years but in recent times is now becoming a significant concern to users of critical or national infrastructure. This concern is based upon the increasing incidence of such events in various parts of the world, compounded by the fact that GNSS spoofing equipment can now be very easily constructed and operated by information freely available on the Internet.

Therefore, if the user application needs resiliency to potential GNSS spoofing events then the consideration of GNSS spoofing detection techniques should be adopted, along with the ability to switch to a suitable backup timing system during the GNSS spoofing event. A number of GNSS timing equipment vendors are beginning to include GNSS spoofing detection capabilities into the timing equipment, and these should be tested in accordance with performance testing systems as described in Sect. 5.5.

5.3.1.4 GNSS Constellation Errors

There have been a number of situations in recent years where there have been errors in the data transmitted by a particular GNSS constellation. The most well-known incident happened in 2016 when a GPS satellite (SV23) was decommissioned from the GPS constellation and in the process, erroneous data was uploaded to the GPS constellation. This error caused 13 μs jumps in the time base of GNSS receivers using GPS as the time base for their timing outputs and took many hours to resolve. To mitigate for such GNSS constellation errors, users of timing systems should deploy timing systems capable of detecting errors in individual GNSS constellations either through cross-comparisons between constellations or other backup timing sources. The use of a suitable backup timing source can used during periods of GNSS constellation errors to ensure that the time base of the user application remains unaffected by the errors. The testing of GNSS constellation errors can be undertaken through the use of GNSS simulators running simulations of such events, and an example of the timing effects of the 2016 SVN23 event is shown in Fig. 5.4 as jumps in the timing output in us (the y-axis) versus time in hours (the x-axis). This graph clearly shows the timing output



```
Microsemi TimeMonitor Analyzer
Phase deviation in units of time;  Fs=505.9 mHz; Fo=1.0000000 Hz; "16/08/2017  11:58:56"; "17/08/2017  08:55:15";
HP 53132A;  Test: 48;  SpeedSim;  SyncBOX;  1PPS Output;  Samples: 47000;  Gate: 1 s;  Stop: 47000;  Total Points: 69955;  Ref ch/;  TI/Time Data Only;  TI 1->2;
```

```
No filter selected
Fo = 1.0000000000000 Hz  N = 47000   Mean=1.302149 usec   Median=-47.70820 nsec
Ymin=-503.2306299513 nsec     Ymax=13.43729966051 usec     Ymax-Ymin=13.94050029046 usec
C:\Program Files\Microsemi\TimeMonitor Measurement\00048.cat
Reading from C:\PROGRAM FILES\MICROSEMI\TIMEMONITOR MEASUREMENT\00048.DAT
Plotting phase for long record
No filter selected
Fo = 1.0000000000000 Hz  N = 47000   Mean=1.302149 usec   Median=-47.70820 nsec
Ymin=-503.2306299513 nsec     Ymax=13.43729966051 usec     Ymax-Ymin=13.94050029046 usec
```

Fig. 5.4 2016 SVN23 event timing effects

of the GNSS receiver faithfully following the test scenario with resulting 13 μs jumps in the timing output. It should be noted that the magnitude of the error in this type of event could have been much larger in magnitude and therefore had an impact on a larger number of applications.

5.3.1.5 Space Weather

Given that the GNSS constellations are space-based systems, they are prone to the effects of space weather which can induce high levels of ionisation in the ionosphere. This ionisation process leads to propagation delays in the GNSS satellite signals as they travel through the ionosphere and manifest themselves in associated timing errors in GNSS timing receivers. The use of multifrequency GNSS should be considered to mitigate the effects of such errors, as such GNSS receivers can compensate for such events through comparison of received satellite signals at different frequencies. Timing equipment vendors are starting to use such multichannel multifrequency (MCMF) technology in their GNSS timing receivers. These types of MCMF GNSS receivers can be tested in accordance with performance testing systems as described in Sect. 5.5.5.

5.3.1.6 White Rabbit Project

Another method of time synchronisation reliability is the method being developed in the White Rabbit project. This project uses a fully deterministic Ethernet network for sub-nanosecond accuracy time transfer. The work was originally performed as the timing distribution network for the accelerator sites at CERN and for the GSI Helmholtz Centre for Heavy Ion Research.

White Rabbit provides sub-nanosecond accuracy of synchronisation of thousands of nodes, has predictability and reliability through deterministic delivery of high priority messages through class of services, and the robustness (most important to reliability) of no losses of high-priority system device control messages.

White Rabbit timing networks use three important technologies: time synchronisation via PTP, frequency syntonisation using SyncE, and phase measurements. In practice, PTP only provides sub-microsecond accuracy. SyncE synchronises all the clocks in the network to the same frequency using a phase-locked loop between these clocks and a master node, removing the jitter and frequency drift in the clocks that is responsible for offsets. The phase measurement determines the phase offset between the master and local clock based on the syntonisation signals, resulting in a very accurate measurement for the particular link delay.

Work has been done using a White Rabbit network for synchrophasor measurements as described in [17].

5.4 Practical Implementations of Time Synchronisation

The practical implementation of time synchronisation for an IEC 61850 system requires meeting two general criteria:

- Minimum requirements of accuracy for the intended application
- Reliability of time synchronisation for all critical operating scenarios.

A practical time synchronisation system will meet accuracy and reliability requirements through redundancy, general architecture, understanding how individual devices actually meet time synchronisation requirements, and a design for test. PTP, using either the IEC 61850-9-3 or C37.238 profiles, is the future choice for time synchronisation, as PTP is the only time synchronisation method that meets both accuracy and reliability requirements for IEC 61850 substations. This is especially true for process bus applications, as reliable time synchronisation is an absolute need for the correct operation of certain protection functions, and PTP is the only practical method to provide this reliability using switchyard networks. IRIG-B, PPS, and NTP time synchronisation methods will continue to be used to support legacy devices and applications where they are required. The practical implementation of time synchronisation therefore assumes the use of PTP as the synchronisation protocol.

Redundancy in general will mean the full use of GNSS through connections to redundant satellite systems, redundant antennas, redundant clock sources in the substation, and sending time signals over redundant communications networks. Redundancy can also mean using a different method for time synchronisation such as the terrestrial systems and White Rabbit method suggested in Sect. 5.3.1.6. These systems are not fully available yet, so have not been applied in utility substations, but they are under active development.

The system architecture must be designed to ensure time synchronisation signals are available to all devices on all networks. IEC 61850 substations with process bus may have multiple physical networks that require time synchronisation. It is also important that all devices on the network, including networking components, support the time synchronisation signals. PTP requires specific hardware support from all networking components, which must be addressed when applying PTP to existing networks. Support for PTP is one element that makes achieving accurate time synchronisation over wide area packet-based networks such as MPLS extremely difficult. As described in Sect. 5.3.1, multiple local master clocks or a chip-scale atomic clock is a more practical choice for reliability.

It is important to understand how all devices interact with and respond to time synchronisation in the sense of how devices respond to acquisition and loss of time synchronisation signals, and how devices indicate their time synchronisation status. There are three general cases to consider: when a device first connects to a time synchronisation signal; when a synchronised device loses the time synchronisation signal; and when a previously synchronised device regains the time synchronisation signal. For many systems, this performance is not that critical, but there are two specific use cases where this is critical to understand: publishing synchrophasors as per C37.118.2 and publishing Sampled Values as per IEC 61850-9-2. In both cases, the protocol addresses this by publishing quality information on the accuracy of time synchronisation, using time inaccuracy information in the case of C37.118.2, and the <<SmpSynch>> attribute in the case of Sampled Values.

The concern about start-up is how long a device takes to become accurately synchronised, and how it indicates this accuracy, as this potentially impacts system start-up procedures. The behaviour of the device must also be understood when the synchronisation signal is lost, meaning the clock is free running. Therefore, the oscillator accuracy and holdover times should be known, and how the device indicates the status of time synchronisation. Importantly, there is no standard that presently defines device should behaviour to the loss and recovery of time synchronisation. However, for standardisation of device behaviour is under discussion in IEC Technical Committee 57 “Power Systems” Working Group 10 “IED Communications and associated data models in power systems”.

Publishers of Sampled Values are the devices to be most aware of. The <<SmpSynch>> attribute has three possible values: 2 (Globally synchronised), 1 (Locally synchronised), and 0 (not synchronised). Subscribers to Sampled Values data may exhibit different behaviours based on the <<SmpSynch>> attribute of the publisher, so the correctness of this value in indicating the actual time synchronisation condition is critical for system performance. It is important to test how publishing devices implement the change from globally synchronised to locally synchronised on loss of signal to prevent interoperability and performance issues. Publishing devices are expected to become consistent with how they implement <<SmpSynch>> as they fully adopt the IEC 61869-9 standard for Sampled Values datasets. It is also important to know that the method used for determining <<SmpSynch>> in IEC 61869-9 is reliant on master clocks are publishing PTP signals that are fully compliant to the IEC 61850-9-3 profile.

Design for test simply means facilities and procedures for testing time synchronisation, as well as providing field personnel with the training and tools to perform the testing. Some basic testing that will be used under acceptance testing of the system may include:

- Verification if the time setting and accuracy is correct for both the clocks when connecting them to the GPS antenna with the coaxial cable included.
- Verification of the redundancy between the two timeservers in all connected IEDs.
- Verification of delay request and delay response data as defined in PTP standard to/from IEDs synchronised via PTP timeserver. Delta time between “delay request” and “delay response” should be less than one microsecond.
- Response of IEDs regarding summer and wintertime changes: IEDs recognised the time change. SV streams continuously sent every 250 µs, and no gap in the sequence number of SV streams was noticed.
- Verification of error messages in case of failure of GPS antenna and grandmaster ID changed.

5.4.1 Case Studies of Time Synchronisation

PTP is already being applied for time synchronisation in IEC 61850 systems. It is useful to consider some actual case studies of time synchronisation to see the actual challenges and considerations. The following two case studies both use PTP for time synchronisation. The first case study looks at the architecture for a full digital substation. The second looks at specific challenges related to time synchronisation and merging units publishing Sampled Values.

5.4.1.1 Case Study 1: Full Digital Substation

This case study is full documented in [18]. This project is a full digital substation including the use of Sampled Values as the source data for protective relays and other devices. The architecture uses separate physical networks for the station LAN and for process bus. The station LAN is a simple Ethernet network, while process bus uses PRP networks for availability and reliability. The substation uses PTP for time synchronisation. The system architecture is as in Fig. 5.5.

The system achieves high reliability by doubling the PTP time references:

- Grandmaster nodes with multiple reference time sources, e.g. GNSS receiver and local reference clock(s). Each node included an external rubidium oscillator synchronised to the GNSS receiver.
- Multiple grandmaster nodes, each with their own reference clocks.
- Multiple redundant fibre routes between nodes.
- Boundary clocks with long holdover times.

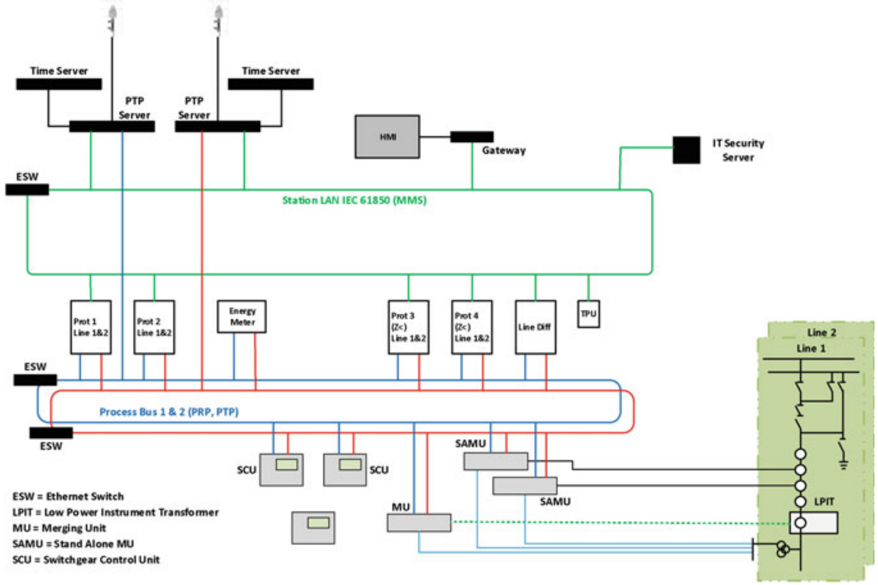


Fig. 5.5 Digital substation architecture

In this implementation, the master clocks chosen did not support PRP, so two master clocks where used, one for each of the PRP networks of process bus. The goal is that no single failure of a time synchronisation signal would lead to functional restriction for different devices. The general clock arrangement is shown in Fig. 5.6.

Installation, testing, and monitoring the system came up with the following learnings around the time synchronisation system.

There are several learnings around master clock redundancy. As both clocks are identical in terms of clock class, clock quality, and clock variance, which master the end devices synchronise to is random. To solve this, the Priority 2 PTP setting in one master is set higher, so this becomes the normal preferred master, while still allowing the end clocks to synchronise to the master with better dynamic parameters. It was observed a single bad reading from a satellite resulted in a worse time quality on one master, leading to end devices to swap master clocks. This swap happened frequently, especially during bad weather. Reducing the sensitivity of the GPS receiver stopped the frequent failovers but impacted the synchronisation of the external oscillators.

There are also several learnings around devices and device behaviours. The Ethernet switches selected all support PTP as components of the networks, acting as transparent or boundary clocks. However, the switches themselves time synchronise only to NTP, and so required an NTP synchronisation signal from the master clocks. Part of testing this installation is removing all three time sources in sequence, to observe end devices swapping master clocks, and to observe device

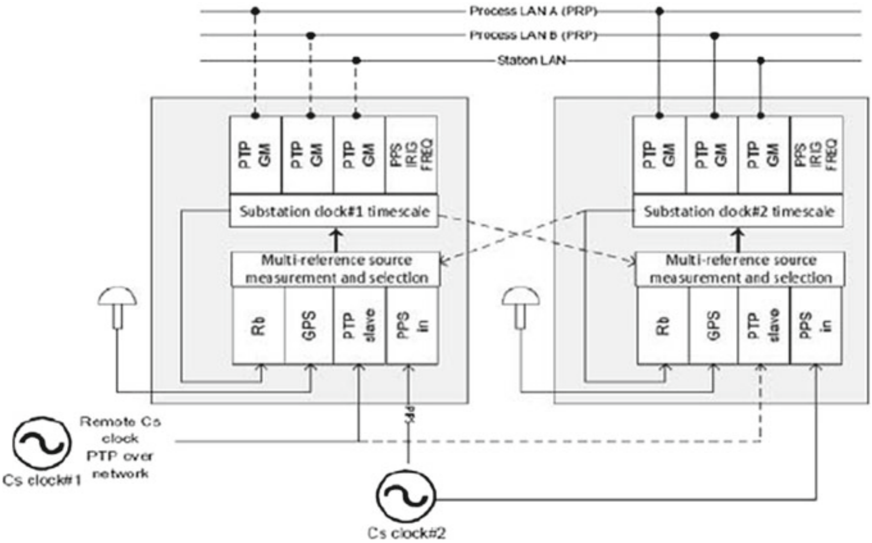

Process LAN A (PRP)
Process LAN B (PRP)
Staton LAN
PTP GM
PTP GM
PTP GM
PPS IRIG FREQ
Substation clock#1 timescale
Multi-reference source measurement and selection
Rb
GPS
PTP slave
PPS in
PTP GM
PTP GM
PTP GM
PPS IRIG FREQ
Substation clock#2 timescale
Multi-reference source measurement and selection
Rb
GPS
PTP slave
PPS in
Remote Cs clock PTP over network
Cs clock#1
PPS
Cs clock#2

Fig. 5.6 General clock arrangement

behaviour in holdover mode. Different devices provided different alarms to the HMI during this process; these alarms need to be homologised. When running in holdover for a long period of time, drift between Sampled Values published by different devices was eventually observed, requiring an adjustment to protective relaying philosophy.

Testing also showed that redundancy for process bus time synchronisation isn't optimal. Removing one master clock for maintenance purposes results in no time synchronisation signals on one of the process bus networks. It is possible to temporarily reconfigure the other master clock to provide redundant signals, but this is a manual process to reconfigure the master clock and network.

This case study shows that it is possible to design a PTP time synchronisation system that provides accurate and reliable time synchronisation through redundancy, system architecture, the devices used, and testing. This case study also shows that the implementation of PTP may need to be adjusted somewhat based on the actual devices used in the IEC 61850 system.

5.4.1.2 Case Study 2: Full digital Substation Pilot Project

This case study is fully described in [19]. This project is a fully digital substation pilot project, in a live transmission substation, including the use of Sampled Values as the input data to protective relays. One of the goals of the project was to test different network architectures. The time synchronisation protocol used is PTP using the IEC 61850-9 3 profile, synchronising devices over both PRP networks and HSR rings.

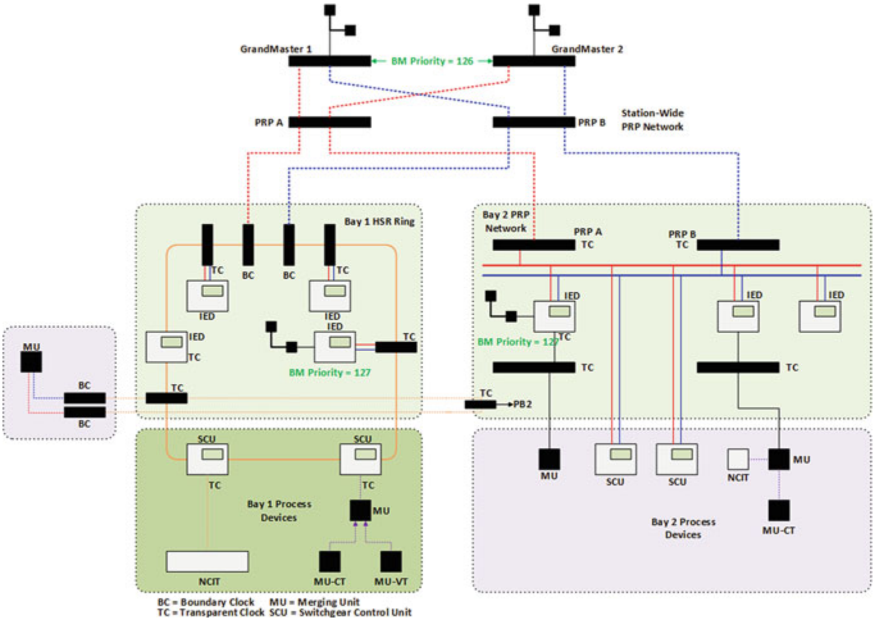


Fig. 5.7 Case study 2 full digital substation

The general architecture of this project is shown in Fig. 5.7 and starts with redundant grandmaster clocks connected to a station-wide PRP network. The station-wide PRP network is connected to two bay level networks. The bay level networks include all protection, control, and I/O devices for the bay. One of these bay networks is an HSR ring, and one is a PRP network. The grandmaster clocks are GNSS clocks synchronising to both GPS and GLONASS satellite systems and attach to the PRP networks as doubly attached nodes. The grandmaster clocks are both given the same grandmaster priority in their configuration.

The general intent in this project was to connect bay level switches as boundary clocks to limit multicast traffic on the network, and to maintain time synchronisation of merging units in case of grandmaster clock failure. In this project, the interfaces connecting the HSR ring to the PRP network, known as Redundancy Boxes (RedBox) are configured as boundary clocks to manage the topological change in architecture. However, it was decided to keep bay level switches on the PRP bay network as transparent clocks due to the small network size. Some of the devices in the bays are only singly attached nodes; they are connected through RedBoxes configured as transparent clocks. One device requires a separate 1 PPS signal for time synchronisation, an example of the occasional need to maintain legacy time synchronisation protocols in actual projects.

Testing

Extensive testing was carried out to prove performance of time circulation. Overall system test included:

- Loss of satellite signals (GPS and GLONASS)
- Loss of LAN A or LAN B in PRP, or loss of Direction A or Direction B in HSR
- Loss of one or both grandmaster clocks and operation of the network when one of the boundary clocks takes over as the master for a segment.

Most important were the process level tests, as time synchronisation of Sampled Values data must be maintained for protection functions to operate. Of particular focus was the behaviour of the <<SmpSynch>> attribute as set by the merging units. This requires the following tests:

- Disconnection and reconnection of merging units from the network to ensure the merging units resume publishing with the correct value of <<SmpSynch>>.
- Disconnection and reconnection of time synchronisation to the merging units. This is to verify the merging unit publishes <<SmpSynch>> with the correct value of 2 (global) or 1 (local) until the merging unit clock holdover time is exceeded.

Learnings and observations

The first learning is that it is preferable to configure clocks on both priority and clock class to achieve desirable performance of the BMCA in end devices. Giving boundary clocks a lower priority (higher number) than master clocks ensures that the BMCA operating in end devices always synchronise to a master clock when it is available, as long as the master clock has a better accuracy when in local mode (<<clockClass>>=7). Also, when boundary clocks had the same priority as master clocks, and there was any mismatch in settings for the PTP profile such as holdover time, delays of 15–30 s in the BMCA selection resulted. Once this was resolved, by changing priorities of the boundary clocks, the system and process level tests were performed, and the time synchronisation system was proved reliable.

Other recommendations and learnings include the selection of grandmaster clocks with a good oscillator providing a holdover period of 12–24 h. As described, it is important to precisely match the profile configuration between clocks and end devices in applications using redundant multivendor grandmaster clocks. And a general recommendation for the industry is to increase to holdover time of merging units to 30 s to maintain scheme availability during temporary loss of time synchronisation signals.

5.4.1.3 Case Study 3: Merging Units and Time Synchronisation

This case study is fully documented in [20] and illustrates the specific issues with time synchronisation for process bus, and how devices publishing Sampled Values must correctly indicate the accuracy of the time synchronisation.

Sampled Values must be explicitly time synchronised for protective relaying to operate reliably. The standard in China at this time uses point-to-point networks for Sampled Values and process bus, as this simplifies time synchronisation to the control of the IED connected to the merging unit. However, the recognition is that

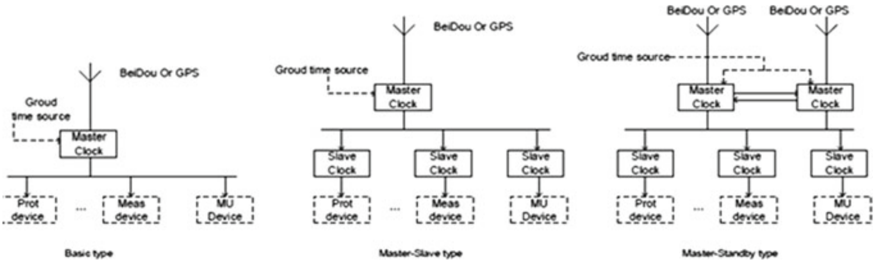


Fig. 5.8 Possible redundant clock architectures

a LAN-based process bus has great application value, and this will be the future direction.

To facilitate this, the three different clock architectures of Fig. 5.8 may be used. 35 kV substations use the basic-type or master–slave-type connections, and substations 110 kV and above use Master-Standby-type connections. Fully digital substations with LAN-based process bus will always use the Master-Standby type, as this supplies redundancy of clock signals.

The architecture is fully redundant. There have been several learnings around the performance of the merging units (MUs) publishing Sampled Values.

One learning is around start-up. Upon start-up and initially acquiring a clock signal, MUs will set the <<SmpSynch>> value to 0 until the MU is fully synchronised, which will maintain the associated protection functions until the MU is fully synchronised. To address this issue, the clocks in the MUs use a "fast tune" time synchronisation on initialisation, then use more traditional time synchronisation to limit jitter.

A second learning has been observed instances of "pseudo-synchronisation" between MUs. This situation can occur when re-synchronising MUs after the loss of the time synchronisation signal. MUs go into holdover when the time synchronisation signal is lost, but do not initially change the <<SmpSynch>> value. When the clock signal is restored, some MUs immediately synchronise to this signal, while others remain in holdover. Both MUs will publish SV with the same value of <<SmpSynch>>. Pseudo-synchronisation occurs when there is a significant difference in the time between the MU that is synchronised and the one in holdover. Both are publishing SV with the same <<SmpSynch>>, and subscribing devices will use this data as correct, though they are not truly synchronised.

5.5 Performance Testing of Time Synchronisation Systems

Given that the use of GNSS comes with known vulnerabilities, then any GNSS-based timing system should be tested to ensure that they can be tested to assess the impacts of any of the threats identified in Sect. 5.5.3. The testing process should be designed such that the user timing requirements can be fully exercised and measured during the threat scenarios to ensure that the timing system can mitigate for these effects. Typically, the mitigation process should be a backup timing source that the timing system can be connected to during the GNSS threat testing and assessing if the timing system can detect the GNSS threat and successfully switch to the backup timing source and then revert to GNSS when the threat has concluded. They should also be tested to prove protection and control system performance, such that even with the loss of both master clocks in a system, protective relays and their associated data sources such as merging units will still be locally synchronised so that local protection functions will still operate correctly.

5.5.1 Application Tests

Application tests prove the time signature synchronisation performance of individual system components during operating scenarios around the loss of time synchronisation signals. As discussed in Sect. 5.2, PTP is the only practical time synchronisation protocol for IEC 61850-based substations. The application tests described here are based around the use of PTP. The case studies of Sect. 5.4 highlight many of the tests required including:

- Loss of satellite signal
- Loss of a redundant master clock
- Performance of boundary clocks on loss of master clocks
- Loss of a network path when using PRP or HSR high availability networks
- Loss and return of clock signals for merging units, including the performance of the <<SmpSynch>> attribute
- Performance of protection elements in relation to the <<SmpSynch>> attribute when Sampled Values are used as inputs to relays
- Performance of BMCA negotiation during changes in master clock availability

The goal in all of these tests is to prove devices are connected to the correct master clock, all devices have the same time as the master clock, devices switch to the correct master clock when the BMCA requires selection of a different master clock, and all devices show a synchronisation locked indication.

5.5.2 Application Testing Tools

The testing tools used in application tests are network monitoring tools with the ability to capture and record the time synchronisation signals present on the network. These tools should monitor PTP traffic, as well as IED data streams and IED synchronisation status. The tools must include general logging capabilities, and the ability to display the data in both time synchronisation messages and IED data messages.

5.5.3 System Tests

The measurement of timing systems is often performed by the use of Time Interval Error (TIE) measurements via the use of counter timers that measure the phase offset between the timing output of the Unit Under Test (UUT) and a trusted timing reference. TIE data can then be post processed to analyse the timing system performance and a number of vendors produce specialist timing measurement equipment or PC-based software that can undertake this analysis. A high-level view of a typical TIE analysis architecture is shown in Fig. 5.9. Which in this case shows a GNSS receiver transporting timing over IEEE 1588 PTP with the ability to exercise the GNSS receiver through the use of a GNSS simulator. The GNSS simulator can be used to run scenarios of GNSS interference, GNSS spoofing, GNSS constellation errors and space weather, and Fig. 5.10 shows an example of TIE data for a MCMF GNSS receiver. It should be noted that the use of GNSS timing accuracy can often be compromised by incorrect antenna cable delay compensation, whereby the physical length of the antenna cable causes proportionally higher levels of delays in the GNSS timing receiver output. GNSS timing receivers normally allow the user to compensate for these delays through a software interface with an antenna cable length value. The performance testing process can also be used to ensure that such calibration values have been correctly applied to the timing system. In addition, this type of performance testing becomes much more critical when timing signals are passed over IP networks with protocols such as IEEE 1588 PTP such that the timing signals recovered from the PTP slave clocks can be measured and verified to be within acceptable limits. This type of testing for IEEE 1588 PTP timing performance often reveals issues in the IP network that can be resolved to improve the overall timing performance.

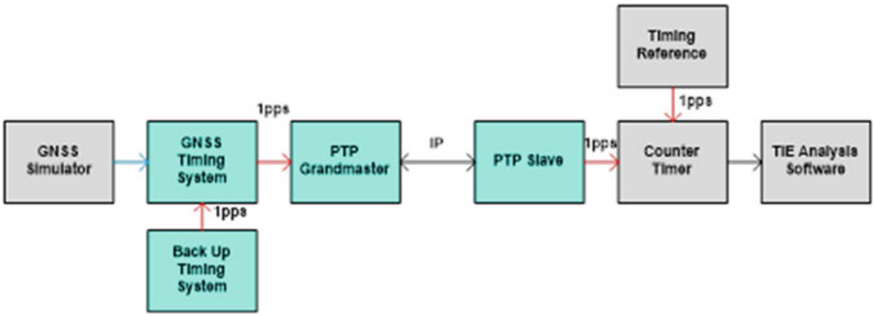


Fig. 5.9 TIE analysis architecture

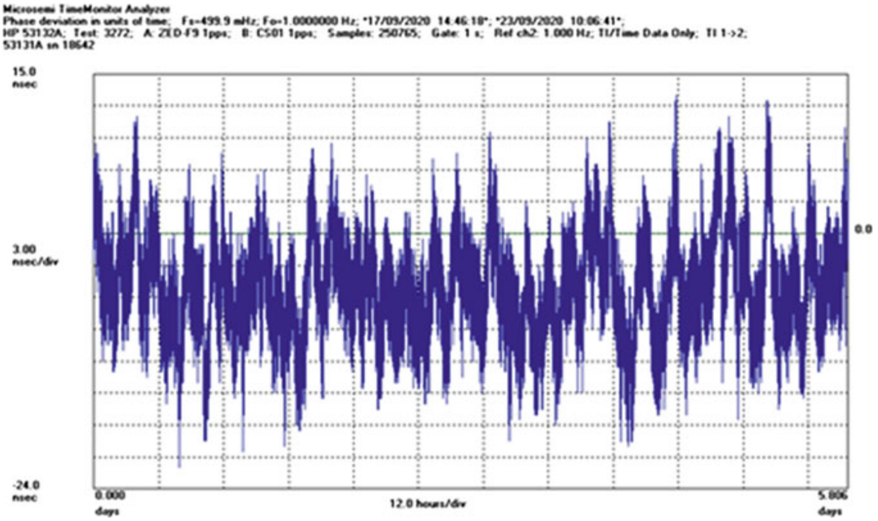


Fig. 5.10 TIE data for a MCMF GNSS receiver

References

1. IEC 61850-9-2: 2011+AMD1: 2020 CSV Consolidated version Communication networks and systems for power utility automation—Part 9–2: Specific communication service mapping (SCSM)—Sampled values over ISO/IEC 8802-3, IEC, Geneva, SW (2020). Copyright © 2011 IEC Geneva, Switzerland. www.iec.ch
2. IEC 61850-7-4:2010+AMD1:2020 CSV Consolidated version Communication networks and systems for power utility automation - Part 7-4: Basic communication structure - Compatible logical node classes and data object classes
3. Flores, P.H., et al.: Implementations and challenges in time synchronisation of protection, automation and control systems: experience and expectations of applications in Brazil. 2019 CIGRE B5 Colloquium, Tromso, NO (2019)
4. IEC 61850-5: 2013 Communication networks and systems for power utility automation—Part 5: Communication requirements for functions and device models, IEC, Geneva, SW (2013). Copyright © 2013 IEC Geneva, Switzerland. www.iec.ch
5. IEC 61850-9-3: 2016 Communication networks and systems for power utility automation—Part 9–3: Precision time protocol profile for power utility automation, IEC, Geneva, SW (2016). Copyright © 2016 IEC Geneva, Switzerland. www.iec.ch
6. IEC 61588: 2021 Precision Clock Synchronisation Protocol for Networked Measurement and Control Systems, IEC, Geneva, SW (2021). Copyright © 2021 IEC Geneva, Switzerland. www.iec.ch
7. IEC 61869-9: 2016 Instrument transformers—Part 9: Digital interface for instrument transformers, IEC, Geneva, SW (2016). Copyright © 2016 IEC Geneva, Switzerland. www.iec.ch
8. IEEE Std C37.118.2-2011 IEEE Standard for Synchrophasor Data Transfer for Power Systems, New York, NY (2011)
9. ITU-r TF.460-6 Standard-frequency and time-signal emissions, International Telecommunications Union (2002)

10. RF 5905, Network Time Protocol Version 4: Protocol and Algorithms Specification, Internet Engineering Task Force
11. IEEE Std C37.238-2017 IEEE Standard Profile for Use of IEEE 1588™ Precision Time Protocol in Power System Applications, IEEE, New York, NY (2017)
12. IRIG Standard 200-04, IRIG Serial Time Code Formats, Range Commanders Council
13. IEEE Std C37.118.1-2011 IEEE Standard for Synchrophasor Measurements for Power Systems, IEEE, New York, NY (2011)
14. IEC 62439-3: 2016 Industrial communication networks—High availability automation networks—Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR), IEC, Geneva, SW (2016)
15. Hunt R., Silvano, G., Rachadel, H., Dalmas, M.: Deployment and evaluation of PTPv2 in a PRP network. 2019 CIGRE B5 Colloquium, Tromso, NO (2019)
16. Ingram, D., Schaub, P., et al.: Assessment of real-time networks and timing for process bus applications—IEC 61850 and IEEE Std 1588. CIGRE SEAPAC 2013, Brisbane, AU (2013)
17. Derviškadić, A., Razzaghi, R., Walger, Q., Paolone, M.: The white rabbit time synchronisation protocol for synchrophasor networks. In: IEEE Transactions on Smart Grid (vol. 11, Issue. 1), IEEE, New York, NY (2020)
18. Hurzuk, N., Loken, R., et al.: Implementation of time synchronisation in the Stattnet R&D project—Digital Substation. CIGRE B5 Colloquium, June 24–28, Tromso Norway (2019)
19. Liu, D.-C., Xu, L.: Application and implementation of time synchronisation of digital substation in China. CIGRE B5 Colloquium, Tromso Norway (2019)
20. Mohapatra, P., Popescu, C., Balasubramani, P., Wehinger, M., Abdulla, A.: A real test of the PTP standard in project FITNESS. PAC World, Vol. 52 (2020)

Cybersecurity Integration with IEC 61850 Systems

6

Dennis Holstein, Mark Adamiak, and Herbert Falk

Abstract

In this chapter, a coherent methodology to seamlessly integrate cyber-physical security (CPS) systems with IEC 61850 protection, automation and control systems (PACS) is described. To do, one needs to understand how adversaries gain access and use of mission-critical protection and control devices and the digital communication networks that connect these devices. For all the right business and technical reasons, IEC 61850 systems have leveraged digitisation and ubiquitous connectivity technologies to enable today's operational systems. The same technologies have offered an open attack surface to adversaries with the skills to develop new tactics to interfere with, disrupt or disable PACS functions. The chapter concludes with the top six cyber-physical response actions to protect IEC 61850 protection, automation and control systems and a list of future study topics and objectives to improve this protection.

Keywords

IEC 61850 • Cyber-physical security • Advanced persistent threats • Risk assessment • Risk mitigation

D. Holstein (✉)
OPUS Consulting Group, Seal Beach, CA, USA
e-mail: holsteindk@ocg2u.com

M. Adamiak
Adamiak Consulting LLC, Paoli, USA
e-mail: adamiakconsulting@aol.com

H. Falk
OTB Consulting Services LLC, Troy, USA
e-mail: herb.falk@otb-consultingservices.com

P. Bishop and N.-K. C. Nair (eds.), *IEC 61850 Principles and Applications to Electric Power Systems*, CIGRE Green Books, https://doi.org/10.1007/978-3-031-24567-1_6

6.1 Cybersecurity Imperatives

To understand what is needed to protect IEC 61850 PACS assets and networks, one must have some understanding of the threats and how they are executed. To do this, the approach is to focus on well-resourced adversaries such as nation-states or criminal organisations. Thus, the security levels as described in IEC 62443-3-3 [1] only provide basic understanding for addressing the threats and vulnerabilities. The approach to rank order the cyber-physical security (CPS) solutions for PACS based on the perceived consequences of a successful attack provides a more holistic approach.

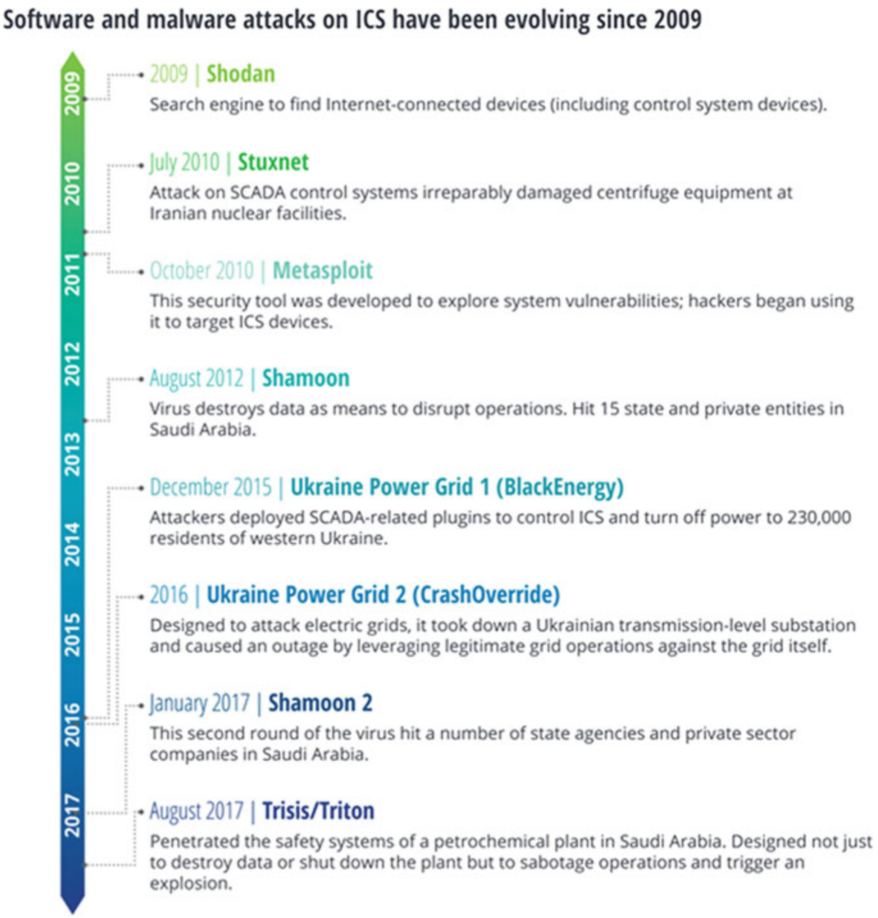
6.1.1 The Onset of Advanced Persistent Threats

Software and malware attacks on industrial control systems (ICS) have been evolving since 2009 [1]. For example, nation-state-sponsored terrorism is using advanced spy-craft technology [2] to find and exploit vulnerabilities inherent in open system communication networks, such as those deployed in IEC 61850 PACS architectures. For example, Fig. 6.1 describes Deloitte's analysis of the cyber threat profile for the US electric power sector [3]. The attacks on the Ukraine power grid in 2015 (BlackEnergy) and 2016 (CrashOverride) are excellent illustrations of Advanced Persistent Threats (APT) which target PACS to seriously disrupt the power services to a large service area.

An in-depth analysis of the Ukraine attacks shows how a well-financed adversary can patiently perform the reconnaissance to identify the vulnerability of the open system network to gain access to and control of the protection relays. This was not a simple one-off attack. The attack exercised was practised multiple times over 6 months to ensure that it would achieve the desired objective. Only when the adversary had confidence in its success was the attack executed.

What is learned from these APT attacks?

1. Endpoint detection and response systems are not effective because security information and event management technologies provide event notifications and alerts after the fact. This does little to trap and isolate the impending attack on PACS assets and networks during the reconnaissance phase.
2. Firewalls, anti-virus, intrusion detection systems and data loss prevention systems depend on existing signatures and rules. APTs use new and creative techniques developed during the reconnaissance phase. Therefore, their signatures and rules are unknown.
3. If Ukraine had a highly trained staff with high-powered analytical tools to recognise the reconnaissance activity, it could have taken timely action to forestall the attack. Reference is made to the discussion of maturity models and their metrics in Sect. 6.2.1.



Software and malware attacks on ICS have been evolving since 2009

2009 | Shodan

Search engine to find Internet-connected devices (including control system devices).

July 2010 | Stuxnet

Attack on SCADA control systems irreparably damaged centrifuge equipment at Iranian nuclear facilities.

October 2010 | Metasploit

This security tool was developed to explore system vulnerabilities; hackers began using it to target ICS devices.

August 2012 | Shamoon

Virus destroys data as means to disrupt operations. Hit 15 state and private entities in Saudi Arabia.

December 2015 | Ukraine Power Grid 1 (BlackEnergy)

Attackers deployed SCADA-related plugins to control ICS and turn off power to 230,000 residents of western Ukraine.

2016 | Ukraine Power Grid 2 (CrashOverride)

Designed to attack electric grids, it took down a Ukrainian transmission-level substation and caused an outage by leveraging legitimate grid operations against the grid itself.

January 2017 | Shamoon 2

This second round of the virus hit a number of state agencies and private sector companies in Saudi Arabia.

August 2017 | Trisis/Triton

Penetrated the safety systems of a petrochemical plant in Saudi Arabia. Designed not just to destroy data or shut down the plant but to sabotage operations and trigger an explosion.

Fig. 6.1 An evolution of cyber threat on the electric power sector

One could argue that the adversary needs to have a comprehensive understanding of the targeted PACS operation including applicable settings in the protective relays and related intelligent electronic devices (IEDs). They also need to know how to penetrate or circumvent the cyber defence mechanism deployed by the utility. This issue is addressed in previous CIGRE studies [4–6]. Figure 6.2 is used to explain how the adversary can use an insider to facilitate the attack on PACS assets and networks.

Threats are described in terms of their type, their objective, their location and success criteria. Three special threats of interest are those executed remotely (external threats), those executed internally by employees or contractors and those that require collaboration between internal organisations. This threat model is commonly known as the “insider threat”. Nation-states and criminal organisations have demonstrated a meticulous plan of action to cover every possibility and sequence

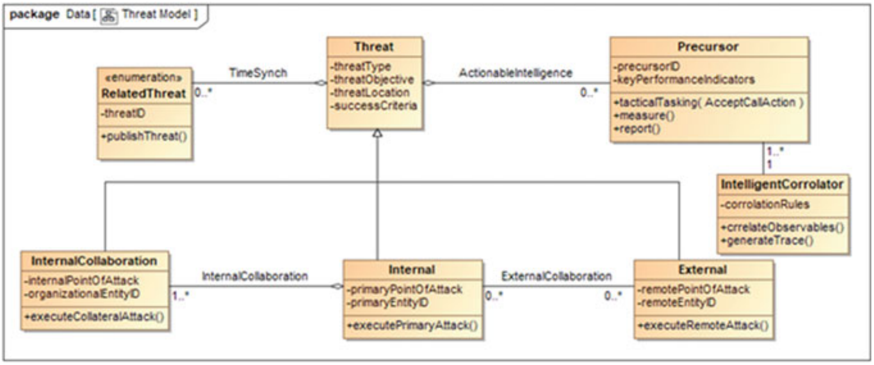


Fig. 6.2 Insider threat collaboration

of events needed to effectively compromise utility employees, support contractors and supply chain providers.

As described in [7], establishing contact with potential targets for compromise is often difficult. It requires finding a likely candidate, getting to know him or her ascertaining the candidate's interest, uncovering exploitable vices, and possible Achilles' heel requires a great deal of patience, time and resources. It is not unusual to take 6 months to 1 year to develop the rapport. It is important to understand the targets of compromise rarely if ever, succumb because of ideology. Personal reasons usually prevail, and ideological justifications often come after a decision has been made to cooperate with the adversary. Thus, models for responses and future actions are designed to cover many long-term, high-risk scenarios by focussing attention on precursors to track key performance indicators (KPIs) describing behaviour patterns developed by an analytical tool called "intelligent correlator" in Fig. 6.2. Unfortunately, most utilities poorly address this process because they have neither adequate staff skill nor analytical tools.

Some APT cases may be time synchronised with other related threats to add more confusion to the situation, in which case an instance of the related threat is modelled as part of the primary threat shown in the centre block [1]. The cardinality notation (0..*) simply indicates that an instance of threat knows about no related threat (0) or it may include many related threats (*).

Figure 6.2 also shows that no precursors or many precursors are part of the threat (0..*). This relationship identifies the actionable intelligence available to the utility organisations with staff skills and advanced analytical tools described by at least one instance of an intelligent correlator that provides the rules to correlate data from disparate sources. This correlation is known as data fusion which uses raw data to generate actionable intelligence. But that is a complex capability for another day.

The open literature is rich with examples that describe how employees and support contractors can be compromised by a well-financed adversary, e.g. nation-state or criminal organisation. Thus, there may be a collaboration between an external adversary with remote access privileges and an internal adversary who knows the nuances of the deployed protection system and its settings.

Given the advanced digitisation and ubiquitous connectivity inherent in 61850 protection and control schemes, there are usually multiple organisations that manage silos of operation. If these organisations have a heightened awareness of the potential attack, they will receive observable alarms initiated by the attack scenario during the reconnaissance phase of the attack and the end-game attack. In this case, the adversary needs to compromise internal employees and contractors within the applicable silos of operation.

6.1.2 Time on Target Doctrine

When CIGRE study committee D2 (Information Technology and Telecommunications) studied future threats and their impact on electric power organisations and operations, they identified “time on target” as a new doctrine to increase the effectiveness of a well-planned attack scenario [5]. The basic idea is to time the cyberattack vectors to create a saturation scenario. These attacks would come from multiple locations and gain access to the PACS assets and networks through multiple entry points.

For example, in the substation, there are access points on the process bus and the station bus that can be exploited. The exploit can be initiated by an insider threat agent or remotely by an external insider threat agent or by an external threat agent. For example, PACS network access ports that are disabled can be enabled at the prescribed time. The same is true for disabling alarm setting to ensure that those monitoring the system operation are not alerted to any anomalous behaviour.

Lastly, attack vector migration can be dormant and awakened by a timed trigger or event or a combination of both. The dormant vector can be installed early in the supply chain and not be detected during the supplier’s bench testing, factory acceptance testing, utility quality assurance testing, site acceptance testing and maintenance testing.

6.1.3 Fundamental Response Strategies

Faced with the rapid development and deployment of APTs, the utility must design a highly agile response strategy to better anticipate and proactively defend against unknown APTs before they evolve. This requires PACS and network engineers to use several new technologies such as artificial intelligence, machine learning and deep learning techniques. Because IEC 61850 protection systems are highly automated, they can readily incorporate these new technologies.

IEC 61850 PACS is enabled to provide data on demand to all applications that need the data. Put another way, data no longer travels from point A to point B, rather data has a point of presence that can be accessed promptly using multicast and publish and subscribe methods. Thus, the availability of these data provides the means to correlate the sequences of PACS network traffic, log data, asset metadata and federated intelligence to provide a context to the behaviour in your system and pinpoint the exact threat. PACS engineers have intimate knowledge of their networks and settings in PACS IEDs which can be leveraged against APT agents.

While standards such as IEC 62443 [1, 8, 9] and IEC 62351 [10–14] give rise to significant advances in mitigating APTs, operational maturity is the key to success. For this reason, we focus on response strategies that are indexed to a simple maturity model.

6.2 Understanding Cyber-Physical Security Issues

This section examines the cyber-physical security issues as they relate to the aforementioned maturity assessment schemes. The objective is to shed light on the complex nature of standing up and maintaining an effective response strategy.

6.2.1 Focus on Maturity Assessment Challenges

In response to the emerging threat landscape of well-financed advance persistent threats, there is an imperative need for utilities to assess the maturity of their security policies, procedures and organisational directives (PP&ODs). Based on their risk assessments, funding is allocated to upgrade the capabilities of PACS staff, processes, operational processes and automation technologies. To justify the allocation of resources, it is helpful to use a maturity assessment to identify and prioritise the investment in people, processes and technology. IEC standard 62443 is a multipart standard that provides a life-cycle framework to address operational requirements for industrial automation and control systems (IACS).

Maturity models allow an organisation to assess their capabilities and maturity level in many practice areas and assign a Maturity Indicator Level (MIL) to those practice areas. Typically, maturity models have 4 levels (MIL0-MIL3), where MIL0 indicates no or minimal maturity in the area, MIL1 indicates basic maturity, MIL2 indicates intermediate maturity, and MIL3 indicates advanced maturity. Some models provide additional levels indicating finer-grained advancement, with the highest MIL always indicating advanced maturity.

To achieve a particular level, all practices must be at or above the indicated level. For example, in an assessment of 10 practices, if nine of the practices are rated at MIL3, but one is rated at MIL1, the overall assessment is rated MIL1. Using the weakest MIL rating for reporting is a common approach. As discussed later, only MIL 1 needs attention.

Organisational directives assign responsibility and accountability to responsible PACS-related organisational units (ROUs) for properly executing maturity improvements and continuously managing and maintaining the needed level of maturity for the deployed cyber-physical security solutions. This requires a high degree of cooperation between operational personnel, including well-aligned enabling processes and procedures to maintain an effective defence posture.

By identifying specific practices that do not meet each organisation's goals for achieving a particular maturity level, resources may be effectively and prudently applied to improve those specifically identified areas to achieve the desired maturity level. In the preceding example, resources could be focussed on improving only the one practice area requiring improvement since the others have already been assessed at the desired levels. The process can then be repeated over time in a continuous improvement cycle to increase the maturity level.

Next is some insight into the available maturity assessment schemes available to support a utility's allocation of funding over the planning horizon, measurement of improvement effectiveness and adjustments needed to improve staff skills, operational processes and technical capabilities. Three maturity assessment schemes considered are as follows.

(1) Carnegie-Mellon Model (CMM) [15],
(2) DOE's Cybersecurity Capability Maturity Model (ES-C2M2) [16] and
(3) Nemertes Maturity Model (NMM) [17].

In the development of IEC 62443, ISA99 reviewed the general-purpose CMM and its use to assess the maturity of IACS solutions. They concluded this multi-dimensional model was far too complex and too difficult to align with the standard's approach to an effective security strategy.

ES-C2M2 is a well-understood scheme. It was released in 2012 after joint development between DOE, DHS and utility experts was piloted by over a dozen utilities during development and has since been updated and used by many other utilities. It has expanded from its initial electricity sector approach to include a natural gas version and a generic version. It is currently undergoing another revision. Computer-assisted tools have been developed to streamline the data gathering and analysis process making it easier for organisations to self-assess their maturity under the ES-C2M2. The Electric Power Research Institute (EPRI) uses this model to develop a set of metrics [18]. This is also a work in progress and needs to be tested and vetted by utility stakeholders.

The Nemertes maturity model is a simplified maturity assessment scheme that is closely aligned with the kill-chain model [19]. CIGRE working group D2.46 reviewed Nemertes' assessment methodology and found it to be easily aligned with IEC 62443 requirements for different levels of security posture [5]. This approach has not been tested or vetted by utility stakeholders. Because it is well-aligned with the kill-chain model and IEC 62443, it warrants further attention.

This simplified model has a few advantages over CMMI v2.0 and ES-C2M2. The simplicity of this approach is captured in Fig. 6.3, which aligns well with IEC 62443's focus on people, process and technology. PACS organisations can use a simple index (0.1.2.3) to rate the maturity of their staff's ability to address the evolving cyber threat landscape. In concert with staff, skills are the need for well-defined policies, procedures and organisational directives that can be

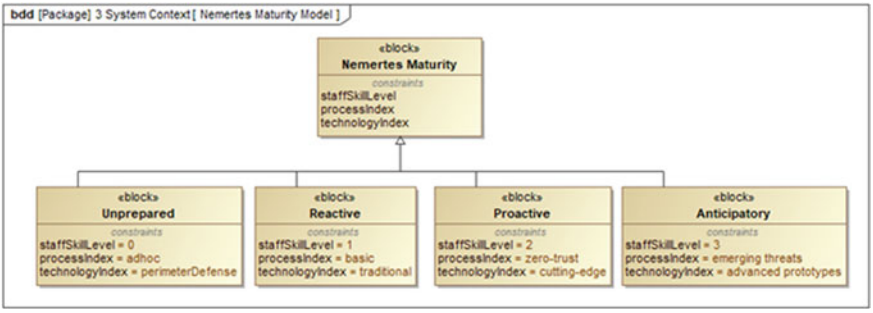


Fig. 6.3 Nemertes maturity model

indexed in terms of processes. Furthermore, staff skills also need to be aligned with technologies deployed by the utility.

At the lowest level (unprepared) is when the PACS staff skill level is rudimentary, processes are for the most part ad-hoc, and cybersecurity protection relies on perimeter defence in the form of firewalls and air gap between the operational networks and the business networks.

When examined in some detail, most PACS organisations fall into the "reactive" category of maturity. Their staff is periodically updated on the threat landscape to improve their awareness of the cybersecurity threats of interest. They do have approved policies, procedures and organisational directives that reflect the requirements imposed by local laws and regulations, such as the NERC CIP and EU's general data protection regulation (GDPR). Most cybersecurity protection is deployed in terms of traditional systems, such as firewalls, demilitarised zones (DMZ) and some features of IEC 62351 that are available from IEC 61850 solution providers.

Many of the larger utilities have stood-up versions of an integrated security operations centre (ISOC). But due to the high cost of operating an ISOC, many utilities need an alternative security operation centre, to share the cost—a federated security operations centre (FSOC). The idea behind the FSOC is to use many of the cloud computing services. However, extreme care is needed to guard against abuse of authentication mechanisms.

The U.S. National Security Agency (NSA) published Detecting Abuse of Authentication Mechanisms which discusses how malicious cyber actors are abusing trust in federated authentication environments to access protected data. The exploitation occurs after the actors have gained initial access to a victim's on-premise network. The actors leverage privileged access in the on-premise environment to subvert the mechanisms that the organisation uses to grant access to cloud and on-premise resources and/or to compromise administrator credentials with the ability to manage cloud resources. The actors demonstrate two sets of tactics, techniques and procedures (TTP) for gaining access to the victim network's cloud resources, often with a particular focus on organisational email [5].

There may be a few "proactive" PACS organisations that have invested in personnel with specialised cybersecurity skills and have updated their policies, procedures and organisational directives to reflect the guiding principle of zero trust. This requires the latest cutting-edge technologies to adequately ensure that only authorised entities (person or computer) have access to and use mission-critical assets. For example, identity and authentication management (IAM) relies on the use of digital signatures and implied trust in the selected certificate authority (CA).

The goal is to reach the "anticipatory" maturity level. At this level, the key is to provide skilled staff and the use of advanced cybersecurity prototypes to address the emerging threats, such as zero-day threats.

6.2.2 How Utilities Address APT Challenges

IEC 62351 standard has been published to provide security recommendations for different power system communication protocols including IEC 61850. In [20], detailed analysis of security threats, possible attacks and security requirements for IEC 61850 communication is presented. Building on this, the security considerations presented in IEC 62351 for securing different IEC 61850 messages such as Generic Object-Oriented Substation Events (GOOSE), Sampled Values (SV), Routable-GOOSE (R-GOOSE), Routable-SV (R-SV) and Manufacturing Message Specification (MMS) messages are discussed in [21] and summarised in an IEEE paper [22].

PACS use cases being considered include the following:

- Transfer trip from one to multiple terminals,
- Remedial action schemes (RAS) from a central controller to multiple remote controllers,
- Synchrophasor transmission,
- Surgical load shedding,
- Grid forming controls and
- Inverter-based black start.

Continuing with [21] and [23], experiments and laboratory demonstrations by a US utility have implemented R-GOOSE for their centralised-RAS; however, the security elements (authentication and encryption) are pending. Their major concern is the additional end-to-end communication message latency (about 1 ms) induced by the encryption mechanism. The encryption mechanism is discussed in Kanabar's paper [22].

A series of webinars [23] addresses security configuration and maintenance, which, in many cases, is viewed as complex and represents an impediment for adoption and deployment. The use of R-GOOSE/R-SV requires that the pairing of published information to subscribers of that information (e.g. a publication group) shares a common symmetric key that utilises a key distribution mechanism as specified in IEC 62351-9. The experiments and demonstrations rely on vendor tools to configure the security policies and manage the certificates. CIGRE Technical Brochure 427 raised several concerns that these configuration tools, testing tools and data collection tools are vulnerable to compromise by insiders including support contractors [6, 24]. Thus, there is a need to seamlessly integrate CPS solutions into proprietary tools discussed in Chap. 10. Protection and automation engineers need to be concerned with the security of engineering tools used to configure IEDs and to manage mission-critical technicians' settings. No standard explicitly addresses the security requirements imposed on IEC 61850 tools. Of concern are the security vulnerabilities introduced when attaching field technicians' notebooks or another device (e.g. portable media) to the substation LAN. For this reason, strong security for both local as well as remote access and use control is most important.

Another issue that needs attention is patch management. No standard or guideline provides sufficient technical detail to effectively address patch management on time. Although this is a general security problem, more research is needed to develop a concrete specification for patch management in IEC 61850 operating systems, protocol stacks and applications. The only work on this issue is the work in ISA99 and IEC TC65 WG 10 to develop IEC/ISA 62443-2-3 [8]. However, this is a general standard for Industrial Automation Control Systems (IACS) and there need to be some more specifications to tailor parts 2–3 for IEC 61850 systems.

No standard or guideline provides sufficient detail to effectively address the timely reporting of events (TRE); e.g. NERC CIP requires a report within 24 h from event notification. Intrusion detection and reporting systems are currently designed to look for known scripts but are woefully lacking in their ability to learn from attack patterns on time. More research is needed to develop derived requirements for IEC 61850 to ensure that cybersecurity events are reported to the proper authority promptly.

Including conformance statements in a standard is still a thorny issue. The best attempt to do this is specified in IEC 62443-2-4 [9]. Parts 2–4 need to be tailored for IEC 61850 systems.

The good news is the availability of applicable standards (IEC 61850-90-5, IEC 62351-9, RFC 6407) and experiments in work by a major US utility. The bad news is the sparse deployment of IEC 62351 implementations in PACS assets and networks. Without these deployments, there is a lack of assessments by PACS organisations that address both management and engineering challenges for an embedded solution. Therefore, PACS organisations must continue to rely on traditional security mechanisms which are reflected in a "reactive" maturity posture described in Fig. 6.3.

Until cybersecurity is integrated into the logical nodes of PACS assets and networks, some utilities are improving their maturity posture to a proactive level by standing up an integrated security operations centre (ISOC). CIGRE Technical Brochure 796 [5] provides a good summary of the capabilities provided by an ISOC. One major benefit to PACS organisations is the offloading of cybersecurity responsibilities for threat awareness, internal and external reporting and specialised skills needed to use the advanced analytical tools.

6.2.3 Security Testing Needs Attention

Functional testing is discussed in Chap. 9, but these tests should include cyber-physical security (CPS) testing as an integral part of the test program. PACS management should use rigorous methods to validate their models and document those methods and results. Using a variety of commercial tools for penetration testing, they should routinely perform tests to assess and determine if any open communication ports third-party not used. If so, they should be disabled. If required, third-party testing is recommended to obtain an unbiased assessment of the CPS solution. These tests should utilise real threats and attack methods that are being used by cybercriminals and other threat actors. The threat scenarios should be based on attacks collected from a recognised global threat intelligence network. Using automated and manual threats, three key capabilities need to be stress tested.

- Inbound threat detection and prevention (before execution),
- Execution-based threat detection and prevention (during execution) and
- Continuous monitoring post-infection and ability to act in the event of compromise (post-execution).

NSS laboratories, located in Fort Collins, Colorado (USA), have been proofing a wide range of product testing and evaluation services. For example, Check Point has actively participated in NSS labs testing since 2011 and has achieved NSS Labs recommendation in firewall, next-generation firewall and Intrusion Prevention System (IPS) group test.

6.3 Leveraging IEC 61850 for Early Threat Detection

The underlying capabilities designed into IEC 61850 logical nodes provide the structure to seamlessly integrate cybersecurity protection solutions. With this in mind, the next step is to explore some of these solutions.

6.3.1 Understanding the Kill Chain

The Law Enforcement Cyber Center uses the “kill-chain” model to define the cyberattack life cycle. The cyberattack on PACS assets and networks is straightforward; hence, any attacker can attack this system soon after getting access and escalating the privileges within the targeted system of interest. In such a case, the attacker must design the site-specific attack and test the attack before finally getting on with the actual attack; otherwise, there are high chances of failure. CIGRE survey, reported in [5], reveals that cybersecurity breaches are active on an average of 200 days in a critical infrastructure before they are discovered.

There are eight stages in the life cycle. For a cyberattack to be successful, the attacker must successfully execute all eight stages of the cyberattack life cycle;

therefore, to prevent a successful cyberattack from being successful, it is imperative to thwart the attack at any of the phases, or break the chain, in the life cycle. The eight stages of the life cycle are as follows:

- Perform initial reconnaissance. The attacker identifies PACS assets and networks and determines operating systems, security, applications, protocols, addresses and other runtime characteristics.
- Make an initial compromise. The attacker uses an exploit or attack to probe and break through PAC network cybersecurity system defences. This compromise could be achieved through social engineering, phishing, extortion or other means.
- Establish a foothold. The attacker establishes or creates persistence on a PACS asset or network, perhaps by installing a backdoor or installing utilities or malware to maintain access.
- Escalate privileges. The attacker gains greater access to PACS assets and data by obtaining credentials, leveraging privileges, belonging to an application or service or exploiting vulnerable software.
- Perform internal reconnaissance. The attacker explores other PACS assets and networks to map the entire environment, identify the roles and responsibilities of key operational staff and locate interesting or valuable data needed to execute the attack scenarios.
- Move laterally. The attacker jumps from one PACS asset to another asset on PACS networks, using network shares, scheduled tasks and remote access tools or clients.
- Maintain a presence. The attacker maintains ongoing access and activity on the PACS assets and networks using backdoors or remote access tools.
- Complete the mission. The attacker achieves his attack objectives, such as stealing sensitive data or executing a scenario that interferes with, disrupts or disables PACS functions.

Solutions to detect threats resident in PACS assets and networks are either anomaly-based or deception-based.

Anomaly-based detection creates a behaviour baseline of hosts, data access, network traffic, user behaviour, etc. Commonly, any activity that is inconsistent with the baseline is flagged as an alert to PACS responsible organisational unit and subsequently to EPU's security team. Anomaly-based solutions have two significant drawbacks:

- Capturing, storing and associating data from disparate sources are complex, expensive and time-consuming. It requires highly sophisticated tools and skilled analysts that are not usually common in PACS engineering organisations.
- False positives occur at a high rate, which can degrade the confidence in the assessment tools and security team.

Deception-based detection is an alternative to anomaly-based detection. Many of the PACS assets (multifunction relays, merging units, etc.) can be used for deception-based detection. The deceptions are not part of the normal operations and are revealed only by a cyberattack. When an intruder spends the time and effort to locate and access a deception that is set up to invite an attack, it is a positive affirmation of a compromise or a highly positive anomaly.

Deceptions take many forms to detect and engage threats at every step of the kill chain. Deceptions are broadly grouped into four types:

- Decoys: A decoy is a fabricated system or software server that presents an attractive target to an attacker. A decoy is usually more attractive to an attacker than a PACS asset or network because it is seeded with interesting (but fake) data and known vulnerabilities are left open.
- Breadcrumbs: Breadcrumbs are used to lead an attacker to a decoy. When an attacker does reconnaissance, breadcrumbs are placed on the endpoints and the PACS network points to create an interesting target.
- Baits: Baits are honey tokens such as counterfeit data or fake PACS operating credentials to a service that the attacker finds valuable. Baits are laid so that ordinary IT and OT procedures or normal user behaviour do not reach them. An attack can be detected by monitoring the access or usage of the bait.
- Lures: A lure makes a decoy, a breadcrumb or a bait more attractive than the actual PACS network assets. For example, to make a software service decoy attractive, it can be set with factory default credentials.

To address the insider threat, decoys, breadcrumbs, baits and lures must be closely guarded. They should not be known to each PACS organisation performing 24/7/365 operations.

6.3.2 Data Fusion in IEC 61850 Systems

If detection of the attack early in the kill chain is disrupted, or used to set traps, it can be used to thwart the adversary's intrusion objectives. Defenders can then implement appropriate countermeasures to protect their mission-critical functions. The fundamental elements of intelligence are the three types of indicators: atomic (source addresses, vulnerability identifiers), computed (derived data involved in an incident) and behavioural (tactics used by the adversary).

Tracking the deviation of a given indicator from its predecessors in the kill chain is the challenge. Connecting the indicators is difficult because the raw data comes from disparate sensors and is subject to unverified assumptions. In military intelligence terms, this process is known as tactical data fusion (TDF). At each stage of the kill chain, the outcome of TDF analysis can be catalogued as follows:

- Reconnaissance to identify and select PACS asset and network targets for intrusion.
- Weaponisation by exploiting a selected vulnerability to deliver a payload using an automated tool.
- Delivery of the weapon to the targeted environment.
- Exploitation to trigger the weapon's action by direct command or by auto-execution.
- Installation to maintain a persistent presence inside the selected PACS asset or network target to manage the attack.
- Command and control (C2) for the adversary to maintain positive control over the weapon's actions.
- Actions on objectives to execute the attack and adjust the tactics to achieve their ultimate objectives.

Two observations are derived from analysis of successful adversary campaigns and extrapolation to existing PACS environments: (1) adversaries have highly sophisticated tradecraft tools and expertise to perform and engage in each of the categories and (2) defenders need to significantly raise their maturity levels with advanced tools and strategies to perform the TDF functions in each category. In short, PACS managers need to migrate from a purely defence-in-depth (DiD) siege mentality to a proactive and anticipatory response strategy.

This dramatic shift in response strategy requires well-defined metrics to measure the performance and effectiveness of defensive actions at each stage of the kill-chain intrusion. As noted by Hutchins [24], framing metrics in the context of the kill chain, defenders have the proper perspective of the relative effectiveness of defence of their defences against the intrusion attempts and where there were gaps to prioritise remediation. Furthermore, there is a clear need to use advanced analytical tools to reconstruct the intrusion scenario at each stage of the kill chain. Without this reconstruction, it is nearly impossible to anticipate the next steps by the attacker. This projection is needed to establish the mitigation strategy to either disrupt, degrade, deceive or destroy the attacker's kill-chain strategy and tactics. One approach called intrusion reconstruction, promoted in several CIGRE technical brochures, is to define model-based systems engineering (MBSE) descriptions of the problem domain in terms of black-box and white-box relationships of the PACS system of interest (SoI). In turn, these logical architectures that emulate the SoI can be used to simulate (with live data feeds) the progression of the kill-chain scenario. Various mitigation options can then be examined to determine which approach is most effective to deny the attackers ultimate objectives. MBSE analysis focuses attention on the behaviour of the attackers, their tactics, techniques and procedure to determine "how" they operate, not specifically "what" they do.

For example, consider the case that from a remote workstation a targeted malicious agent containing a weaponised application installs a backdoor for outbound communications. Access to and execution of the weaponised application may be controlled by a means known only to the attacker. If so, this will be important information for the defender to select the appropriate mitigation option. Due to the reuse of known indicators collected over several weeks/months, the agent is blocked. Furthermore, analysis of the remaining kill chain reveals a new exploit or backdoor to PACS operational network. Without this knowledge, future intrusions from remote workstations delivered by other means may go undetected. This example illustrates the importance of the speed of response to deploy countermeasures, which gives the defender a tactical advantage. Background for this example is discussed at length in CIGRE Technical Brochure 762 [25].

This example illustrates the need for highly specialised training and tools to detect, process and reach an actionable conclusion. It also emphasises the need for timely coordination and cooperation between those responsible for operating the PACS assets and networks. Additionally, a well-defined situation assessment that can be shared with external agencies is needed. If the attack employs a combination of threat agents, selecting and executing the best response option are even more complicated. This further supports the need for a well-defined MBSE model of the SoI to select the best response and to avoid unintentional consequences.

6.3.3 New Crypto-Based Technologies for IEC 61850 Systems

Most physical PACS network links provide ill-defined and uneven guarantees of confidentiality and privacy or data integrity. Industry networks are increasingly wireless, and wide area networks are impossible to physically secure against pervasive surveillance. Therefore, any information from a user to a service or between users should preferably be encrypted at the object level using standards-based cryptographic techniques to render it unintelligible to eavesdroppers while at the same time offering the data integrity/trust model necessary as actionable information.

All types of communications from the user, customer or function should be protected: personal information, found at the organisational level or sensitive sensor inputs, should be encrypted to preserve privacy and control (and security). However, even access to otherwise public resources should be obscured through encryption to prevent an eavesdropper from inferring users’ patterns of browsing, profiling, service use or extracting identifiers that may be used for future tracking. This assurance is even more necessary in the cloud environment where all service level agreements (SLAs) state that data security is the responsibility of the data owner, not the cloud provider.

Information security techniques should be considered to achieve a logical state of “safe harbour” throughout the entire engineering process beginning at the earliest design stages to the operation of the productive system if possible. Using appropriate techniques such as encryption, data must be persistently protected in all phases of its life, in transit, at rest and overtime.

Data protection is the responsibility of the PACS data owner, not the infrastructure in which the data exists. Data protection must persist and travel with the data object, indifferent to network topography, supporting persistent protection of data regardless of data location, use and reuse.

Information security techniques must be consistent with and address the protection goals of availability, confidentiality and integrity. All of these goals are important from privacy and data protection perspectives that specifically require that unauthorised access and processing are prevented and that also ensure accuracy and protection from manipulation, loss, destruction and damage.

At the same time, however, the organisational and technical processes must be in place to allow appropriate handling of the data and provide the possibility for individuals to exercise their rights while only accessing data when necessary. This principle calls for appropriate technical and organisational safeguards and access management. To achieve information stability, data accountability is required, to ensure, and to be able to demonstrate, compliance with privacy and data protection principles (including legal requirements). This requires clearly defined responsibilities, internal and external auditing and controlling all data processing. In some organisations, data protection officers are installed to demonstrate compliance, perform data protection impact assessments and internal audits and handle complaints.

Data protection providers need to regard the entire life-cycle management of sensitive data from collection, processing, to deletion, systematically focussing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of sensitive data.

The responsible party, which could be a data protection provider, is responsible for carrying out a data protection impact assessment based on published standards (e.g. NIST/ISO/ANSI), and the results referenced when developing those measures and procedures.

6.3.4 Understanding Role-Based Access Control (RBAC)

As suggested earlier, RBAC and Attributre Based Access Control (ABAC) are the common means to enforce the limitation of access and use by the requesting organisation. RBAC is most discussed in applicable standards and supporting reports with the parameters shown in Fig. 6.4. Examples of roles and permissions are identified in the two enumeration blocks. These parameters are specified by the project manager and specified in the digital certificates discussed earlier.

ABAC parameterisation, shown in Fig. 6.5, is equally important but has received less attention in the applicable standards and supporting reports, the exception being IEC 62351-90-19 which gives it proper attention. What ABAC provides to augment RBAC are location, device and time of when the access and use privileges are enabled. Again, ABAC parameters values are set by the project manager.

Details about how RBAC can be implemented are discussed in Sect. 6.4.4.

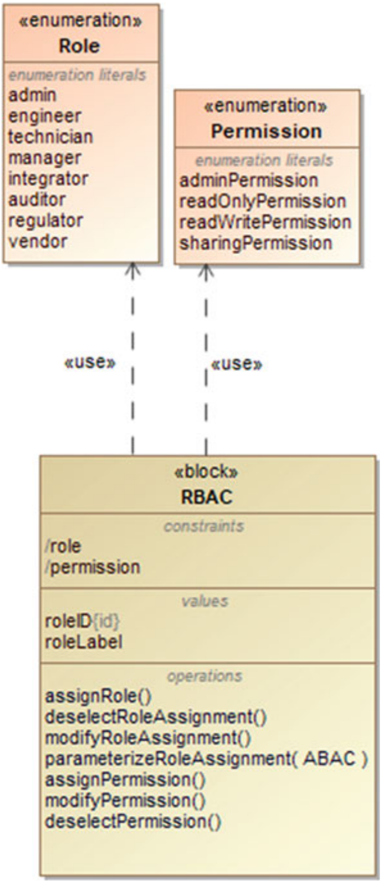


Fig. 6.4 Role-based access control parameterisation

6.3.5 Extended Access Control Mechanisms

Information security techniques must play a central role, and these same information security techniques can also include actions that eliminate old and unnecessary data, thereby preventing unnecessary or unwanted processing of that data, without the loss of the functionality of the information system.

Attribute-based access control (ABAC) enforced by cryptography, at the object level, is an example of an approach that could be implemented to meet these objectives. This object-level ABAC process, (defined by NIST in SP800-162, SP1800, and by ANSI in X9.69 and X9.73 as well as ISO 11568) can achieve the declared objectives.

Protected messages are represented as extensible markup language (XML) markup using the canonical XML encoding rules (cXER) or represented in a binary format that is backward compatible with existing deployed systems. These systems rely on cryptographic message syntax, using the basic encoding rules (BER) or the canonical subset of BER, the distinguished encoding rules (DER).

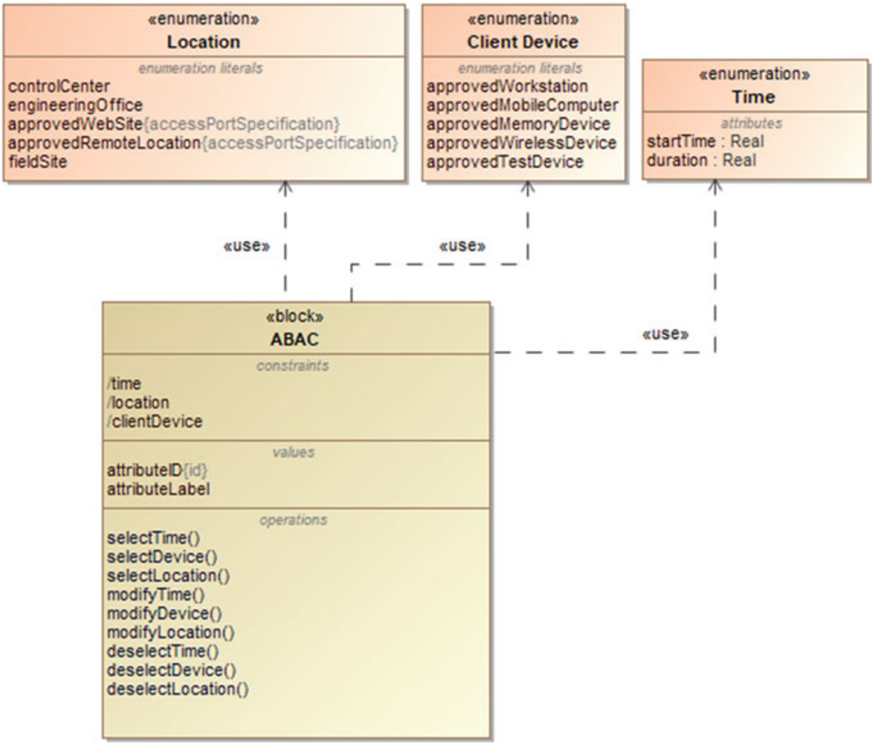


Fig. 6.5 Attribute-based access control parameterisation

Messages and objects are protected independently. There is no cryptographic sequencing (e.g. cipher block chaining) between messages or objects. There need not be any real-time connection between the sender and recipient of the message. This makes the syntax suitable for use over store-and-forward systems.

Standard attributes are defined using an extensible design to allow any organisation with a need to define additional attributes for any purpose. Attributes are defined that allow security assertion markup language (SAML) and XML's key management specification (XKMS) content to be carried in each of the cryptographic types defined in X9.73, supported by the key management defined in X9.69.

The syntax is cryptographic algorithm independent and extensible. It supports the provision of data confidentiality using encryption and tokenisation techniques, data integrity, data origin authentication and non-repudiation services. Any algorithm may be used for message or object encryption, digital signature, signcryption and key management. A variety of key management techniques are supported, including key exchange, key agreement, password-based encryption and constructive key management.

1. Selective field protection can be provided in two ways. First, they can be protected by combining multiple instances of this syntax into a composite message. Second, they can be protected in a single message by using identifier and markup tag names and content-specific manifests that are cryptographically bound to content to select message components. This approach allows reusable message and/or object components to be moved between documents without affecting the validity of the signature.
2. Precise message and object encoding, and detailed cryptographic processing requirements of binary and XML markup message representations are provided.

Simple Object Application Protocol (SOAP) message extensions are defined for each of the cryptographic types defined in X9.73 to enable the protection of financial services information in Web Services environments. The typical application of the enveloped-data content type will represent one or more recipients' digital envelopes on the content of the data or signed-data content types.

6.3.6 Security Requirements for Remote Services

Chapter 14 describes access to PACS network and devices from a remote (outside the substation security perimeter). Several CIGRE technical brochures developed by Study Committees B5 and D2 have addressed the security risks and practical solutions for remote services to mitigate that risk. Figure 6.6 identifies the local laws and regulations that must be satisfied in the PACS-centric policies, procedures and organisation directives (PP&ODs). In turn, the basic CPS objectives for remote services must satisfy the PP&ODs.

This led to the identification of two parts of IEC 62443 that address the issues. Figure 6.7 illustrates the interaction of parts 2–4 requirements imposed on the solution providers, and parts 2–3 identify the need for system segmentation such as the use of a demilitarised zone (DMZ). These are best described in terms of the multiple requirements for access control, use control, data confidentiality, data integrity, restraints on data flows (interfaces), resource availability and timely reporting of events. These CPS requirements should be seamlessly integrated into the remote access services described in Chap. 14.

6.3.7 The Need for Security-Smart PACS Data Objects

IEC 61850 introduced the concept of smart PACS objects. IEC 62351 overlays the cybersecurity requirements onto the IEC 61850 objects. CIGRE Technical Brochure 790 [26] introduced the concept of "security-smart" objects for PACS applications. The basic idea is to use a standards-based specification for secure, self-protecting data objects (SSDO), that are data-label aware with services based on that awareness. When properly implemented, SSDO provides differential access and use control that is independent of network configuration.

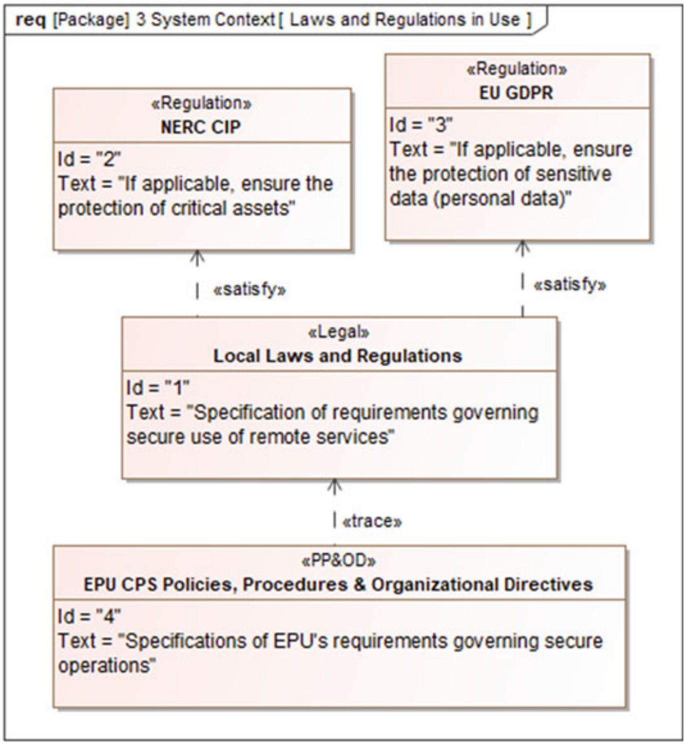

req [Package] 3 System Context [Laws and Regulations in Use]
«Regulation»
NERC CIP
Id = "2"
Text = "If applicable, ensure the protection of critical assets"
«Regulation»
EU GDPR
Id = "3"
Text = "If applicable, ensure the protection of sensitive data (personal data)"
«satisfy»
«satisfy»
«Legal»
Local Laws and Regulations
Id = "1"
Text = "Specification of requirements governing secure use of remote services"
«trace»
«PP&OD»
EPU CPS Policies, Procedures & Organizational Directives
Id = "4"
Text = "Specifications of EPU's requirements governing secure operations"

Fig. 6.6 Local laws and regulations that must be satisfied in a PACS-centric environment

Cryptographic key management for PACS is also comprehensively addressed in the IEC 62351-9 standard “key management”. This part forms a basis for handling keys at the client, server and key generation/distribution and is referenced by other IEC 62351 parts that use key management to address secure process communication (parts 3 through 7) and RBAC (part 8). Digital certificate management is addressed in Sect. 6.3.8.

The good news is commercial solutions are available. However, PACS stakeholders must evaluate and compare different implementations to determine which solution best fits their PACS-centric SSDO protection mechanisms. As a minimum, the evaluation should include the following:

- A well-defined process to designate roles and credentials that are seamlessly integrated with job responsibilities. Specifically, the role is defined by the credentials where each credential represents an attribute of the data described in the underlying information classification model.
- The information classification model should be aligned with local laws and regulations and well-specified in PACS sensitive security policies, procedures and organisational directives.

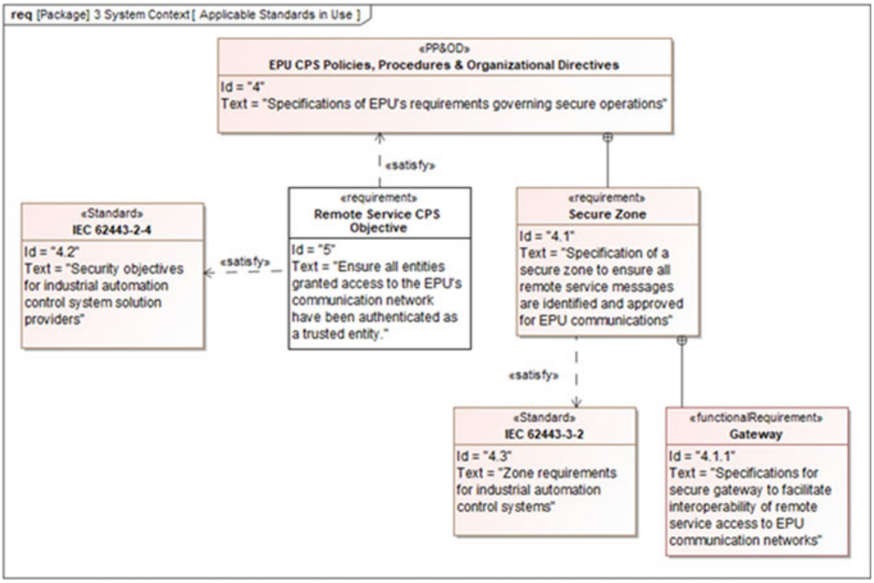

req [Package] 3 System Context [Applicable Standards in Use]
«PP&OD»
EPU CPS Policies, Procedures & Organizational Directives
Id = "4"
Text = "Specifications of EPU's requirements governing secure operations"
«satisfy»
«Standard»
IEC 62443-2-4
Id = "4.2"
Text = "Security objectives for industrial automation control system solution providers"
«satisfy»
«requirement»
Remote Service CPS Objective
Id = "5"
Text = "Ensure all entities granted access to the EPU's communication network have been authenticated as a trusted entity."
«requirement»
Secure Zone
Id = "4.1"
Text = "Specification of a secure zone to ensure all remote service messages are identified and approved for EPU communications"
«satisfy»
«Standard»
IEC 62443-3-2
Id = "4.3"
Text = "Zone requirements for industrial automation control systems"
«functionalRequirement»
Gateway
Id = "4.1.1"
Text = "Specifications for secure gateway to facilitate interoperability of remote service access to EPU communication networks"

Fig. 6.7 IEC 62443 requirements for remote services

- A federated management system to securely generate, distribute, recover and dispose of cryptographic keys and key fragments.
- Unique communication requirements for distribution of keys and digital credentials. The best solutions do not require encrypted communication of keys and digital credentials.
- A trusted certification authority to authenticate digital certificates (credentials) that describe access and use privileges.
- Every authorised user and PACS application must have a digital credential when they issue their first request.
- Solution providers must conform to the standards to ensure consistency between versions released and interoperability between SSDO management systems and embedded solutions in PACS devices. PACS managers should insist that all stakeholders enforce conformance to a well-defined interface control document (ICD).

Secure PACS applications require management of intelligent electronic devices (IEDs) such as network devices and protective relays shown in the SysML-based model, see Fig. 6.8. Of interest in this example are two IED types: network devices and protection and control relays. Management of these devices is the responsibility of an authorised user, e.g. network engineer or technician, or relay engineer or technician. Security requires access control specified in RBAC and ABAC privileges assigned to the authorised user. For this example, the authorised user logs on to an EPU controlled workstation that has the responsibility to verify access

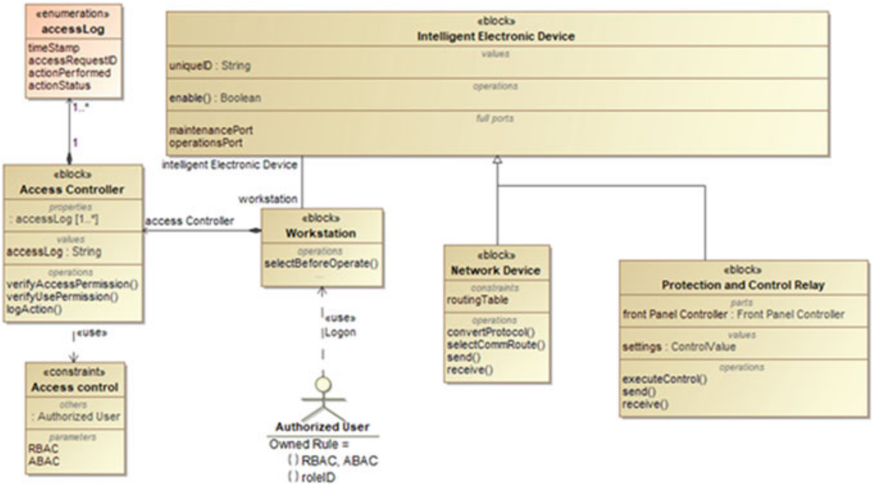


Fig. 6.8 Typical participants in PACS applications

permissions and use permissions. Once verified, the process then proceeds as a select-before-operate sequence of transactions.

6.3.8 Digital Certificate Management

Multiple PACS functions use digital certificates to enable access control (RBAC) and use control privileges (ABAC). IEC 62351-8 and IEC 62351-9 describe the semantics for smart data objects contained in these certificates. An understanding of the life cycle of digital certificates provides the proper context for PACS applications.

Digital certificates including their keying materials can be used to identify and authenticate an entity (human or IED) access authority and use privileges for managing a network device, workstation or a power system device. These privileges include generation, exchange, storage, safeguarding, use, vetting revocation and replacement or renewal of certificates. Successful digital certificate management is critical to the secure use of certificates to provide protection and control data confidentiality and in some cases data integrity.

Figure 6.9 is an overview of the certificate life cycle. Elements of the process are labelled to facilitate cross-referencing and to help identify the logical sequence flows. A "+" symbol is used to note that a task may be complex and require multiple iterations and coordination between stakeholders. The dashed connector is used to identify a data association. The red association connector is used to highlight specific actions required to update or revoke a digital certificate.

In summary, the management of these certificates requires the following capabilities.

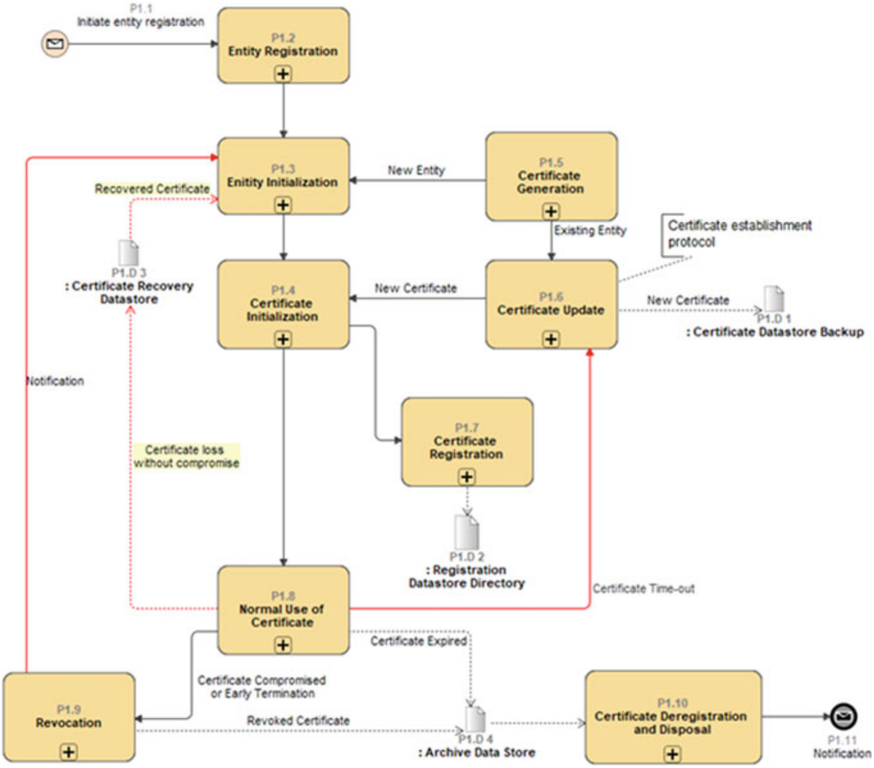


Fig. 6.9 Overview of the digital certificate life cycle

- The digital certificate management system shall provide the capability to generate and distribute digital certificates that maintain the secret values on time to support operations. Note: timeliness requirements imposed by critical operations that require high security determine the means to distribute the digital certificates.
- The certificate management system shall prove the capability to periodically update the digital certificates. Note: the period for certificate use varies based on the need to limit an entity's time of access and use. For some situations, a persistent digital certificate is appropriate with no time-out specified.
- The certificate management system shall provide a secure means to maintain the digital certificates to support certificate recovery when the certificate management system fails and becomes disconnected, or the certificate is lost but not compromised.
- When applicable, the certificate management system shall encrypt the certificate data from end to end, so it is protected when at rest or in transit. Note: security through encryption needs to be efficient and transparent to some operation

functions, e.g. protection and control. Other functions may not need encryption, e.g. sample data streaming.

- The certificate management system shall provide the capability to revoke a digital certificate if it is compromised or its time of effectiveness expires.

6.3.9 Leveraging Self-Protecting Data Objects

Leveraging the SSDO capabilities requires modification to existing components of the protection and control IED. The example shown in Fig. 6.10 identifies three subsystems of the protection and control relay that require consideration: data handling subsystem, P&C logic subsystem and P&C data management subsystem. The new participant is the crypto-content management subsystem, which is logically part of the data handling subsystem. To perform its encryption and decryption function, the crypto-management subsystem needs access to information owned by the P&C data management subsystem, which in turn needs access to data owned by the P&C logic subsystem.

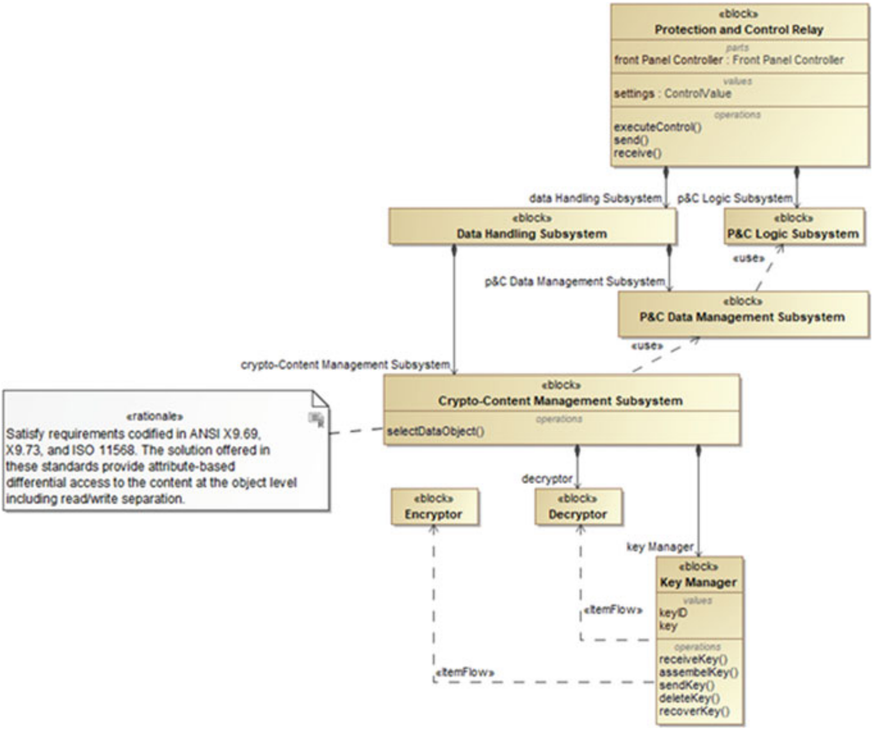

«block»
Protection and Control Relay
parts
front Panel Controller : Front Panel Controller
values
settings : ControlValue
operations
executeControl()
send()
receive()
data Handling Subsystem
p&C Logic Subsystem
«block»
Data Handling Subsystem
«block»
P&C Logic Subsystem
«use»
p&C Data Management Subsystem
«block»
P&C Data Management Subsystem
«use»
crypto-Content Management Subsystem
«rationale»
Satisfy requirements codified in ANSI X9.69, X9.73, and ISO 11568. The solution offered in these standards provide attribute-based differential access to the content at the object level including read/write separation.
«block»
Crypto-Content Management Subsystem
operations
selectDataObject()
decryptor
«block»
Encryptor
«block»
Decryptor
key Manager
«block»
Key Manager
values
keyID
key
operations
receiveKey()
assembelKey()
sendKey()
deleteKey()
recoverKey()
«itemFlow»
«itemFlow»

Fig. 6.10 SSDO participants in PACS applications

Part of the crypto-management subsystem is the key manager that is responsible for receiving keys (or key fragments, assembling keys from key fragments and sending the keys to the encryptors and decryptors. In addition, the key manager is responsible for the secure deletion of keys and key recovery.

Control of keys is critical because in a PACS environment multiple parties are likely to have the same key pairs. It is a better design to have dynamic certificates that can be rekeyed. Furthermore, this key management scheme requires that connectivity be ensured.

6.3.9.1 A Means to Improve Front Panel Access Control

Figure 6.11 focuses attention on local access to the front panel of the protective relay. An access controller (a part of the front panel controller) provides the capability to verify access permission and verify use permission, time stamps the action and logs the status of the request (0: denied, 1: approved).

Local access to changing settings on a protective relay front panel needs attention. One approach is to use a radio-frequency identification (RFID) smart card enabled with access and use control privileges to gain local access to the protective relay. To implement defence-in-depth, the RFID smart card could be used to

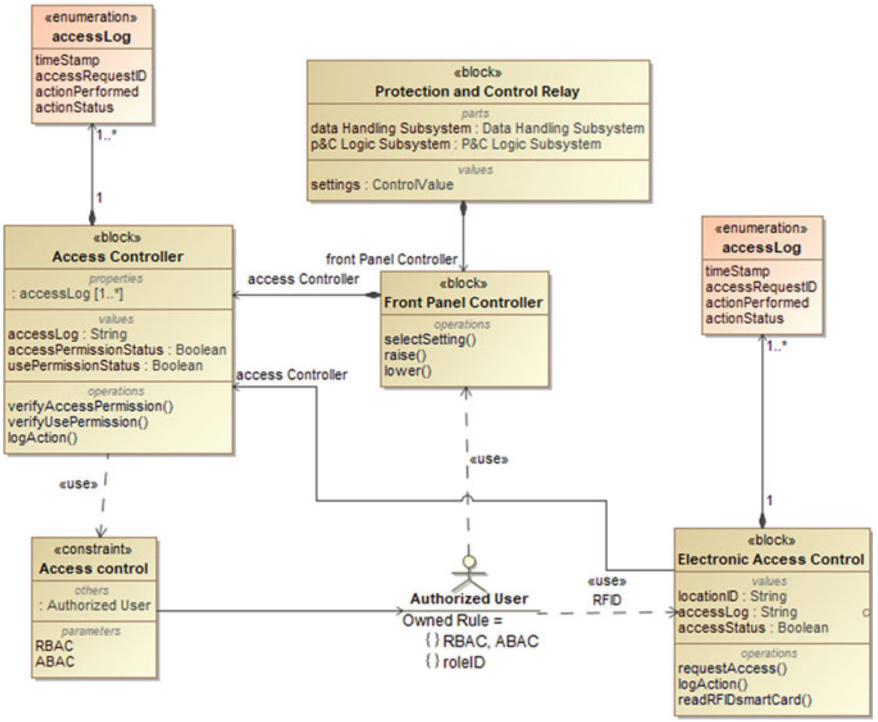


Fig. 6.11 Local access control to change settings

gain access to the substation yard, access to the substation house, access to the substation cabinet and access to the front panel reads of a protective relay. In each case, the block electronic access control in Fig. 6.11 reads the RFID smart card with the access request information and logs the action. Each instance of the read action is time-stamped and includes the location (substation yard gate, substation house, substation cabinet and protective relay front panel) and logs the access status (0: denied, 1: approved).

Another approach is to have the IED/relay authenticate the user with a numeric ID and passcode, both of which are centrally managed in a RADIUS/LDAP server with centrally enforced account management policies. This approach also works with existing IEDs where a numeric keypad and a screen are available on the front panel and does not increase the attack surface by, e.g. introducing a new RFID interface.

6.4 Security Implementation in R-SV and R-GOOSE

6.4.1 Message Security

In today's utility environment, wide area secure communication is a requirement. The ability to secure R-SV (Routable Sampled Values), R-GOOSE, GOOSE and SV is defined in the IEC 61850 and IEC 62351 standards (appropriate parts). The security goals that were identified are as follows:

- Ability to provide Information authentication and integrity (e.g. the ability to provide tamper detection). The use of authentication is required for operational systems.
- Figure 6.12 Confidentiality (via encryption) in R-GOOSE and R-SV is optional.

Message authentication is achieved through the calculation and inclusion of a secure Hash (Message Authentication Code—MAC) that is computed using data from the entire message except for the part of the message that contains the MAC (Fig. 6.13). This signature is referred to as a Message Authentication Code or MAC, and given that a Hash algorithm is used, the term Hashed Message Authentication Code or HMAC is used. A Hash is an amalgam of all bytes that make up the message and is combined with a secret key to encrypt the Hash.

Since the IEC 61850 messages can be sent to many receivers, all members of the publish-subscribe group must be able to encode and decode a message. To implement this functionality, a Symmetric Key is used and is distributed to all members of the publish-subscribe security group. A key is a large number—typically 16 to 32 bytes long (directed by policy) and is generated with cyber randomness (e.g. normal random functions do not have enough entropy to satisfy this requirement). The secure distribution of the Symmetric Key is performed by a function/device known as a Key Distribution Centre (KDC). Distribution over the wire to members of the security group is performed by a protocol known

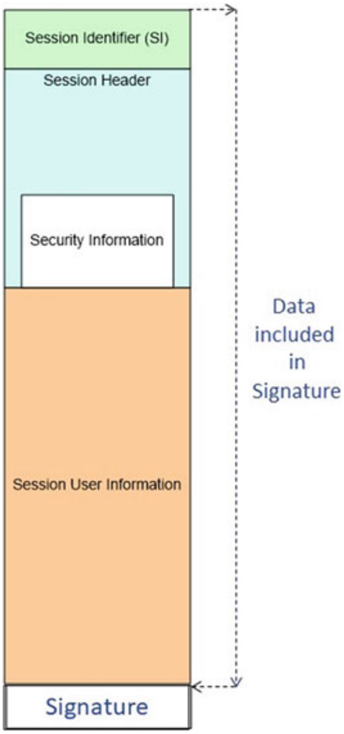
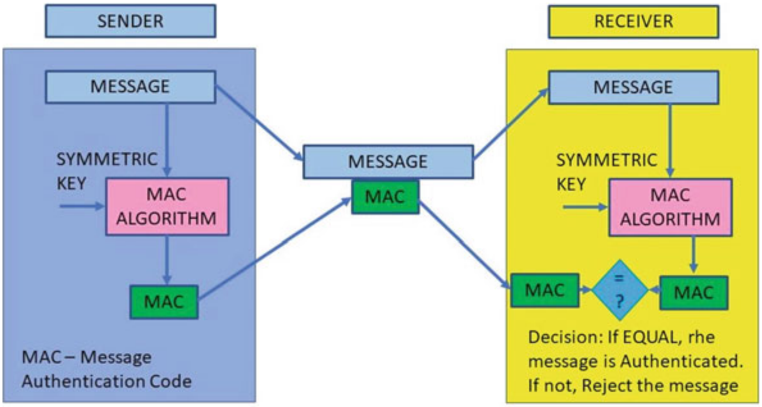


Fig. 6.12 R-SV and R-GOOSE message structure


SENDER
MESSAGE
SYMMETRIC KEY
MAC ALGORITHM
MAC
MAC – Message Authentication Code
MESSAGE
MAC
RECEIVER
MESSAGE
SYMMETRIC KEY
MAC ALGORITHM
MAC
= ?
MAC
Decision: If EQUAL, rhe message is Authenticated. If not, Reject the message

Also known as a Hash based Message Authentication Code – **HMAC**
Also called a Message Integrity Code - **MIC**

Fig. 6.13 Message authentication process

as the Group Domain Of Interpretation (GDOI) as defined in IEC 62351-9 [13] which refers to several Internet Request For Comments (RFCs) including RFC 6407 [27]. The same Symmetric Key is used to compute the message signature and to encrypt the message. If encryption is selected by policy (set in the KDC), only the payload of the message is encrypted. Further details regarding the KDC follow in this section. The message authentication "Hash" is appended to the end of the published message (see Fig. 6.12). Upon receipt, the subscriber re-computes the message Hash using the same algorithm and key. If the received Hash is the same as the re-computed Hash, the message is declared to be authenticated (see Fig. 6.13).

As with all GOOSE communication exchanges, the exchange is configured in the SCD or publisher's CID file (note: a device may belong to multiple groups). IEC 61850-6 also has elements that allow the KDC(s) to be defined and allows configuration of which KDCs an IED/Application should communicate with to receive keys and policies. In addition, subscribers can identify their publisher's source and destination address. This allows anti-replay to be implemented per IEC 62351-6.

6.4.2 Key Distribution Centre—KDC

As noted above, implementation of security on R-GOOSE, R-SV, GOOSE and SV requires that asymmetric key be distributed to all members of a publish-subscribe group, also known as a security group. Membership in a security group is usually defined by the Substation Configuration Description (SCD) file. Members of a security group and the KDC must be provisioned X.509 identity certificates and can validate other X.509 identity certificates from one or more X.509 certificate authorities. On the start-up of the KDC, the identity certificates are exchanged and authenticated by both the group members and the KDC. If the identity of the Group Member is authenticated, and it has been granted rights to obtain the keys and policies, the KDC will deliver these to the Group Member. The Symmetric Key is delivered to the members of the security group through a protocol, as noted above, known as the Group Domain of Interpretation (GDOI). As an example, in the case of an SV message, the security group includes the publishing merging unit (MU) and all subscribers to the MU's dataset. It should be noted that all security implementations are based on existing Internet standards and RFCs (albeit, one was created to meet 61850 needs). The KDC is also responsible for the periodic re-keying (re-key time is user selectable) of all members of a security group. Keys should be periodically changed as the longer a key is in use, the higher the probability (albeit still small) of the key is cracked.

Note: PKI provides policies, and procedures needed to create, manage, distribute, use, store and revoke identity digital certificates. These include the following:

- The ability to request identity and certificate authority X.509 certificates through the use of Simple Certificate Enrolment Protocol (SCEP) or Enrolment of Secure Transport (EST).
- The ability to determine if an X.509 certificate has been revoked through the use of the Online Certificate Status Protocol (OCSP).

Symmetric Key Delivery, through GDOI, can be performed by the KDC via two different mechanisms known as PUSH and PULL. In both modes, there are two sets of keys/policies delivered to be utilised by the exchange of GOOSE, R-GOOSE, SV or R-SV. These are known as Traffic Encryption Key (TEK) payload. This set is provided in order to provide cybersecurity for two key rotation periods even if KDCs are offline. Additionally, the key/policy to be used to protect the PUSH is exchanged. This is known as the Key Encryption Key (KEK) payload. In PULL mode, a Group Member PULLs or requests a key from the KDC. Before a key is delivered, the KDC validates the certificate of the requesting Group Member. Group members must execute a PULL request on start-up to request keys to synchronise key usage or to address lost keys when a PUSH is not able to be received or authenticated. When PUSH is set by policy in the KDC, the KDC sends or pushes a new key to the Group members.

When the KDC policy is set to PUSH, keys to the Group Members are sent from the KDC to the security group members. In this mode of operation, the group member can acknowledge receipt of a key to the KDC (set via policy). In the re-keying process, events on the grid may inhibit the delivery of a new key. When security is implemented on functions such as transfer trip and remedial action, failure to deliver a new key must not be known to inhibit the operation of the function. To address this scenario, a policy is known as Key Delivery Assurance (KDA—specified in IEC 62351-9) can be utilised. With KDA enabled, the KDC can ascertain if key delivery attempts to a user-set percentage of the group members (policy set in the KDC) are reached, and permission to change keys to the publisher is inhibited. Alternatively, if key delivery to the user-set number of group members is successful, a KDA message is sent to the publisher of the group which allows the publisher to change keys at the specified time. KDA should only be utilised if the publisher supports PUSH; otherwise, the operational integrity of KDA is questionable.

The recommended rotational period is twenty-four hours. With two keys being delivered at one time, there are enough keys delivered to allow key rotation (e.g. between the two keys) for forty-eight (48) hours even without KDA.

The KDC function should be extensible to meet the needs of most any size domain of management including, but not limited to, enterprise, control centres, substations, generation facilities, distributed energy resources (DER), distribution networks and home meter communications.

Recently, IEC 62351-9 has been extended to provide key management for Precision Time Protocol as specified in IEEE 1588:2019 and the emerging power profiles IEC/IEEE 61850-9-3 and IEEE C37.238.

6.4.3 IEC 61850 Client–Server Security

In client–server security, a “secure” message transfer is to be established between a function like a SCADA Master and the “server” or SCADA remote in the field. IEC 62351-6 allows several different combinations of transport-level and application-level security—two of which are shown in Fig. 6.14.

There are differences between Information Technology (IT) and Operational Technology (OT) cybersecurity priorities. OT Security concentrates on availability, integrity and confidentiality (AIC). Authentication is becoming more important so AICA (adds authentication) is becoming more important. The selection of the appropriate options for each client/server security profile is policy decisions to achieve the identified utility security policies.

The IEC 62351-4 security profile requires the use of Transport Layer Security (TLS) to provide confidentiality and integrity. Mutual authentication of the connecting nodes is also performed within the context of TLS. Application-level authentication is provided through the exchange of PKI certificates within the application layer.

IED 62351-4 end-to-end (E2E) security can provide confidentiality, integrity and authentication within the application layer depending upon the negotiated policies. This means that the use of TLS is optional for this security profile.

Authorisation is achieved through local means. As of this writing, the Role-Based Access Control (RBAC) configuration mechanism for IEC 61850 is still under development (e.g. IEC TR 61850-90-19).

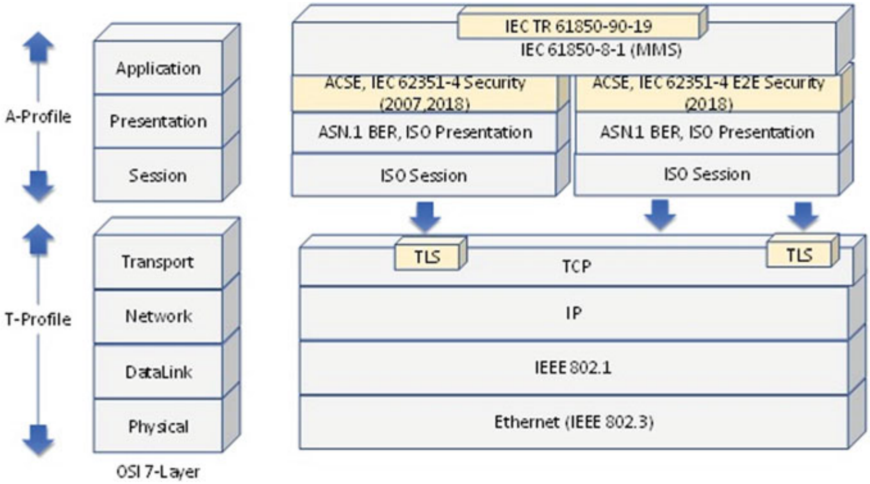


Fig. 6.14 TLS security options in IEC 61850

6.4.4 Role-Based Access Control—RBAC

As explained in Sect. 6.3.4, RBAC is a security mechanism that restricts user access to a system at a level needed to achieve a specific function. IEC TR 61850-90-19 leverages the RBAC constructs outlined in IEC 62351-8. Within IEC TR 61850-90-19, it is possible to grant/deny access to IEC 61850 services as well as access to IEC 61850 objects, including but not limited to Logical Nodes, data objects (DOs) and Functionally Constrained Data Attributes (FCDAs). Access control can also include conditions based upon IEC 61850 object values or Areas of Responsibilities (AORs). AORs can be geographical areas, IED mode based (e.g. local and remote) and other constructs. AORs and roles can be embedded in an identity certificate or via the preferred mechanism of a digital attribute certificate.

There are predefined role vs right bindings that can be found in IEC 62351-8. IEC 62351-8 also specifies how to create custom role vs right binding. IEC TR 61850-90-19 goes beyond IEC 62351-8 and allows the specification of rights to permit/deny access to specific IEC 61850 objects and services. The object permissions can be based upon a wildcard, Logical Node, Functionally Constrained Data (FCD) or Functionally Constrained Data Attribute (FCDA) down to the lowest definition in a data object. There is also a mechanism to utilise values to control security configuration as may be required for environmental emergency conditions (e.g. fire or earthquake) where normal security restrictions are relaxed to allow service restoration (shown as the stoplight in the Fig. 6.15).

The RBAC abstract model is serialised into a subset of the eXtensible Access Control Markup Language (XACML) per https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf. The support of XACML is anticipated

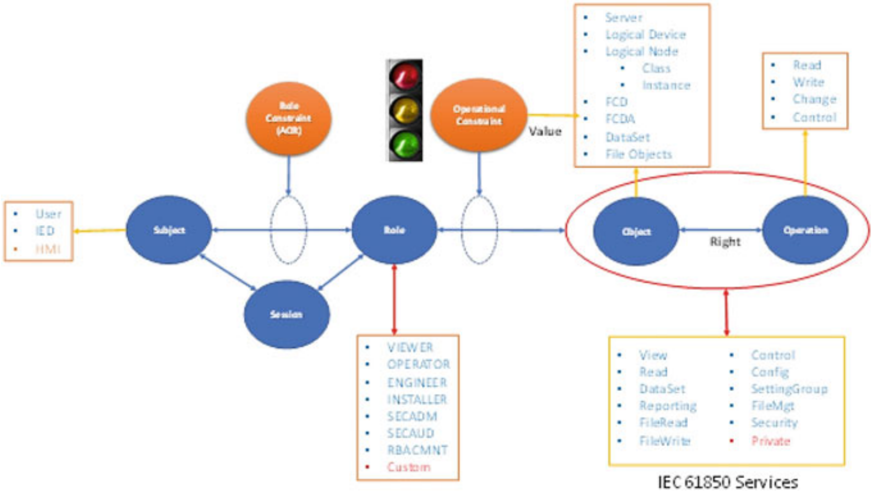


Fig. 6.15 RBAC concept

to be mandatory with the second serialisation being based upon an IEC TR 61850-90-19-specific XML Schema Language (XSD). The resulting serialisations result in an XML file that must be transferred securely to the Point of Enforcement (POE) such as an intelligent electronic device (IED).

6.5 Conclusions (Call to Action)

6.5.1 Top 6 CPS Actions to Protect IEC 61850 PACS

- It is imperative that CPS requirements be baked into every process of the IEC 61850 life cycle. This includes the supply chain of all components included in the solution (for example, see U.S. Executive Order 13920, effective January 16, 2021). It also includes each stage of configuring and testing at the component, subsystem and systems levels. Last is the need to address CPS requirements for decommissioning and disposal activities.
- Deploy software- or hardware-based collectors to ingest network traffic, log data, PACS asset and user metadata to learn the behaviours of PACS network while identifying and classifying the consequence of an APT on your system.
- Provide PACS-related organisations with advanced analytical tools to discover and prioritise anomalous behaviours through a combination of machine learning and deep learning algorithms.
- Provide visualisation mapping to understand a time-based narration of how an APT is evolving in your PACS network and to enable the protection engineers to drill down into the details of the threat.
- Integrate cybersecurity orchestration and incident management tools to provide semi-automatic or fully automatic response and remediation.
- Tools needed to configure security policies, perform testing and collect data need to be vetted to ensure they do not expose the PACS assets and networks to cyberattack, see [6].

6.5.2 Future Study Topics and Objectives

Study committees B5 and D2 need new cooperative, or joint working groups, to identify and assess emerging cyber-physical security issues related to IEC 61850 systems. These assessments should address the full life cycle of the design, development and qualification of systems, subsystems and components that comprise an IEC 61850 system deployed and operated in a live environment. For example, these studies should address migration solutions to update IEC 61850 systems in use. Following are the high-priority topics.

- Emerging laws and regulations, such as the general data protection regulation (GDPR) or variations of the GDPR defined by the local authorities. These requirements and constraints should be applied to all IEC 61850 sensitive data, such as IED settings, configuration tools and testing tools.

- Emerging NERC CIP requirements should be addressed in all future studies. There will be a need to reconcile the NERC CIP emerging requirements and the emerging laws and regulations.
- Digital certificate management schemes, including but not limited to IEC 62351's approach, should be addressed to better understand both client-side and server-side certificate management mechanisms in IEC 61850 systems for various authentication, encryption and secure communication protocols. Cross-signing by multi-utility and supporting organisation certificate authorities (CAs) also needs attention to avoid abuse.
- Software-defined measures, the networking (SDN) and network function virtualisation (NFV) are emerging technologies for IEC 61850 systems (see Chap. 11). An assessment of SDN/NFV implementation and lessons learned from early deployments is needed to identify the potential improvements in cybersecurity protection. NFV brings into play the potential of virtualising selected IEC 61850 functions. Such an approach needs further study to identify CPS risks and viable solutions to mitigate those risks.
- More work is needed to identify a measure of effectiveness (MoEs) and metrics for various CPS maturity schemes. Specifically, assessment needs to identify costs, benefits and challenges to implement and manage each candidate maturity scheme in an IEC 61850 operating environment.

References

1. Industrial communication networks—Network and system security—Part 3-3: System security requirements and security assurance levels, Standard 62443/FDIS-3-3 (ISA-99.03.03), TC65WG10, January 2013
2. Cherkashin, V., Feifer, G.: Spy Handler: A Memoir of a KGB Officer: The True Story of the Man Who Recruited Robert Hanssen and Aldrich Ames. Basic Books (2008)
3. Livingston, S., Sanborn, S., Slaughter, A., Zonneveld, P.: Managing cyber risk in the electric power sector. Deloitte. As of 17 (2019) [Online]. Available: https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/cyber-risk-electric-power-sector.html
4. CIGRE WG D2.38: TB 698—framework for EPU operators to manage the response to a cyber-initiated threat to their critical infrastructure. CIGRE, Technical Brochure #698 (2017) [Online]. Available: https://e-cigre.org/home.asp
5. CIGRE WG D2.46.: TB 796—cybersecurity: future threats and impact on electric power utility organisations and operations. CIGRE Study Committee D2, CIGRE, 21, rue d'Artois, 75008 Paris, FRANCE, Technical Brochure 796 (2020) [Online]. Available: https://e-cigre.org/home.asp
6. CIGRE WG B5.38.: TB 427—the impact of implementing cybersecurity requirements using IEC 61850. Technical Brochure #427 (2010) [Online]. Available: https://e-cigre.org/home.asp
7. Schwartz, H.A.: Significant cyber incidents since 2006. Center Strateg. Int. Stud. (2020) [Online]. Available: https://csis-website-prod.s3.amazonaws.com/s3fs-public/200626_Cyber_Events.pdf

8. TC65WG10.: Security for industrial automation and control systems—network and system security—Part 2-3: patch management in the IACS environment. Int. Electrotech. Comm. Draft Tech. Rep. IEC/DTR 62443-2-3 (ISA-99.02.03), 2014-01-07
9. IEC 62443-2-4: 2015 Industrial communication networks—network and system security—part 2-4: security program requirements for IACS service providers, Standard, IEC 62443-2-4: 2015, TC65WG10, Geneva CH, 2015–06–30
10. IEC 62351-3 + AMD1: 2018—Power systems management and associated information exchange: data and communication security—Part 3: profiles including TCP/IP, IEC 62351-3 + AMD1: 2018, TC57WG15 (2014)
11. IEC 62351-4: 2018—Power systems management and associated information exchange: data and communication security—Part 4: profiles including MMS and derivatives, Standard IEC 62351-4, TC57WG15 (2018)
12. IEC 62351-6: 2007—Power systems management and associated information exchange: data and communication security—Part6: security for IEC 61850 (note: new edition under development). Standard IEC 62351-6, TC57WG15 (2007)
13. IEC 62351-9:2017—Power systems management and associated information exchange—data and communications security—Part 9: cyber security key management for power system equipment. Standard IEC 62351-9: 2017, TC57WG15 (2017) [Online]. Available: https://webstore.iec.ch/publication/30287
14. IEC 62351-8: 2011—Power systems management and associated information exchange: data and communication security—role-based access control (note: new edition under development). Standard IEC 62351-8: 2011, TC57WG15 (2011)
15. CMMI_Institute.: CMMI v2.0: online capability maturity platform accelerates speed to performance, resiliency, and scale (2019)
16. Stevens, J.: Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)(Case Study). DTIC Document (2014) [Online]. Available: http://www.energy.gov/oe/services/cybersecurity/electricity-subsector-cybersecurity-capability-maturity-model-es-c2m2
17. Johnson, J.T.: Cybersecurity by the numbers: maturity metrics of successful security organisations. Presented at the SAI education at ISC, Las Vegas NV, 9 April 2019, Presentation (2019)
18. Suh-Lee, A.A.C., Rasche, G., Wakefield, M.: Cyber Security Metrics for the Electric Sector, vol. 3.0. Electric Power Research Institute (2017) [Online]. Available: https://www.epri.com/#/pages/product/3002010426/?lang=en-US
19. Zhou, X., Xu, Z., Wang, L., Chen, K., Chen, C., Zhang, W.: Kill chain for industrial control system. In: MATEC Web of Conferences, vol. 173, p. 01013. EDP Sciences (2018)
20. Hussain, S.S., Ustun, T.S., Kalam, A.: A review of IEC 62351 security mechanisms for IEC 61850 message exchanges. IEEE Trans. Ind. Inf. (2019) [Online]. Available: https://www.researchgate.net/
21. Holstein, D.: Logical node implementation of cybersecurity in IEC61850 PAC assets and networks. In: Mark Adamiak, R.M., Falk, H., Cease, T.W. (eds.) PACS Use Cases of Actual Implementations of Cybersecurity in the Logical Nodes and Lessons Learned from these Implementations. Email exchange (2020)
22. Kanabar, M., Cioraca, A., Johnson, A.: Wide-area protection and control using high-speed and secured routable goose mechanism. In: 2016 69th Annual Conference for Protective Relay Engineers (CPRE): IEEE, pp. 1–6 (2016) [Online]. Available: http://ieeexplore.ieee.org
23. Triangle_Microworks.: Simplifying Secure Routable GOOSE & Sampled Values. 2020–07–30 Webinar
24. Hutchins, E.M., Cloppert, M.J., Amin, R.M.: Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Lead. Issues Inf. Warfare Secur. Res. Tech. **1**(1), 13 (2011) [Online]. Available: https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf
25. CIGRE WG D2.40.: TB 762—remote service security requirement objectives. CIGRE, Technical Brochure 762 (2019) [Online]. Available: https://e-cigre.org/home.asp

26. CIGRE WG B5.66.: TB 790—Cybersecurity requirements for PACS and the resilience of PAC architectures. CIGRE, Technical Brochure (2020) [Online]. Available: https://e-cigre.org/publication/790-cybersecurity-requirements-for-pacs-and-the-resilience-of-pac-architectures
27. RFC 6407 Group Domain of Interpretation
28. Aleksandraviciene, A., Morkevicius, A.: MagicGrid Book of Knowledge. Vitae Litera, UAB, Kaunas, Lithuania, p. 170 (2018)
29. Industrial communication networks—network and system security—Part 3-2: security levels for zones and conduits, standard 62443/CD-3-2 (ISA-99.03.02), TC65WG10 (2013)
30. CIGRE JWG B5/D2.46.: TB 603—APplication and management of cybersecurity measures for protection and control. Technical Brochure #603 (2014) [Online]. Available: https://e-cigre.org/home.asp
31. Weis, B., Rowles, S., Hardjono, T.: The group domain of interpretation. Internet Req. Comm. **6407** (2011) [Online]. Available: https://tools.ietf.org/html/rfc6407

Planning and Design for IEC 61850 Implementation

7

Pablo Humeres Flores

Abstract

Designing is the first step in the road to get a protection, automation and control system based on any technology. Planning will be the process to make it happen, from requesting materials and devices to commissioning. In order to really take advantage of the benefits that IEC 61850 offers, the deployment process must start correctly. This chapter presents the various steps of this process, the requirements that must be defined, the impacts caused by the changes and the strategies to be followed.

Keywords

PAC system • Design • Technology • IEC 61850 • Impacts

7.1 Planning to Implement an IEC 61850 Solution

The protection, automation and control systems have been impacted by a significant technological evolution in the recent years, involving not only the increase in the processing capacity of Intelligent Electronic Devices (IEDs), but also the possibility of intensive and safe use of communication networks, to exchange data between these devices in order to improve the performance of the implemented functions.

The requirements for the protection, automation and control system (PACS) will be defined considering the application levels (Station and Process Level) to be implemented and the IEC 61850 models and services. This will define the signals sent by communication or wired between the primary equipment and the

P. Humeres Flores (✉)
CGT Eletrosul, Florianopolis, Brazil
e-mail: hpablo@cgteletrosul.gov.br

P. Bishop and N.-K. C. Nair (eds.), *IEC 61850 Principles and Applications to Electric Power Systems*, CIGRE Green Books, https://doi.org/10.1007/978-3-031-24567-1_7

protection and control devices, and between the IEDs. In addition, taken into consideration the PACs functionalities the necessary performance will be defined, together with the logical and physical Ethernet network infrastructure for the acquisition of status, measurement and control signals. All of them must be defined from the primary equipment in the substation yard to the local SCADA system (human–machine interface—HMI) and Remote Operation Centres.

When a company is planning a solution based on the IEC 61850 standard, it is important to observe the impacts that this will have on the entire installation project. If this complete vision does not exist, there will not be benefits of the advantages that the standard offers in the implantation, maintenance and operation of a substation.

The evolution of the applications of the standard in recent years has consolidated its use in the Station Level, affecting especially the control room. The application of the Process Level will impact the substation yard, the primary equipment and the entire infrastructure for the control room.

In fact, the decision to apply a solution based on the IEC 61850 standard must be taken at the beginning of the project and must have the contribution of all areas and aspects involved: civil, electrical, protection and automation, commissioning, maintenance, asset management and operation.

The decision to apply a disruptive technology involves adapting the entire organisation and processes. It means investment in qualification, training, new software tools, new ways of producing documentation and organisational changes.

7.1.1 Impacts on Yard Equipment and Control Room

The application of the standard has a significant impact on the infrastructure of the control room and the yard. The evolution of IEDs' processing and communication capacity allows us to apply different alternatives of architecture, redundancy and multifunction application.

IEC 61850 provides a self-descriptive (semantic) data model with the meaning in the structure. Contrary to legacy protocols like IEC 60870-5-101 and DNP3, the information is structure in a logical way, using names and classifying the data in objects and sub-objects, detailing the information at a level not possible in its predecessors. This structure required a device's operating system redesign and more processing power.

All communication between IEDs and yard equipment and also between them is based on an Ethernet infrastructure, requiring that the different devices have the functionalities defined in the design of the communication system, which includes the redundancy and network restoration mechanisms, time synchronisation and data protocols (MMS, GOOSE, Sampled Values).

The migration of protection and control functions to a digital environment also allows for the possibility of virtualisation and of applying concepts of centralised control units on a single computer and no longer necessarily in specific boxes. This has a tremendous impact on the control room, which will have fewer devices, less electrical wiring and a safer environment with no current circuits coming from the yard.

Control rooms and cable supports around the station should consider the requirements for installing fibre optic cables. In the control rooms, structured cabling techniques will be applied, specially adapted to electrical substations or industrial systems. The type of network architecture design determines the cabling application to be implemented.

In the yard, the evolution of equipment that makes the function of converting measurements and states into communication signals Sampled Value and GOOSE can be either dedicated equipment such as in the case of Stand-Alone Merging Units (SAMU) or Low Power Instrument Transformers (LPIT), which directly convert optical signals into publications on the Ethernet network.

The development of LPIT has a decisive impact on the substation yard, since its weight and dimension allow for much lighter foundations or even its fixation directly on other primary equipment. In addition, they do not suffer saturation in measurement as in conventional instruments, allowing their application for measurement and protection purposes simultaneously. The Merging Unit that converts the optical signal into a Sampled Value (SV) publication can be installed close to the instrument or inside the control room.

Switching devices, such as circuit breakers and disconnectors, will incorporate electronic devices with communication to publish states and receive commands, maintaining only wired circuits for electrically driving motors to move rods, reload springs, compressing air or gas, etc.

Power transformers and reactors are the types of devices that are especially convenient for incorporating electronic devices in their projects, reporting data of operating conditions and receiving commands and forming an information system to define maintenance actions.

All electronics incorporated in yard equipment must be designed to withstand aggressive environments, such as temperature and high level of electromagnetic influence. They must also have a high performance in converting states and measures and publishing without introducing communication delays.

7.1.2 Impacts on the Utilities

The technological evolution of protection, automation and control systems, migrating from electromechanical solutions to digital technology, has significantly changed its implementation process. The procedures for the design, operation, maintenance, testing and management of life cycle systems impacted the professional profile, the organisational structure, the technological resources and the tools applied in all stages.

The utilities are organised in a segmented structure, separating protection, control, communication and telecommunication specialists in different areas of the company. Activities are organised at different process levels, with specific responsibilities for each one: specific field teams from each knowledge area and centralised engineering teams for support and analysis. The new projects were developed by the engineering teams independently, connecting in the last stage with the equipment in operation.

The evolution of the systems to an IEC 61850 solution with distributed IEDs and Ethernet communication changed the functionality of the devices and the boundaries of each team. It is no longer possible to perform routines in a segregated manner. This challenges the teams to understand and apply the principles of local communication: network, computers, communication protocols, routers, time synchronisation and, at the same time, continue with the knowledge of protection, control and supervision.

The strategy adopted by the companies is the adequacy of processes, the integration of teams and the definition of activities and knowledge at different levels. What is also needed is the modernisation of tools for document management, software and databases applications and the implementation of monitoring systems. Another fundamental aspect was the implementation of a remote access infrastructure to allow immediate support from specialists, optimising costs and availability.

In any case, for all these teams, two actions are essential: qualification and adequate work tools. This means conceptual understanding of an IEC 61850 system and training in the specific configuration and diagnostic tools. Software tools must be defined in line with the level of technology implemented. In addition, they have to be in accordance with the specialty and responsibility of each team.

The principles have been applied in stages, consolidating technologies and features. The teams perform increasingly integrated work with experts giving each other support and basic knowledge of all areas of control, protection and supervision.

7.2 Designing an IEC-61850-Based Solution

The functional requirements of a PAC system are not only related to the type of technology applied for its operation. It starts with the definition of the control, protection and supervision functions. In addition, regulatory requirements determine the concession and operating conditions of the electric power system. A technical specification must describe the functionalities, the infrastructure and the connection with the primary equipment. When we decide for an IEC 61850-based implementation, the main difference is the form of the description of the requirements, based on a descriptive SCL language, and the acquisition of signals that occurs with communication protocols (horizontal and vertical) between the control house and/or with yard equipment. Refer to Fig. 7.1.

In the other chapters of the book, specific aspects necessary for the design of an IEC 61850 implementation are detailed. Chapter 3 presents the specification standards for defining the functions (process interface, protection, control, automation, monitoring, recording, reporting and communications) as well as the specification process (standard scheme), specification tools and documentation. Chapter 4

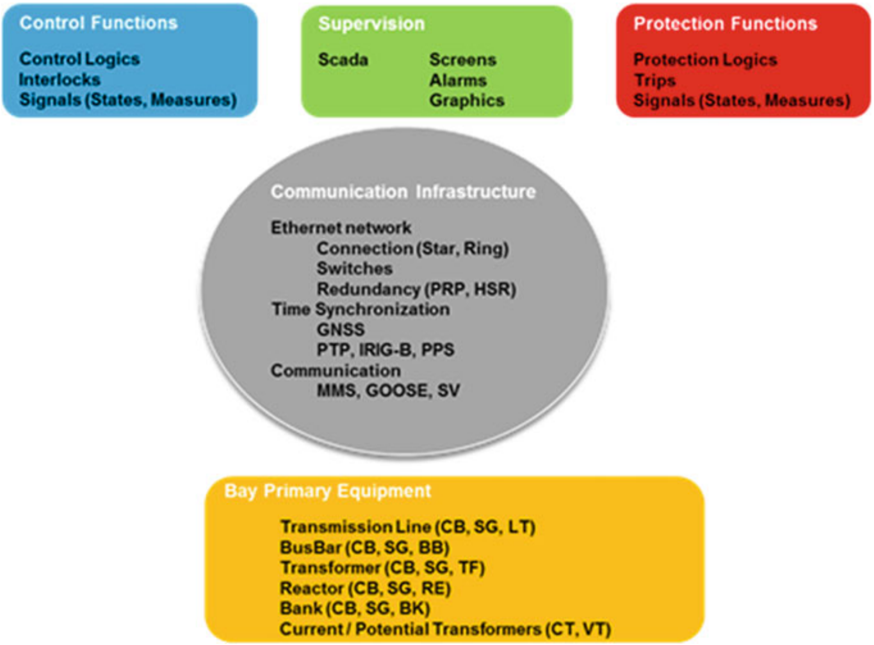


Fig. 7.1 IEC 61850 system application [1]

presents the communication architecture and services issues, which must also be considered and defined in the project. In Chapter 5, we have details of the aspects of time synchronisation, which is fundamental in an IEC 61850 application and which must be defined in the project specification. In Chapter 6, the issues of cybersecurity are discussed, without whose definitions we will not guarantee a safe implementation. Obviously, there are other aspects to be observed related to the other chapters. It is in the project that the entire implementation process, technologies and solutions to be applied must be defined.

The specification should describe the implementation process and management aspects over the life cycle of the system [6]. This defines the acceptance procedures, tests and tools for the design, maintenance and operation of the implementation as well as the training programme of the technical teams according to each responsibility and level of complexity involved in the specific activity is necessary.

Considering that the intention is to apply an IEC 61850-based solution, it must also contemplate the requirements and the method that conformity will be verified.

Generated by a software tool, the SSD file contains the substation information, including the single-line diagram and a function library, logical nodes—LN.

The logical node name can be edited:

- Logical node prefixes and instances can be edited,
- Logical node can be inserted from an existing library,
- Structural changes can be made to logical devices,
- Data objects can be created or relocated through the drag and drop other function,
- Consistency checks are made automatically to ensure that the rules and character numbers of objects are not violated.

A configuration tool should handle the information shown in Fig. 7.2.

The final product is a complete description of the substation in the SCD file. It will not only serve to configure the equipment, but also to generate all the system documentation.

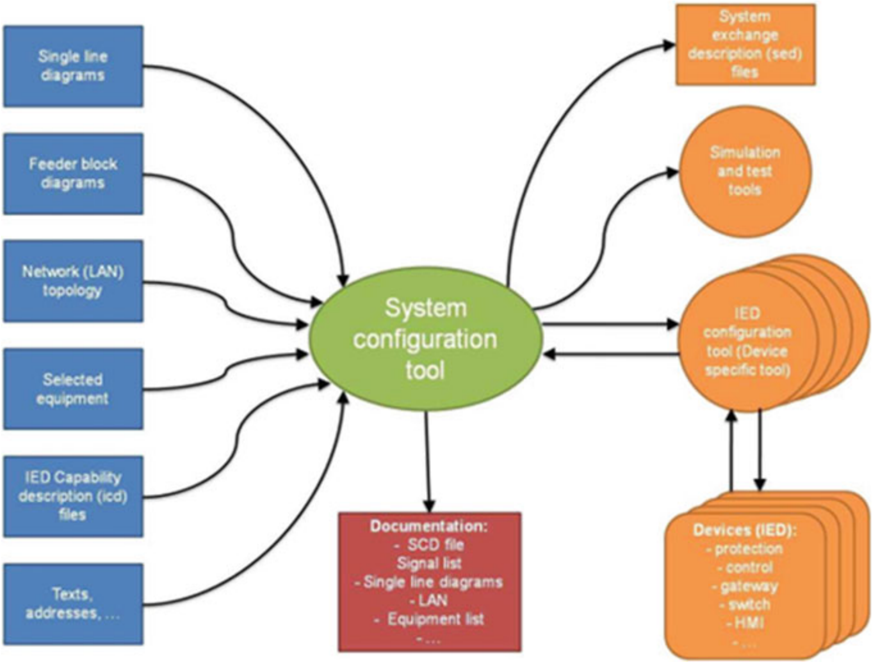


Fig. 7.2 Input and output for an independent system configuration tool [2]

7.2.1 Project Steps and Definitions

The application process of an IEC 61850 solution allows the description of the substation using a standardised language (SCL). The project starts with the configuration of a file using some software tool where we describe the characteristics of the substation: single-line diagram, existing bays, protection and control functionalities, Ethernet network architecture, time synchronisation and information for the supervision system. This way, there is a specification with the entire description of the PAC system (SSD). With it, the supplier defines the necessary IEDs to meet the requested features and requirements, configuring the application on each device (CID) [8].

During the implementation process, this file will continue to incorporate more details and history of changes. At the end, there is a file that will describe the substation (SCD). This file will allow the management of the entire system, with eventual functional changes and communication architecture.

In some cases, the project defines IEDs as we need functionality. In other cases, the IEDs to be applied may already be defined. In this case, the implementation will be different because we will go from logical devices to the mapping. Figure 7.3 shows the workflow possibilities for a project based on the IEC 61850 standard.

The correct application of the solution and the quality of the project depend on the adequate availability of software tools, adherence of the IEDs to the standard and the qualification of the design, maintenance and operation teams (from the utility company and the supplier).

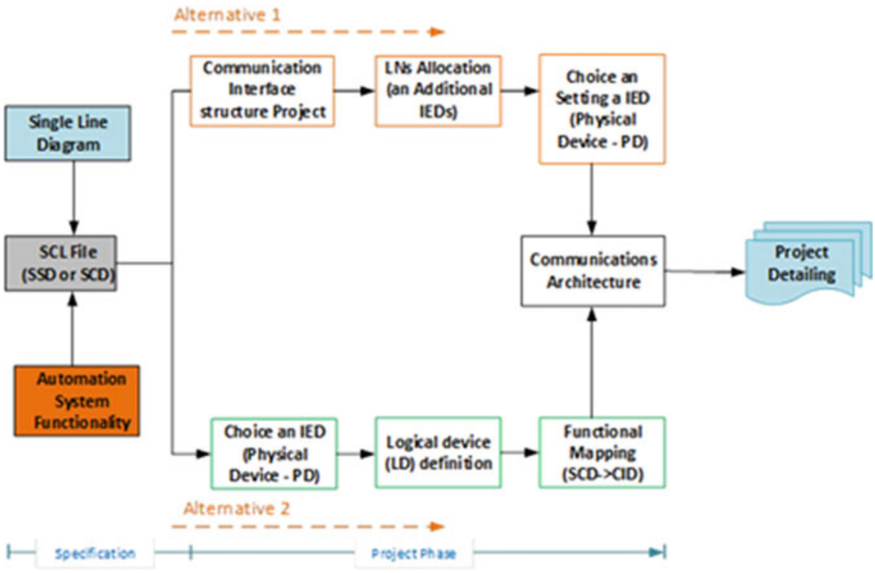

Alternative 1
Communication Interface structure Project
LNs Allocation (an Additional IEDs)
Choice an Setting a IED (Physical Device - PD)
Single Line Diagram
SCL File (SSD or SCD)
Communications Architecture
Project Detailing
Automation System Functionality
Choice an IED (Physical Device - PD)
Logical device (LD) definition
Functional Mapping (SCD->CID)
Alternative 2
Specification
Project Phase

Fig. 7.3 Representation of the specification and design process of a PAC system [3]

The basic elements of a project are as follows:

- The single-line diagram of the substation,
- The single-line diagram AC and CC of auxiliary services,
- Nomenclature of high voltage devices,
- Substation address structure,
- List of addresses,
- Parameterisation list,
- Lists of signals and data flow requirements,
- Information for registration and local storage,
- Grouping of signals and alarms,
- Information to the operation centres,
- Communication information between IEDs (including communication services),
- Operational information, such as status of switching equipment, analogue values and transformer status (TAP, ventilation, temperatures, etc.),
- Control and selection of operational conditions: reclosing selection (single phase, three phase), enabling control (local/remote) and maintenance condition;
- Information to support maintenance,
- Information for statistics and planning,
- Information for failure analysis,
- Function block diagram,
- Details on functional requirements,
- The specification of the functionalities to be performed (including performance data and availability requirements) and their allocation in the single-line diagram,
- Local HMI requirements: operations, interfaces with the process and other control centres,
- Redundancy and topology requirements,
- Interface with existing systems,
- Physical layout (floor plan, ducts, electrical cables),
- Security requirements for digital systems,
- Necessary automation and monitoring schemes,
- Hardware requirements (standards),
- Test requirements and tools,
- Standard test checklist,
- Documentation requirements,
- Training for operation, engineering and maintenance.

In the project stage, the following aspects will also be necessary:

- Short circuit study,
- Electrical drawings of all electromechanical equipment,
- Schematic drawings that include at least the following:
  - Constructive drawings of panels

  - Wiring between all equipment
  - Interlocking and other logic
  - Equipment list
  - Schematic (auxiliary relays, circuit breakers)
  - Quantity of IED: models, firmware and hardware versions
- Interconnection drawings,
- Equipment position drawing,
- Cable lists,
- List of materials,
- Network interconnection diagrams and layout of the communication network,
- List of communication cables,
- Configuration files,
- Design definition of HMI screens,
- FAT procedures and test scenarios,
- SAT procedures and test scenarios.

For substation automation systems based on communication systems, the following additional elements can be included:

- Diagrams showing all devices (for protection and control), clients, data acquisition network, time synchronisation and remote access network,
- Devices connected to the acquisition network and definition about redundancy; how device time is synchronised in time (NTP, IRIG-B or other sources); and how devices allow remote access,
- Network parameters such as IP and MAC address for each device and the port number on the Switch,
- Connection with the Digital Disturbance Recorder—DDR.

The project also defines the necessary tools for the different stages of implantation and management of the substation's useful life according to the devices and their interrelation in the substation. The software tools can be divided according to the type of device for parameterisation.

- Station level,
- Bay level,
- IED level.

The tools can also be defined according to the life cycle phase at the substation:

- System specification tool,
- System configuration tool,
- IED configuration tool,
- Wiring design tools,
- Simulation tools,
- Protection engineering tools,

- Tools for testing devices,
- Diagnostic tools,
- Documentation tools,
- Maintenance tools.

According to the aspects presented, it can be considered that the project of a system continues to demand the description of its functionalities, connections, requirements, documentation, tools and tests. The application of an IEC 61850 solution has an impact on replacing the way some aspects are defined.

For example, the cabling that in a traditional project needs a list of cables, electrical and three-wire design is now described by the definition of the Ethernet communication network: VLANs, connections and network architecture. A logical design described by auxiliary electrical relays and wired contacts is now presented as logical functions associated with physical devices freely.

The advantages are many due to the ease of changes and improvements throughout the project, without the need for physical impacts in the implementation of the project. The physical wiring is associated with electrical drives of the primary equipment and DC and AC power for these devices. But all signs and logic are free and can be easily changed and documented.

In addition, the system tests can be much more efficient, being able to facilitate complete and repetitive simulations and addressing not only the protection and control functionalities, but also the entire communication infrastructure.

7.2.2 Selection of Functionalities

The standard defines the logical system as the combination of all applications and communication functions, performing some complete task such as the management of the substation, using logical nodes. The physical system is composed of all the devices that host these functions and the physical interconnection network of the communication. The system limit is given by the logical or physical interfaces. Within the scope of the standard, the system always refers to the PAC system.

The definition of the functions is related to the groups of logical functions of the protection, automation and control system, classified according to Fig. 7.4. We can define each one of them in the specification, including the horizontal communication of GOOSE signals.

The definition of roles can follow company design patterns, in addition to the characteristic functions for each type of bay, transformer, line, busbar, reactor, capacitive bank, generator and auxiliary service. Generic GGIO (Generic Input/Output) and GAPC (Generic Automatic Process Control) functions, not defined in the standard, can be standardised within projects according to the company's definitions.

Another important aspect is to define the relation of the nomenclatures of the IEC 61850 functions, including the generic GGIO, with the operational nomenclatures. A good strategy is to use templates that relate this information. It is

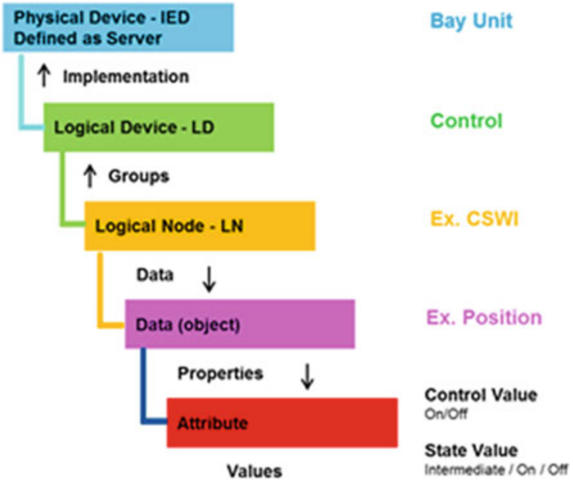


Fig. 7.4 Hierarchical structure of the IEC 61850/logical nodes data model [1]

necessary to establish how the system information will be presented to the different clients of the SCADA system. First, to the real-time operation team, defining the descriptions in alarm, single-line and historical displays. Second, to the post-operation team for analysis of occurrences in the protection and control of the power system. And lastly, to the maintenance team with the necessary information for analysis and predictive, scheduled and corrective actions.

To make this relationship, we can do it including inside the SCL file, in the point description, or externally with other forms of documentation. It is more common to use spreadsheets to make this relationship using dictionaries that determine the treatment of each piece of information. This is also because of devices that are not included in the IEC 61850 solution, because they apply older technologies with protocols such as Modbus, DNP3 or IEC 60,870-5-104. Refer to Fig. 7.5.

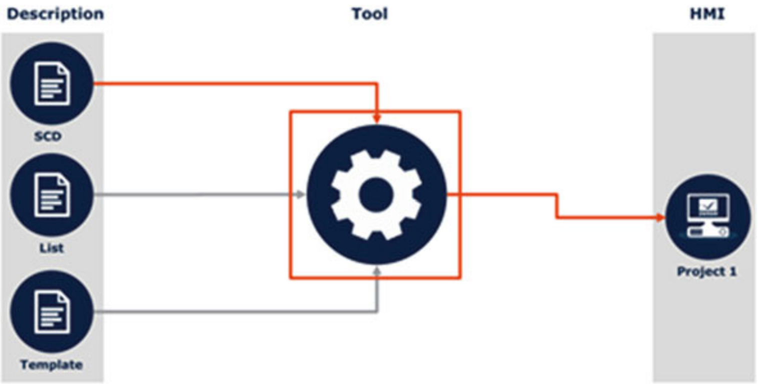


Fig. 7.5 Relationship of the IEC 61850 project and the SCADA system [1]

Therefore, the definition of functionalities must meet all aspects of the project: protection, automation, control, supervision, maintenance, operation, asset management, communication and monitoring.

7.2.3 Definition of Requirements

The IEC 61850 standard has several mandatory and other optional requirements. That is why it is essential that a technical specification includes the desired features. The description of these requirements is presented in the following parts of the standard [5]:

- Part 3: General requirements,
- Part 4: System and project management,
- Part 5: Communication requirements for functions and device models,
- Part 6: Configuration description language for communication in electrical substations related to IEDs.

When a descriptive specification is applied as an SSD file, it is possible to guarantee the requirements to be applied in the designed IEC 61850 solution, involving the protection, automation, control, communication and supervision functions. It is also possible to do this in a descriptive specification, in a traditional way. However, it will be more fragile and more likely to not meet all the specified functionality. Another important aspect is the definition of the performance requirements of the system. Several of them are defined in the standard, but it is important to highlight them in a specification and define how tests will be applied to certify their accordance.

The requirements of an IEC 61850 system need to define criteria for the vertical communication of the SCADA system, the horizontal communication between the control room IEDs and the yard, the Ethernet communication network and the time synchronization system. The requirements depend on the application for which the function is intended, being consistent with the times involved and guaranteeing the performance of the entire protection, automation and control system.

7.2.4 Definition of the Communication Network

The technical specification defines all communication protocols involved in the protection, automation and control system solution. Depending on the level of implementation that is being applied, it may only involve vertical communication and MMS communication—Table 7.1, or GOOSE in functions at the interlock substation level or system conditions—Table 7.2.

If it involves the digitisation of the yard, with the application of the Process Level, it will involve GOOSE signals for opening primary equipment through the

Table 7.1 Vertical communication performance [1]

Vertical communication-MMS				
Measures		States		Control
Maximum	Medium	Maximum	Medium	Maximum
10 s	5 s	8 s	2 s	2

Table 7.2 Horizontal communication performance [1]

Horizontal communication			
Goose		Sampled values	
Maximum	Medium	Maximum	Medium
10 ms	5 ms	10 ms	5 ms

performance of protection or control functions, as well as measures published in Sampled Values.

The guarantee of communication performance is essential, since we are replacing wired signals of states and measures, which involve fundamental functionalities for a reliable and safe control of the power system.

Tests at each step of the implementation process (in the factory, in commissioning and in the maintenance procedures) must verify and guarantee the compliance with the criteria defined in the project.

The communication requirements, MMS, GOOSE and Sampled Values are presented below. GOOSE messages were considered in protection applications defined in the IEC 61850 standard, and technical specifications used by utilities.

Documentation of the communication architecture is also an important requirement of the specification, with respect to physical and virtual connections. At the same time, it is an area in constant evolution, so it is important to plan a solution looking to the future, and not just from the moment of the project being implemented.

Another important aspect is the monitoring of the network, its performance, availability and cybersecurity, which requires equipment dedicated to this purpose, observing all segments of the network and managed in a global view.

7.2.5 Network Requirements

A technical specification may or may not define an architecture for the network. It depends on choosing only performance requirements or applying company standards that facilitate design and maintenance, as it is a known solution.

The so-called star connection has individual IEDs connected to a specific communication port on a specific LAN switch. The LAN switches are then connected in a form of hierarchy.

The switch architecture can also be a “broken ring” in which case you also need to define the re-convergence mechanism generally using the Rapid Spanning Tree Protocol (RSTP).

Both the star and RSTP ring architectures work extremely well for Master–Slave as well as Client–Server-type communications such as IEC 61850-8-1 MMS. These mechanisms have an inherent requirement for the devices involved in the message exchange to establish a confirmed link between them in order to send their messages.

However, star and RSTP rings have an inherent weakness that in the event of a network failure for any reason, Publisher–Subscriber-type messages such as IEC 61850-8-1 GOOSE and IEC 61850-9-2 Sampled Values will be lost until the communication path is restored. In both cases, the loss of LAN includes loss of the individual connection from the IED to the LAN switch. Whilst RSTP has the inherent benefit that the ring will be automatically restored by the recomposition/re-convergence process, that may take 100 ms or more depending on the number of switches in the ring, it still does not heal the direct connection from the IED to the switch. More complex IED connection methods can be used such as “dual homing” double ports on the device or “RSTP small ring” dual ports between the IED and the LAN switches, and the potential for lost messages can be catastrophic for real-time-critical messages such as GOOSE and Sampled Values.

In order to provide higher assurance that real-time-critical GOOSE and SV messages are not lost, the messages can be sent via two different paths simultaneously, and hence, there is no wasted time waiting for a path to recover as the alternate path should still be working correctly. This “no lost message” requirement can be satisfied by either of two so-called “bumpless” protocols introduced in IEC 62439-3: Parallel Redundancy Protocol (PRP) or High-availability Seamless Redundancy (HSR) in a ring network. Both PRP and HSR require devices capable of processing the duplicate messages, and some architectures need some specific devices to connect one network with another. PRP networks can be used by devices that do not support PRP, provided all such non-PRP devices are connected to the same “side” of the two PRP LANs. HSR requires all IEDs in the loop to support HSR directly and all be capable of handling the required maximum bandwidth of all messages, or they must be connected to the HSR ring via special interfaces. In this case, the requirements will be as follows—Refer Table 7.3.

Documentation of the communication architecture is also an important requirement of the specification, in physical and virtual connections. At the same time, it is an area in constant evolution, so it is important to plan a solution looking to the future, and not just the project being implemented.

Table 7.3 Communication network performance requirements [1]

Recomposition local communication network			
RSTP		PRP	HSR
Maximum	Medium	Maximum	Maximum
6 s	1 s	0 ms	0 ms

Monitoring the network, its performance, availability and cybersecurity will require equipment dedicated to this purpose, observing all segments of the network and managed in a global view.

7.2.6 Time Synchronisation

Time synchronisation is another key feature in a digital system. The standard allows for more than one technology, with advantages and disadvantages in each one. Each service involved has different requirements. The specification must include the definition of services and the desired solution. Therefore, it is important to have an engineering overview to plan and define requirements. Thus, we can highlight the main definitions [7]:

- Time servers, their physical and functional requirements, as well as the redundancy criteria in case of failures,
- Integration of time servers (architecture) and their connections,
- Number of satellite constellations,
- Positioning of antennas and connections to time servers,
- Dedicated infrastructure (wired) or via an Ethernet network and, in this case, the application of virtual LANs,
- Protocols to be applied and their adequacy to the requirements of equipment (computers, IEDs etc.) and services,
- Adherence of the system to international standards related to time synchronisation protocols and compliance with the standards of different equipment and services,
- Monitoring that will be carried out to guarantee the time synchronisation service and how it will be informed to the operation and maintenance team,
- Factory and site acceptance tests,
- Routines for predictive and corrective maintenance of the system.

To allow for events to occur at the appropriate time (i.e. synchronised event), the network time synchronisation is focussed on two objectives:

- Allow Sampled Value (SV) measurements to be synchronised,
- Allow the temporal identification in which the events occurred or not (that is, computer forensics).

The first mission occurs during the event; the second mission occurs after the fact—Refer Table 7.4.

Chapter 5 provides further detail.

Table 7.4 Objective of time synchronisation [1]

Mission type	Applied	Artifice	Objective	Example apps
Event synchronization	During events	Application messages, flags	To ensure events occur on time and in correct sequence	Transaction processing process control, authentication
Computer forensics	After events	Time stamps	To determine when events occurred and in what sequence	Digital signatures, crime investigation, fault diagnosis

7.2.7 Certification and Homologation Requirements

The deployment of an IEC 61850 solution involves an engineering process that begins prior to the power company's technical specification. It starts with the development of products, devices, systems and software applied in the solution. Figure 7.6 represents the steps involved.

During product development, companies apply the necessary tests to ensure compliance with different international standards. For product approval, a conformity certification is required, that is, that the product and/or system meets the requirements of the IEC 61850 standard. The most common is that this process is carried out by an independent entity with international recognition. The certification test documents this, indicating that it meets all mandatory items and describing which of the options are applied. In this stage, interoperability tests are also carried out considering the product definitions.

In a second step, acceptance product tests take place, which would be the approval of the product for the solutions applied by the company. Each company has an approach for this step. It can be a generic approval stage, to be applied

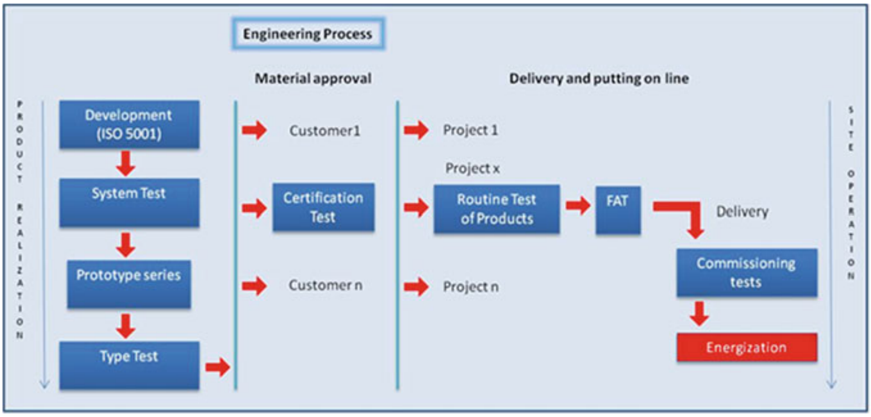


Fig. 7.6 Process Engineering [4]

in future applications, or part of a project's acceptance tests. It can be carried out by the company's own team, integrators or the manufacturer itself presenting technical reports.

The criteria must be defined in the technical specification. Static and dynamic performance tests are applied, including the local communication infrastructure and the supervision system: alarms, signals and commands. The execution of these tests considers firmware version, IED model, protocols architecture, configuration applied to IEDs and the disabling of unapplied functions. It also includes the supervision and control system, the human–machine interface (HMI) and all the associated infrastructure of the network's computing and communication platform.

In these activities, companies often use research centres and consulting companies dedicated to homologating products and systems, which have a dedicated and prepared environment for this. In tests involving the complete solution, platforms are used at the supplier itself, which needs to apply specifics tests defined by the customer.

The major difficulty in validating these tests is the subsequent changes, mainly in relation to new versions of firmware generating risk of secondary repercussion effects. Some companies accept new versions to attend to problems detected after the implantation of the systems, without being able to apply the same extent of testing as initially performed.

7.2.8 Definition of Cybersecurity Solution

In an IEC 61850 solution, cybersecurity is essential because the entire communication infrastructure adopts a standardised solution therefore publicly known and which must be protected to guarantee data and information traffic, in accordance with the protection objectives defined in ISO/IEC 27000—CIA Triangle: Confidentiality, Integrity and Availability. This aspect is discussed in more depth in Chapter 6.

Although the security requirements and mechanisms in the industrial network are similar to a network traditionally applied by Information Technology—IT, there are important differences, because the premise of the IACS (Industrial Automation and Control Systems) is that they were designed to meet requirements for scalability, performance, efficiency, interoperability, redundancy and especially availability. Typically, protection, automation and control systems focus on long uninterrupted life cycles. These requirements, therefore, cannot be affected by cybersecurity protection mechanisms.

The application of tools in all the processes involved is essential: configuration, testing, data collection and security. They contribute to improving security of the system because they consolidate the correct application of the project, the possibility of monitoring and certification of the solution.

The impact that cybersecurity actions have on applied tools must be considered, in the sense that they continue to perform their functions, or whether new resources are required to meet the additional requirements of security mechanisms. The main aspects to be considered are as follows:

- **Functional impact**: The behaviour, configuration, usability, application and effectiveness of the tool are compromised,
- **Management impact**: Licensing, patches, updates, distribution, IP, documentation and other areas that are not part of the real functionality of the tool are affected,
- **Improvement impact**: The tool needs new resources to configure, manage, control, test, encode, decode and interface with systems.

The development of cybersecurity systems should obtain the best cost–benefit. In this sense:

- **Clear guidance for IEC 61850 system suppliers for implementing cybersecurity metrics:** Practical definitions of security metrics based on protection and automation data that are already being collected. This will make it easier, faster and cheaper to implement a security metric programme that supports effective decision-making. In addition, these metrics provide a means of communicating security performance and can be used to guide resource allocation, identify best practices, improve the effectiveness of risk management and demonstrate compliance,
- **Define a security metric framework for IEC 61850 products and services:** A clear set of consensus-based data requirements and metric definitions will allow IEC 61850 suppliers to efficiently incorporate and enhance their security products with metrics,
- **Common standards for data sharing and significant benchmarking:** Safety metric measures will be used to calculate a uniformly significant benchmark between business partners and regulatory agencies. A shared security metric framework and the ability to track and compare results will standardise incident reporting, leading to the identification of best practices and improvements in general cybersecurity practices.

An important aspect to evaluate is if the costs and the security tests to be applied are accessible. The positive side in this sense is that IEC 61850 systems apply security in depth, so defence can be obtained step by step in overlapping layers: OS protection, denial of service detection, patch management, antivirus, application authentication, role-based access control, etc.

7.3 Installation

As we have seen before, the implementation of a substation that applies the IEC 61850 standard with Station and Process Bus has a different dynamic than a wire-based solution. And one of the stages in which this can be realised is at the time of installation in the field.

As previously mentioned, the infrastructure applied in an IEC 61850 solution is quite different from a conventional one. This is reflected in the installation in different aspects.

The implementation of the control room will be less due to the decrease in the number of panels; since there is no wiring of field signals, it is possible to install more than one IED in each panel. Obviously, the implementation time and the cost of the control room will be less.

The definition of the electrical cables to be installed is more defined since they are basically used to supply equipment and drive motors. There will also be less cables to test. Thus, delays in the design of protection and control have no impact on the time of implementation because they do not impact the physical installation of new cables.

The cable ducts in the yard will be smaller, involving less civil works and size. In some cases, the LAN cables may installed in conduit that is not even buried, thus reducing installation time and costs.

Corrections or changes required when putting into service are relatively easy, impacting changes in settings and communication settings, but without physical impacts.

The tests in the SAT field are also minor, since in FAT it is possible to simulate all the real environment, being sufficient to guarantee that in the field installation the connections with the primary equipment are adequate and the services available.

Obviously, all this is reflected in a smaller number of services, which will result in shorter implementation times and costs.

In the other hand, we will have new requirements, especially for the Ethernet infrastructure of local communication. This will mean the installation of an optical fibre Ethernet network infrastructure in the substation yard, which means another professional profile for the construction staff.

This infrastructure also needs a certification that the installation of the fibres was applied maintaining the levels of optical signal. It will also be necessary to verify the entire configuration and connection of the Ethernet network.

Another new element, due to the new central role in the system, is the synchronisation of time, which also needs an appropriate and specific procedure to ensure the correct installation and verification of equipment and services.

7.4 Definition of Commissioning Plan

The commissioning plan must be provided for the technical specification, in order to define the procedures, resources, tests and activities involved to put in-service the following equipment and aspects:

- Primary equipment,
- Protection and control system,
- Supervisory system,
- Local network infrastructure,
- Communications between devices,
- Time synchronisation,
- Cybersecurity.

Definition of the resources involved also includes the necessary tools such as test sets and software for simulating signals and faults, as well as monitoring the entire system.

The plan should also include the processes for updating all documentation and registering versions of software, firmware and settings as well as all records of tests performed and their results.

The optimisation of the commissioning process in the field is a reflection of a good FAT test procedure and of adequate qualification of the involved teams and the definition of responsibility of each one in the process.

As companies and teams have greater domain and technological understanding of an IEC 61850 solution, the commissioning process will be more efficient, impacting the quality of the results and the execution times.

Chapter 9 defines the commissioning procedures.

7.5 Maintenance Aspects at the Specification

Application planning for an IEC 61850 installation should consider not only an implementation plan but also its management throughout the installation life cycle.

This means defining a predictive and corrective maintenance policy for the installation.

The reliability of the system is related to the possibility of monitoring the system. For this reason, the Key Performance Indicators (KPI) must be defined in the project, which will be managed throughout the life cycle of the system.

It is also necessary to ensure compliance with the test requirements. This functionality of the IEC 61850 standard is essential to guarantee the real possibility of maintenance actions in a safe manner. So in the process of homologating the system, it must be fully tested. The necessary tools for this must also be provided in the project and be approved in the acceptance process.

A challenge in this regard is the possibility of having different vendors and different generations of IEDs, and thus having different tools with different possibilities for intervention.

It will also be important to have a strategy for intelligent devices in the yard. This has an important impact on asset management and the procedures of the teams involved.

The company needs to have a strategy for qualifying its teams. Basic knowledge is not associated with projects. Projects must provide for training and product and systems.

Also to be considered in the project is to evaluate the life cycle of the system, especially in relation to regulatory aspects. This directly impacts the economic and financial aspects of the investment.

7.6 Decommissioning

The decommissioning of an IEC 61850 installation has different characteristics than a conventional solution, because its technological and physical updating can happen throughout its life cycle. Then, we will have the decommissioning of parts of the installation that will be replaced by new systems, but being able to maintain functionality with different generations of devices.

Primary equipment typically has a useful life of 30 years. The expected life cycle for electronic equipment is around 15 years. The possibility of monitoring the performance of the devices also allows to evaluate the best time for their replacement.

Technological updates can also occur to add new functionalities and requirements. In this direction, we have an important evolution of new solutions involving, for example, travelling waves, phasors, artificial intelligence that can have a maturity and functional importance that points to the convenience of anticipating technological updates.

The IEC 61850 standard is intended to be time-proof, maintaining data model standards and horizontal and vertical communication protocols which should facilitate the removal of older systems by new solutions whilst maintaining functionality with the parts not replaced.

References

1. Flores, P.H. et al.: Aplicações da Norma IEC 61850 - Sistemas de Automação Operando com Redes de Comunicação (Applications of IEC 61850 standard—automation systems operation with communication networks) (in Portuguese). Cigré Brasil, Rio de Janeiro (2020)
2. CIGRE Technical Brochure 466: WG B5.12 Engineering guidelines for IEC 61850 based digital SAS (2011)
3. Flores, P.H., Paulino, M.E.C., Lima, J.C.M,. Penariol, G.S., Carmo, U.A., Bastos, M.R., Ramos, M.A., Paulillo, G., Lellys, D.: Implementation of digital substation automation systems in Brazil—Challenges and findings. CIGRE 2018, paper number B5–201, Paris (2018)

4. CIGRE Technical Brochure 637: WG B5.45 acceptance, commissioning and field testing techniques for protection and automation systems (2014)
5. IEC 61850: 2016 SER Series Communication networks and systems for power utility automation—ALL PARTS
6. CIGRE Technical Brochure 628: WG B5.39 documentation requirements throughout the lifecycle of digital substation automation systems (2013)
7. Flores, P.H., Zimath, S.L., Lima, J.C.M, Puppi, L.V.S., Bastos, M.R., Ramos, M.A., Lellys, D., Mendes, M.F., Lisboa, L.A.L.: Implementations and challenges in time synchronisation of protection, automation and control systems: Experience and expectations of applications in Brazil. Study Committee B5 Colloquium, paper number B5–205, Tromsoe (2019)
8. Flores, G.H., Alexandrino, M.,Guglielmi Filho, A.J., Souza Junior, P.R.A, Harispuru, C., Demidov, N.: Aplicação de ferramentas de engenharia eficiente utilizando arquivos padronizados da norma IEC 61050 (Application of efficient engineering tools using standardized files of the IEC 61050 standard) (in Portuguese). XIV Seminário Técnico de Proteção e Controle STPC, Foz do Iguaçu (2018)

8 Implementation for IEC 61850 Functional Schemes

Nirmal-Kumar C. Nair

Abstract

This chapter describes the recommendations and best practices of implementing PAC functions and schemes that are planned and designed as per IEC 61850 discussed in Chap. 7. It covers the architecture and general principles of describing functional schemes based on CIGRE technical brochures and the Substation PACS IEC 61850 model guide of one of the largest global utilities. This includes description of exemplars for protection function, automation functionality and process interface use case. This chapter also includes description of two actual case studies for Substation SCADA Automation application and Primary distribution substation automatic bus transfer scheme.

Keywords

IEC 61850 • Protection automation and control (PAC) schemes • Process interface functions • Automatic bus transfer scheme

8.1 General Recommendations for IEC 61850 Functional Schemes [1]

Implementation of any IEC 61850 function [2] can be made easier or harder by virtue of the particular IED capabilities. It is essential that asset owners develop specifications which do not merely ask for 'all IEDs shall be IEC 61850 compliant'—detailed consideration of the application requirements is fundamental and critical. This goes beyond just identifying key logical nodes, but also includes logical devices, data objects and attributes essential for the system to be realised easily

N.-K. C. Nair (✉)
University of Auckland, Auckland, New Zealand
e-mail: n.nair@auckland.ac.nz

P. Bishop and N.-K. C. Nair (eds.), *IEC 61850 Principles and Applications to Electric Power Systems*, CIGRE Green Books, https://doi.org/10.1007/978-3-031-24567-1_8

and of course ‘in-service’ operation, maintenance, test, replacement augmentation and enhancement activities.

Special attention should be given to the specification and implementation of the whole scheme with respect to future changes when IEDs or functions are added, replaced or removed:

(a) Is the solution using appropriate and correct IEC 61850 data modelling and communications?
(b) What changes can/cannot be made without reconfiguration of all the existing IEDs?
(c) Does changing any part of the system require testing of the other parts of the system?
(d) How complex is the logic to be realised in the different IEDs? What is the reusability/scalability transferability of the logic for future designs or other vendors’ IEDs?
(e) What is the impact on the communication in terms of network load?
(f) How can the scheme be debugged in case of problems (message analysis)?
(g) What is the impact of replacement of a device without a fully identical data model and communications support?
(h) Is the solution ‘vendor independent’?
(i) Does the solution suffer any implementation restrictions (mappings, naming conventions, optional elements, etc.)?

The general procedures for specifying IEC 61850 protection schemes, particularly considering operational and maintenance requirements as well as future system modification [3, 4], consist of the following steps:

(a) Determine functional requirements based on: the layout of the substation from an electrical point of view,
    - the identification of the types of equipment,
    - the identification of the protection and control philosophy,
    - the performance requirements,
    - the identification of what data is available or necessary,
    - the consideration of protection schemes: identify what events will cause what actions by what function,
    - the determination of information flow requirements; identify what information is required from each substation device and what information should be sent to each substation device, the determination of information security requirements and the contingency operation.
    - the logical device hierarchy and operation control modes, the required/available ‘isolation’/operation mode control mechanisms and facilities,
    - the required/available testing mechanisms and facilities to connect PCs and equipment,
    - the acceptance or otherwise of requirements for GGIO and GAPC mapping.

(b) Users will determine which logical nodes and data are needed for which applications.
(c) Check availability of required IEC 61850 logical nodes and data in the approved devices.
(d) Develop IEC 61850 data exchanges within the substation. The data to be exchanged between devices and applications in the substation must be defined:
    - GOOSE-based messages,
    - Sampled Analogue Value messages,
    - Client/Server messages.

IEC 61850 is specifically used for the engineering process to configure IEDS to communicate in an interoperable way. IEC 61850 specifically does not standardise algorithms, e.g. as may be used by one vendor for their PDIS function versus another vendor's different algorithm. However, the parameterisation and settings associated with both PDIS elements as well as the inputs to and outputs of the PDIS that must be communicated over the system are standardised semantics to facilitate the Reusable Engineering process. The mapping between IEC 61850 LN/DO/DA and the signals and variables used in the applications also needs to be specified and clarified.

8.1.1 Semantics of Logic

One of the 'associated' configurations of a protection scheme is the scheme logic. Currently, IEC 61850 does not provide logical nodes as logic elements such as

- AND gate,
- OR gate,
- Inverter gate,
- Time delay,
- Set/Reset latch.

These logic elements have been considered as 'local issues' not specifically needing to be communicated over the LAN and hence not within the IEC 61850 area of interest of configuration of the communicating elements. Logic is therefore to be handled by the vendor's proprietary IED Configuration Tool outside of the IEC 61850 environment. IEC TC57 WG10 is currently reviewing aspects for the potential inclusion of some form of logic within the IEC 61850 area. In some cases, there may be outputs of the logic elements that need to be communicated to IEC 61850 logical nodes and/or the signals from one logic element to another can be considered as a form of communication, notwithstanding that it may not appear on the LAN and only within the IED—it is nevertheless a configuration of the scheme. In the meantime, implementing any scheme using IEC 61850 must also consider the interaction of logic to the scheme operation.

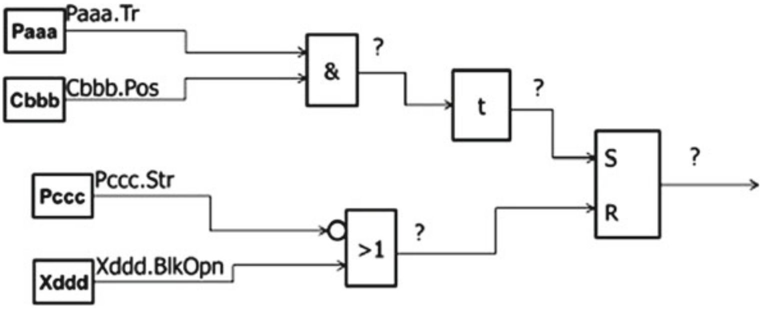


Fig. 8.1 Illustration of the semantics of logic issue

The first issue is the semantics of the logic. One of the essential features of IEC 61850 in creating Reusable Engineering is the defined semantics. A PTOC.Op semantic is always known to be the operation status of the overcurrent element. However, the semantics of an AND gate output status is not related to a defined function of the PACS as it is a combination of functions. This issue is illustrated in Fig. 8.1 titled as Semantics of Logic confusion.

The second issue that must be considered in logic systems is the mechanism to specify that logic. IEC 61131 in essence only defines the tool set for implementing a logic scheme. The format of the engineering files produced by the IEC 61131-based tool is not specifically defined by IEC 61131. Some IEC 61131 tools may well produce an XML format file but at this stage the structure and semantics of those files are entirely proprietary and hence not readily able to be integrated into a generic 'vendor-agnostic' SCD file where the same logic configuration could be extracted by different vendor IED Configuration Tools for use in different IEDs.

Whilst the objective of IEC 61850 is specifically not interchangeability (Part 1, Chapter 4), as far as the overall engineering process is concerned, logic is an area where the configuration of the logic elements can yield considerable benefits in IED engineering effort. There are some moves to integrate IEC 61449 as a more universal function block to assist in more 'universal' definition of the logic.

Therefore, in any scheme engineering process, consideration must be given to the effort and the reusability of any logic requirements.

8.1.2 Logical Device Grouping/Hierarchy

Fundamental to any protection scheme is the ability to easily control its behaviour at the level of individual functions. IEC 61850 now has the ability to specify a logical device hierarchy (also referred to as nesting or grouping) using the GrRef Data Object. If Logical Device (LD) hierarchy is not implemented, it may be necessary to use multiple controls instead of a group control that encompasses several ‘child’ logical devices and associated logical nodes.

The scheme implementation, and indeed the IED selection to suit system and design and operational requirements, must give consideration of the requirement and ability to define specific logical device hierarchy arrangements.

As an example, it may be useful to be able to ‘switch off’ all the measurement functions which report to SCADA and disturbance recorder functions whilst undertaking commissioning or routine maintenance on the IED itself or other IEDs in the system.

The protection logical device itself may have several sub-devices—an example being differential protection and Breaker Fail protection. Whilst the transformer differential protection is being tested with the transformer on line, the mode of the differential logical device needs to be set so as not to cause the XCBR trip. On the contrary, it is required to maintain normal operation of other internal protection functions, e.g. PTUF under frequency or PTUV under voltage, and/or the IED must respond to breaker fail operation GOOSE from other downstream feeders. An example of grouping of LD as hierarchy is shown in Figs. 8.2 and 8.3.

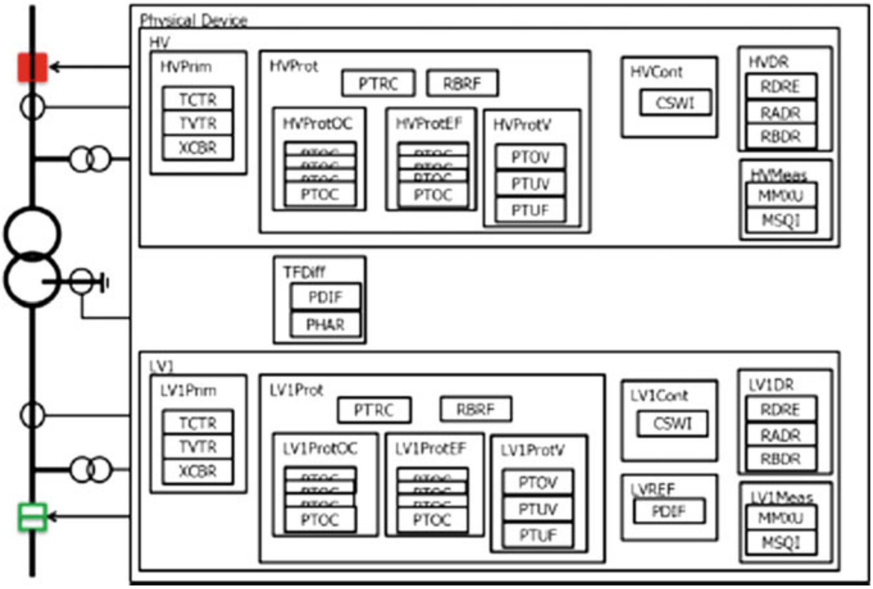


Fig. 8.2 Example logical device nesting: T/F IED

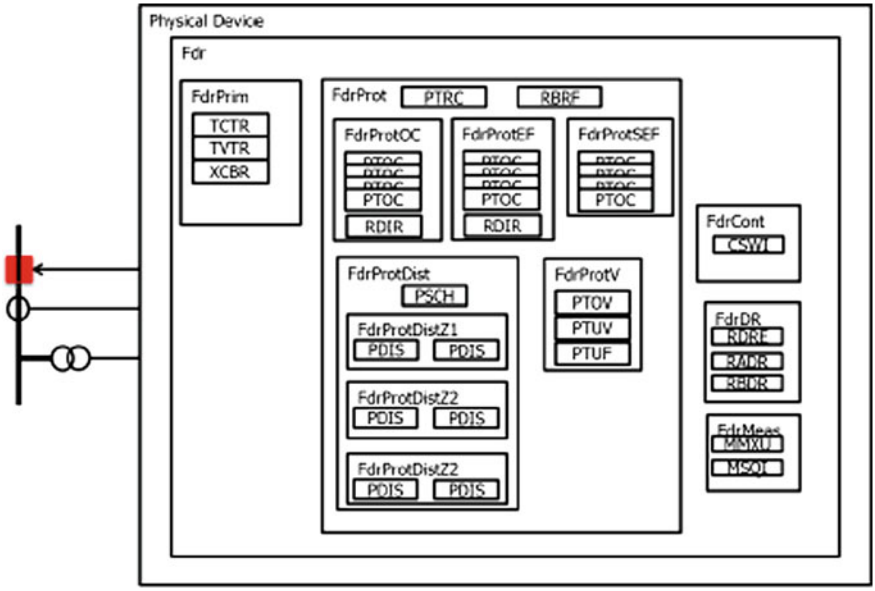


Fig. 8.3 Example logical device nesting: line distance and overcurrent IED

8.1.3 Instance Modelling

In considering any application, it is ultimately necessary to identify the full data model requirements for the system. It is not sufficient to assume that as an 'intelligent electronic device' that all required pieces of information are provided by any conformant IED. This extends to the requirements for the number of instances of a logical node and the required data objects and Attributes required for each instance. If these are not specified at the IED procurement stage, they will not necessarily be available in the chosen IEDs.

IEC 61850 7-4 Ed2 Clause 5.11.1 provides specific guidance on how complex functions such as multiple stages must be modelled. Examples of this are shown in Fig. 8.4 for multistage overcurrent/earth fault IED and Fig. 8.5 for a 3-zone ph–ph and ph-g distance IED.

8.1.4 Optimising Data sets: PTRC

Multifunction IEDs will have numerous protection functions with multiple logical node instances as discussed above. In order to minimise the number of GOOSE messages being published and subscribed, and depending on the test philosophy implemented by the user, the PTRC logical node can be used as a common output of the IED which 'follows' the source protection function logical nodes Pxxx. This

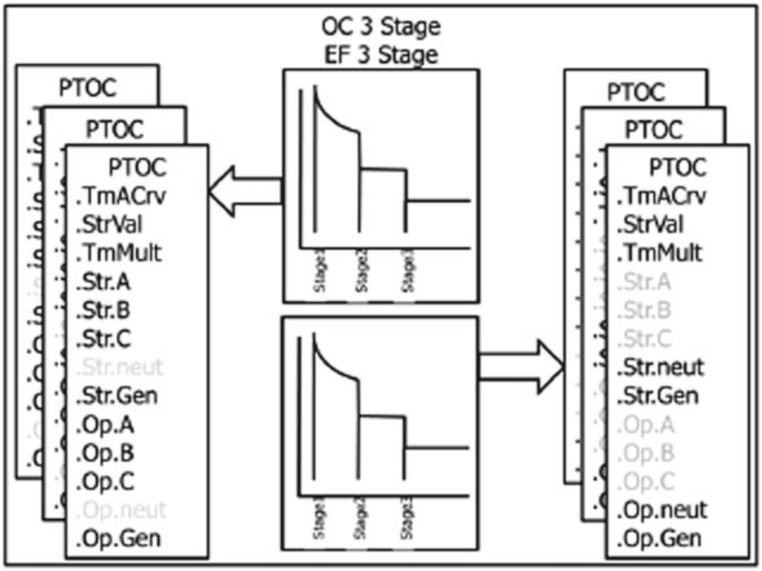


Fig. 8.4 Logical node, data objects and attributes instance modelling O/C-E/F IED

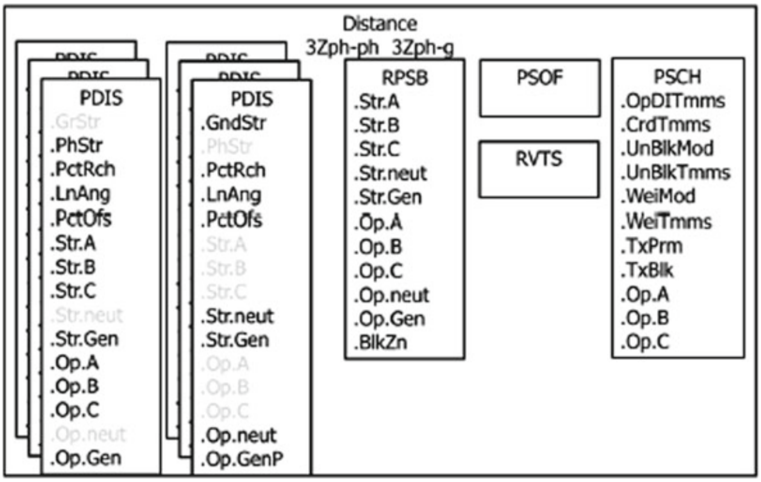


Fig. 8.5 Logical node, data objects and attributes instance modelling-distance IED

is in effect the same mechanism in non-IEC 61850 IEDs using a common output contact for multiple functions.

The PTRC is structured effectively as a multi-dimensional OR gate as shown in Fig. 8.6.

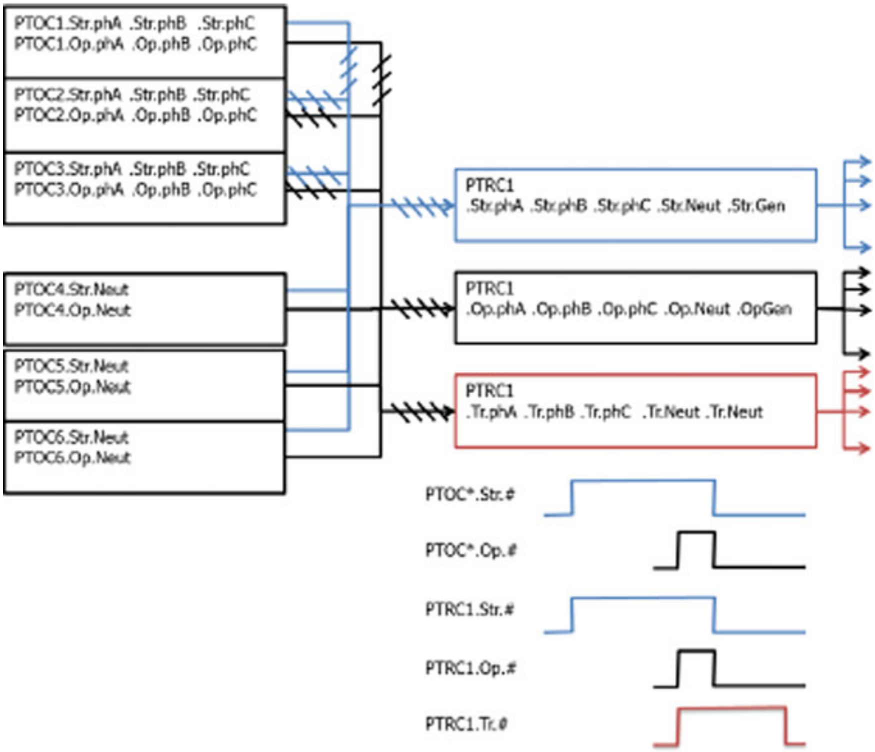

PTOC1.Str.phA .Str.phB .Str.phC
PTOC1.Op.phA .Op.phB .Op.phC
PTOC2.Str.phA .Str.phB .Str.phC
PTOC2.Op.phA .Op.phB .Op.phC
PTOC3.Str.phA .Str.phB .Str.phC
PTOC3.Op.phA .Op.phB .Op.phC
PTOC4.Str.Neut
PTOC4.Op.Neut
PTOC5.Str.Neut
PTOC5.Op.Neut
PTOC6.Str.Neut
PTOC6.Op.Neut
PTRC1
.Str.phA .Str.phB .Str.phC .Str.Neut .Str.Gen
PTRC1
.Op.phA .Op.phB .Op.phC .Op.Neut .OpGen
PTRC1
.Tr.phA .Tr.phB .Tr.phC .Tr.Neut .Tr.Neut
PTOC*.Str.#
PTOC*.Op.#
PTRC1.Str.#
PTRC1.Op.#
PTRC1.Tr.#

Fig. 8.6 Optimised GOOSE—use of PTRC

Each of the '.Str' inputs to the PTRC will result in replication of any operated status as PTRC1.St = 1. This is therefore any 'any protection started' signal from the IED.

Similarly, each of the '.Op' inputs to the PTRC will result in replication of a combined PTRC1.Op = 1. This is therefore any 'any protection operated' signal from the IED.

In addition, the PTRC provides an additional 'treated' output as a PTRC.Tr = 1 which is maintained from the same start time as the PTRC1.Op for a specified duration defined as PTRC.TrPlsTmms.

8.2 RTE Substation Protection Automation and Control Systems IEC 61850 Model [5]

This section covers modelling experiences of RTE's new PACS in accordance with IEC 61850 standard. For their smart Protection Automation and Control system, RTE defines an interoperability framework for this system to ensure its objects of modularity, scalability and interoperability. The first element of interoperability framework is a specific RTE-specified IEC 61850 data model which defines the IEC 61850 model wanted by RTE for all control functions. The examples illustrated in this subsection later are based on the functions specified for RTE's R#SPACE PACS and on the functional specifications of protection functions. The principles applied in the modelling method are as follows:

- Do not consider implementation constraints. This means to treat functions without taking into account whether they are implemented in a single IED or distributed over several IED.
- Each function modelled is associated with a LD (logical device) (consequence of the principle above)

    a. The choice of associating the concept of a logical device to that of a Function must be adapted to avoid subsequently producing an SCL file, non-compliant with the model of the standard (IEC 61850-6). Indeed, the standard, and in particular the SCL, separates the bay part from the IED part. RTE's choice implies describing each LD [function] in each bay concerned. However, the LD is part of an IED and must be described in the appropriate part.

- Strictly follow IEC 61850 edition 2 standards and their published amendments (edition 2.1).
- The documents and functional designs are mainly limited to the Functional Constraints ST of the data objects and punctually refers to MX and SP. All other Functional Constraints are not considered in the RTE model.

The following chapters are associated with each function in the RTE's IEC 61850 models:

1. Description of the function—description in the function in the PACS specifications
2. LN used—gives a list of the logical nodes used for modelling the function as well as the extract from the standard which describes this LN. If no appropriate LN exists in the standard, LN and DO can be created following the prescriptions of the standard.
3. Specificities—gives indications on the chosen principles whether in regard to the standard, operational particularities, electrical characteristics, processing, etc.
4. Static description—lists all the LNs, DOs and possibly the DAs used in a table. If applicable, each DO is mapped with the corresponding entry in the Rte-specific configuration information (FCS).
5. Dynamic description—associates all LNs needed to model the function in a diagram and shows their interaction with other functions.

It should be noted that LD internal exchanges are given as an indication. Certain functions, associated with the PACS specification to a specific function, have been grouped together in one LD in order to achieve more consistent IEC 61850 modelling in Rte's implementation. With regard to referencing high voltage elements, certain functions at the substation level provide information intended for different bay or substation level functions. This is the case, for example, for the VT to be used as bus bar voltage reference for recloser functions. The simplest way to designate a VT would be to give a number to each topological element. The disadvantage of this approach is that it does not allow to have a generic definition and must be reiterated for each substation. Using a generic means of identification of substation elements is a more effective and general approach. This identification must include:

1. The voltage level. Several voltage levels are likely to exist in a substation and can be necessary for certain functions. E.g. Local State Estimator or verification of the consistency of analogue measurements can require elements to be identified at several voltage levels. Some electrical grid operators assign a figure to each voltage level. E.g. in the case of Rte '7' for '400 kV', '6' for 225 kV, etc.
2. The topological element concerned (bus bar, feeder, etc.)
3. A unique number identifies the topological element. A numbering system can be different for each type of topological element
4. A unique reference (if applicable) for identifying the sub-assembly of the topological element (e.g. bus bar section number)

This approach has also been used for identifying instrument transformers. This involves adding the following information:

- The reference of the phase which is traditionally given by multiples of 30°. For a given voltage level, these references can be associated with phases a, b and c of the standard IEC 61850. Several applications require to know exactly which phase is the reference (cf. §4.3.2).
- The type of instrument transformer (current or voltage);
- The accuracy class of the winding of a current transformer;
- An additional reference if there is a redundant acquisition chain.

This information has been compiled in a new LD called LTED with: 'L' because this new LN is part of a system group like LLN0; 'TED' for 'Topological Element Designation'. The following associations are defined between the phases in the IEC 61850 model and the primary HV phases of the substation as given in Table 8.1.

Table 8.1 Association between HV phases and IEC 61850 model

Poles/phases of HV equipment	Referencing in the specifications including information per phase	Instance number of functions modelled with an LN per phase	Instance prefix of functions modelled with an LN per phase as per the standard 61869-9
0, 11	phsA	1	I *nn p* TCTR *n* or U *nn p* TVTR *n*
4, 3	phsB	2	
8, 7	phsC	3	
/	Neutral or cable shield-to-ground	4 (MU/SAMU only)	

8.2.1 Communication with the Power System Control

During the modelling, the information published by the LDs representing the functions and intended for the telecontrol gateway (LDGW) and substation level HMI (LDPO) is identified by a little circle next to the link which represents the transmission. In practice, all messages intended for the LDPO are of the report type, independently of the type of exchange indicated in the dynamic modelling of functions.

Several signals have to be grouped into a general signal for the HMI and/or the telecontrol gateway. This grouping is performed by substation level functions using specific grouping LD (LDGRP). These groupings include the following:

- The signalling of recloser function failure DEFAUT.ARS (DEF.ARS), elaborated from the signals of different LD modelling recloser and service restoration functions.

Monitoring of functions and equipment related to a functional bay is processed at the substation level based on equipment-specific LD (e.g. LDSUIED) and LD-specific health indications. This includes the following:

- Power supply
- IED fault
- Communication fault
- Stand-alone power supply monitoring of remote equipment
- Monitoring of the current/voltage circuits and failure signals of the associated analogue acquisition chain. This includes the following:
  - Failures of SAMU or MU acquiring currents or voltages for protection functions.
  - A SAMU/MU operational fault is a failure of the acquisition circuit for the electrical quantities used by the protection systems. Consequently, the DO

health of the LLN0 of the LDTMs representing the analogue acquisition functions.
- Information subscribed from distance protection functions LDPX indicating fuse failure.
- In case of the differential protection of cable, failure information from the remote SAMU/MU.

In the RTE signal reference list (RISA), the failure of a function is often associated with an IED failure or the loss of its power supply. In an IEC 61850 system, IED failures are detected by LDSUIED (IED supervision function) or by the communication failure (e.g. loss of GOOSE). Since the modelling is independent of the PACS architecture, an IED failure cannot be associated with a function in a generic way. For this reason, the decision was taken not to link signals associated with IED failures (DO LDSUIED/LPHD.Health) to function failures in the modelling. Signals indicating the failure of a function are generated at the substation level or at the bay level based on LLN0.Health of the associated LDs.

The following proprietary LN, based on IEC 61850-7-5 draft document and IEC 61850-80-5 draft document, has been added in order to represent the monitoring of IED inputs and outputs:

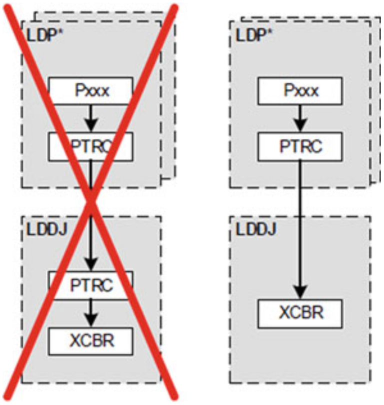
- LPDI System Physical Digital Input
- LPDO System Physical Digital Output
- LPAI System Physical Analogue Output
- LDLD System Physical LED representation
- LMBI System Physical Modbus Interface
- LMSI System Physical Modbus Slave Interface

The DOs associated with a parameter or a setting can be indicated in certain static models, depending on the representation describing publishing conventions. This is especially the case for settings using the SGCB mechanism. When possible, the DOs of IEC 61850 are to be used for configuration and setting of functions. Settings and parameters have been added to the static models, but it should be noted that the present modelling does not completely cover all DOs concerned by settings. A Rte-specific LN (LSET) for parameters not included in the LN defined in the standard has been created.

8.2.2 Tripping Order of Protection Functions

The question arises when it is necessary to have a single PTRC for sending the tripping order to the XCBR or if several PTRC can send this order to a single XCBR. The signalling of starting or tripping of protection functions must be relayed to the telecontrol gateway and local HMI. To do this, Rte has decided to use an LN PTRC per protection function (i.e. one per LDP*) which regroups the DO Op of all concerned protection LNs (Pxxx) of the function.

Fig. 8.7 SCU (LDDJ) and PTRC



As a consequence, in this modelling, LN PTRC is not associated with the LD representing the circuit breaker interface (LDDJ instantiated in SCU/BIED). The tripping order of a circuit breaker by a protection function is published using the DO PTRC.Tr to the subscribing LN LDDJ/XCBR.

As shown in Fig. 8.7, there is no PTRC in the LDDJ, i.e. no unique PTRC associated with an LN XCBR in the circuit breaker LD.

Downstream/Upstream fault direction indications to the telecontrol gateway and local are published by the PTRC depending on received DO Str of class ACD (DA dirGeneral) from protection-oriented LN inside the LD. Definitions of DOs are published by the LNs. The following approach is adopted as follows:

- The detection of a fault is represented by the starting of the protection system (start = Str)
- The trip decision (operate = Op)
- The trip order (trip = Tr)

The notion of sending trip orders via the normal or backup channel makes no sense in the context of IEC 61850 (process bus). Consequently, it has been decided not to take this into account in the modelling. This issue is covered by the redundancy of trip contact-associated LDDJ, representing the circuit breaker interface.

The subsequent sub-sections illustrate a few examples of RTE implementation of their IEC 61850 Functional schemes.

8.2.3 Protection Function Exemplar: Passive Load Feeder Protection (LDPAP)

The passive load feeder protection (PAP) function participates in the elimination of insulation faults on feeders permanently or temporarily connected to bus bar which feature only load and no or insignificant generation. Often, this feeder is

Table 8.2 Logical nodes used for passive load feeder protection

LN	Description
LLN0	Definition extract from IEC 61850-5
	This LN is containing the data of the logical device independently from all application function related logical nodes (device identification/name plate, messages from device self-supervision, etc.)
LSET	Rte Extended Setting LN
PTOC	Definition extract from IEC 61850-5
	A function that operates when the a.c. input current exceeds a predetermined value, and in which the input current and operating time are inversely related through a substantial portion of the performance range
PTUV	Definition extract from IEC 61850-5
	A function which acts when the input voltage is less than a predetermined value
PTRC	Definition extract from IEC 61850-5
	This LN shall be used to connect the ‘operate’ outputs of one or more protection functions to a common ‘trip’ to be transmitted to XCBR similar like a conventional trip matrix
	In addition or alternatively, any combination of ‘operate’ outputs of the protection functions may be combined to a new ‘operate’ of PTRC

a tie line between two active substations, but also two-ended feeders with load at one line end are possible. The protection function is implemented on the passive (or weakly powered) side of the feeder. The logical nodes that are used for this function are shown in Table 8.2.

The following specific considerations apply for this function:

- The LDPAP uses pole discrepancy signals and the position of the circuit breaker published by LDDJ for a single-phase initialisation of the auto-recloser, or to extend a single-phase recloser cycle to a three-phase recloser cycle of a circuit breaker.
- The quality (*q*) attribute of DOs, published by the LDTAC, is used to indicate Teleprotection equipment failure indication.
- PAP function uses residual current. This residual current is calculated by the application associated with the LD from phase currents *Ia*, *Ib* and *Ic* carried by AmpSv DO’s subscribed from LDTM and used by the LN PTOC.
- The diagram of the Teleprotection information transmission between two substations is shown in Fig. 8.8. It shows the transmission of the tele-trip order between two substations.

1st case: Use of a dedicated teleprotection IED:—After reception of a Remote Trip order issued by a local function (Protection, Breaker failure, etc.), the signals are published by the PSCH.Tx* of the LDTDEC of the local bay. This signal is subscribed by the local LDTAC. The trip signal is sent to the remote substation via the proprietary telecommunication link of the teleprotection equipment.

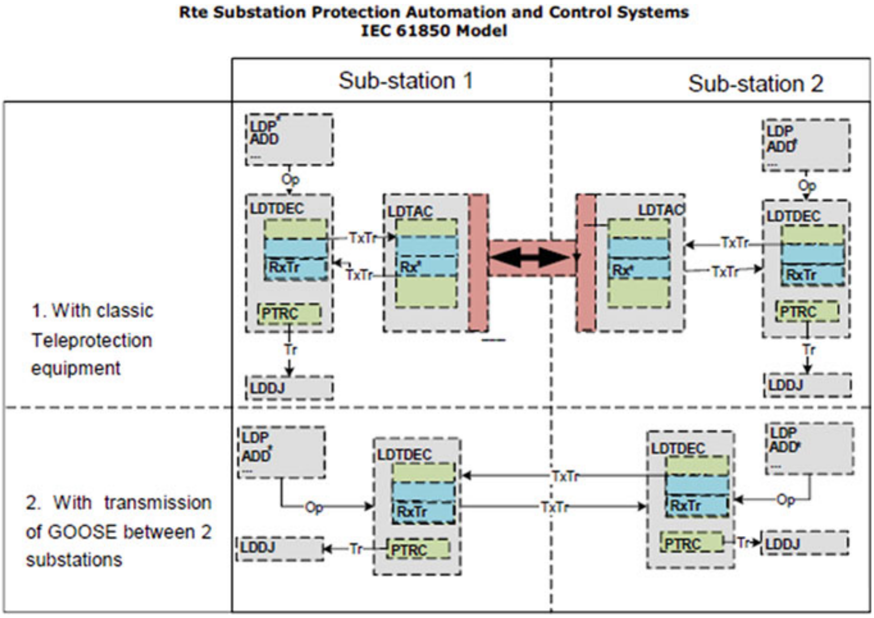

Rte Substation Protection Automation and Control Systems
IEC 61850 Model
Sub-station 1
Sub-station 2
1. With classic Teleprotection equipment
2. With transmission of GOOSE between 2 substations
LDP
ADD
Op
LDTDEC
RxTr
PTRC
Tr
LDDJ
LDTAC
Rx*
TxTr

Fig. 8.8 Tele-trip signal modelling diagrams

The associated teleprotection equipment of the remote substation then publishes PSCH.TxTr subscribed by a LDTDEC of a bay of the remote substation. It is the latter which sends the trip order to the circuit breaker via the PTRC.Tr.

2nd case: Direct communication link—Tele-trip signals are published by the PSCH.Tx* of the LDTDEC of the local substation, after reception of a trip order issued by appropriate functions (e.g. Protection, breaker failure, etc.) addressed to the remote LDTDEC. Once it is received by the LDTDEC of the issuing substation, the trip order for the circuit breaker is transmitted via the PTRC.Tr.

- The selection of the faulted phase by the PAP is modelled by an LN PTUV. This phase selection is based on the comparison between two voltages, one being a sum, corresponding to the application level associated with LDPAP and is not represented in the modelling. The DO Op. ph* is used to indicate the faulted phase.
- The time delay setting after phase selection is fixed in PAP function specification to a value of 500 ms. For this reason, this time delay is not included in the modelled settings of this function.
- The static description of this functional scheme is given in Table 8.3.
- The dynamic description corresponding to the implementation of LDPAP functional scheme is as shown in Fig. 8.9.

Table 8.3 Rte substation PAC IEC 61850 model

LD protection antenne passive (LDPAP)				
LN	DO	CDC	Libellé FCS	Commentaires
LLN0	Health	ENS	DF.PAP*	* = number of the instantiated LDPAP
PTOC1	Op	ACT	DT.PAP*.IR	• Tripping by residual I criterion • Presence of residual current
	StrVal	ASG	Ir_seuil	Residual current threshold setting
	OpDlTmms	ING	Tt	Time delay for three-phase tripping
PTOC2	OpDlTmms	ING	Tm	Time delay for single-phase tripping
PTUV0	Op	ACT	DT.PAP*.PHASE*	• Tripping by phase criterion • Phase selector has determined the faulted phase
	StrVal	ASG	Urseuil (k)	Residual voltage detection threshold
	MinOpTmms	ING		Time delay for voltage memorisation
PTRC0	Op	ACT		Tri-phase/fast protection Initiation of ARS (auto reclose)
	Str	ACD	PAP*.MISE ROUTE	
	Tr	ACT	DT.PAP*	Trip order (PhA, PhB, PhC)
	TRMod	ENG	P1	Trip mode for single phase mode
LSET0	OnOff1	SPG	C0	Activation/deactivation of the teletrip mode
	OnOff2	SPG	C1	Management of nominal/degraded operation mode If ON: nominal mode Tdec If OFF: degraded mode, Tdec delayed
	OnOff3	SPG	C2	Blocking of PAP function in case of upstream fault detected by distance protection
	OnOff4	SPG	P2	Use of current threshold for single phase fault
	OnOff5	SPG	P3	Trip Blocking in case of multi-phase fault

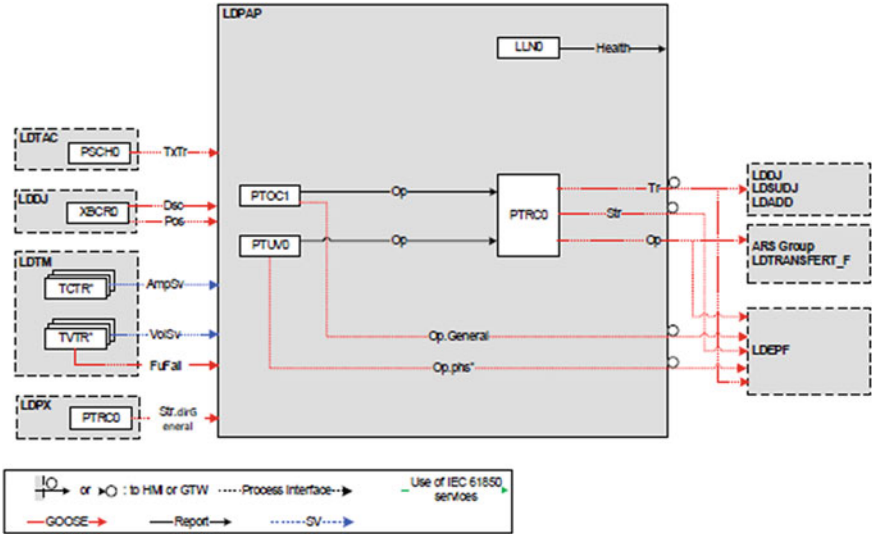


Fig. 8.9 LDPAP dynamic description

8.2.4 Substation Automation Exemplar: Overload Management Function (LDADA)

The overload management function (ADA) is used in the case of transit constraints on the HV grid. This automaton elaborates alarms or trips if the load current exceeds a configured threshold. The operation timeline is described in Fig. 8.10, where T-Alx is the alarm time delay and T-CJx is the tripping time delay of the circuit breaker. Table 8.4 identifies the logical nodes to be used for the overland management function.

The specification of the overload management function (ADA) requires the use of a current criterion. Therefore, the LN PTOC and FXOT are used with current inputs instead of LN PDOP which is based on power.

- One PTOC/FXOT pair is used per threshold. This function uses three thresholds, i.e. three pairs. The thresholds are normally associated with an admissible overload period (e.g. 20 min, 10 min, etc.).
- The setting group for each seasonal regime is particular to each bay, which means one LDADA is instantiated in each bay where the function is needed.
- The LN PTOC of the standard only manages the time delay leading to a trip (TDJx) published by PTRC.Op of the LD. PTOC.Str indicates the detection of a fault (starting) and cannot be used for the alarm output as it cannot be associated with a time delay. Consequently, the time delay leading to an alarm (T-Alx) is modelled by the LN FXOT which uses the same input data as the PTOC.

- The function COMP-ADA (complement to ADA function) (cf. §6.16) is a substation level function which is modelled separately.
- The ADA function generates a signal indicating the direction of the load flow (forward/backward). This signal must be associated with the trip order and sent to the SCADA and to the LDCOMPADA. This association not being provided by the PTRC, it was decided that the subscribing functions concerned would generate this information from the DO Op and Str of the PTRC.
- The ADA function also generates a signal indicating the direction of the load flow (forward/backward) associated to the alarm threshold and used by LDCOMPADA. This association is being provided by the LDADA. The application associated with LDCOMPADA generates this information directly from the subscribed DO FXOT.Op and PTOC.Str.
- The activation/deactivation of the ADA function is performed using LLN0.Mod. The feedback signal is LLN0.Beh.

The static description of this functional scheme is shown in Table 8.5.

The dynamic description corresponding to the implementation of LDADA functional scheme is shown in Fig. 8.11.

8.2.5 Process Interface Functional Exemplar: Circuit Breaker Interface (LDDJ)

This function represents the process interface of a high voltage circuit breaker. The monitoring interface is covered by a dedicated LD (cf. Circuit Breaker Monitoring—LDSUDJ). Table 8.6 lists the logical nodes to be used for realising this interface.

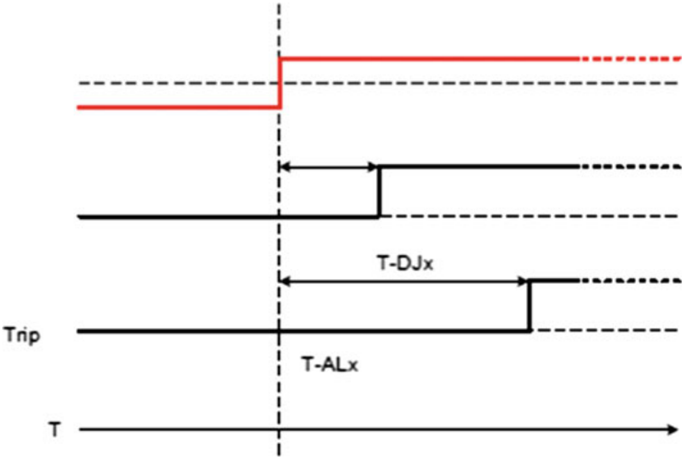


Fig. 8.10 ADA operation timeline

Table 8.4 Logical nodes used for overload management function

LN	Description
FXOT	Logical node FXOT shall be used to set a high-level threshold value to be used in control sequences. If a second level is necessary, a second instance can be modelled. FXOT can typically be used whenever a protection, control or alarm function is based on other physical measurements than primary electrical data
LLN0	This LN shall be used to address common issues for logical devices. For example, LLN0 contains common information for the LD like health, mode, beh and NamPlt
PTOC	This LN shall also be used to model the directional time overcurrent (PDOC/IEEE device function number 67, IEEE C37.2:1996). The Definite Time overcurrent (also PTOC/IEEE device function number 51, from IEEE C37.2:1996) shall be modelled by use of PTOC and selecting the related curve
PTRC	This LN shall be used to connect the 'operate' outputs of one or more protection functions to a common 'trip' to be transmitted to XCBR. In addition, or alternatively, any combinat 'operate' outputs of the protection functions may be combined to a new 'operate' of PTRC

- The Circuit Breaker Interface LD (LDDJ) of each circuit breaker is associated with a LDCMDDJ assuring its control and a LDSUDJ assuring the interface with the monitoring sensors of the same circuit breaker. This triplet is represented in the dynamic modelling.
- One LN XCBR per phase and a 'regrouping' LN XCBR are used in the modelling.
- Signal 'DF.IN.COM.DJ': The DO LDDJ/LLN0.health (ENS specification) can be used, but this requires the use of one of the three variables of this ENUM DO for a simple binary signal. This may constitute a problem for acquisition and transmission, but is compatible with the standard—option retained by RTE.
- The LDDJ publishes the position such as acquired at the process interface in real time, including pole position mismatches which appear during manoeuvres. The 'filtered' position, which indicates the pole discrepancy only after a time delay, is published by the LDCMDDJ.
- The circuit-breaker function LDDJ which hosts the LN XCBR (normally implemented in the SCU) is subscribed to the DO Tr of the different protection functions. It is also subscribed to DO OpOpn and OpCls of LN LDCMDDJ/CSWI and, if applicable, to other functions controlling the circuit breaker without passing by the LDCMDDJ.
- These terminal blocks references that correspond to the binary terminal I/O of the SCU do not appear in the IEC 61850 model of the circuit breaker.
- The XCBR.BlkCls signal is used to elaborate the 'Closing locked' signal in order to prevent the closing if the circuit breaker is not able to ensure subsequent tripping.
- The T-ENC and T-DEC parameters, which define the impulsion duration for opening and closing the circuit breaker, are modelled by using the ≪pulseConfig.onDur≫ and ≪pulseConfig.offDur≫ Data Attributes.

Table 8.5 Logical nodes used for LDADA functional scheme

Overload management function (LDADA)				
LN	DO	CDC	FCS name	Comments
FXOT*	Beh	ENS		
	Op	ACT.general	ALARME.DEP.SEUIL*	Timer alarm when threshold reached (* = 1, 2 or 3 depending on the threshold)
	OpDlTmms	ING.setVal		Alarm time delay T-Alx The value is managed by the SGCB and varies with the regimes
	StrVal	ASG.setMag		IS* current threshold (same value as for PTOC) The value is managed by the SGCB and varies with the regimes
LLN0	Beh	ENS	AUT.DEB	Signal 'Function activated/deactivated'
	Health	ENS	DF.AUTD	ADA Function state
	Mod	ENC	AUT.DEB	Command to activate/deactivate the function (ES/HS)
	NamPlt	LPL		
	The SGCB mechanism is used to manage the 5 setting groups (commands: AUT.DEB Regime x) of ADA (signals: REG.INT1 AUTD.TC, REG.ETE AUTD.TC, REG.INT AUTD.TC, REG.INT2 AUTD.TC, REG.HIV1 AUTD.TC, REG.HIV AUTD.TC, REG.HIV2 AUTD.TC)			
PTOC*	Beh	ENS		
	Op	ACT.general		Trip order of circuit breaker sent to PTRC (* = 1, 2 or 3 depending on the threshold)
	OpDlTmms	ING.setVal		Alarm time delay TDJX The value is managed by the SGCB and varies with the regimes
	Str	ACD.dirGeneral		Directional information elaborated during passage over a threshold
	StrVal	ASG.setMag		Current threshold IS* The value is managed by the SGCB and varies with the regimes

(continued)

Table 8.5 (continued)

Overload management function (LDADA)				
LN	DO	CDC	FCS name	Comments
PTRC0	Beh	ENS		
	Op	ACT.general	FONCT.AUT.DEB	Tripping decision of 3 phases
	Str	ACD	AUT.AVAL AUT.AMONT	Information on the direction of the fault
	Tr	ACT		Trip order to XCBR

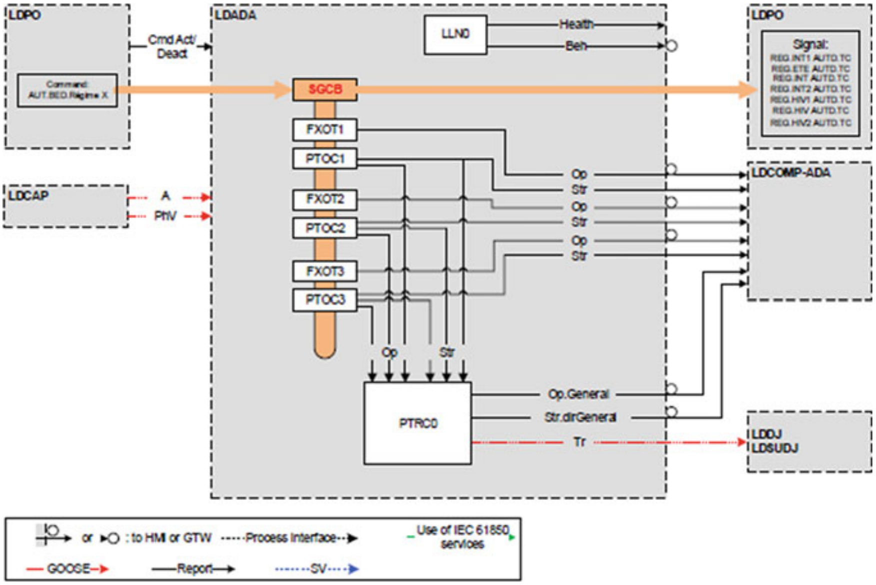


Fig. 8.11 Dynamic description LDADA

- The circuit breaker can be configured to either trip or block in case of low pressure. This is achieved by LDDJ either subscribing to messages with published data objects LDITFSUDJ/SIMG0.InsBlk or LDITFSUDJ SIMG0.InsTr at the instantiation.

The static description of this functional scheme is shown in Table 8.7.

The dynamic description corresponding to the implementation of LDDJ functional scheme is shown in Fig. 8.12.

Table 8.6 Logical nodes used for circuit breaker interface

LN	Description
CSWI	This LN class shall be used to control all switching conditions above the process level CSWI shall subscribe the data object POWCap ('point-on-wave switching capability') from XCBR if applicable If a switching command (for example Select-before-Operate) arrives and 'point-on-wave switching capability' is supported by the breaker, the command shall be passed to CPOW OpOpn and OpCls shall be used if no Control Service is available between CSWI and XCBR (see GSE in IEC 61850-7-2)
GGIO	This node shall be used only to model in a generic way process devices that are not predefined by the groups S, T, X, Y or Z. If needed, all data objects listed in Clause 6 can be used single or multiple for a dedicated application of LN GGIO. Data objects with proper semantic meaning should be preferred. The extension rules according to IEC 61850-7-1, Clause 14 shall be followed
LLN0	This LN shall be used to address common issues for logical devices. For example, LLN0 contains common information for the LD like health, mode, beh and NamPlt
XCBR	This LN is used for modelling switches with short circuit breaking capability. Additional LNs, for example, SIMS, etc., may be required to complete the logical modelling for the breaker being represented. The closing and opening commands shall be subscribed from CSWI or CPOW if applicable. If no 'time-activated control' service is available between CSWI or CPOW and XCBR, the opening and closing commands shall be performed with a GSE message (see IEC 61850-7-2)
XSWI	This LN is used for modelling switches without short circuit breaking capability, for example disconnectors, air break switches, earthing switches, etc. Additional LNs, SIMS, etc., may be required to complete the logical model for the switch being represented. The closing and opening commands shall be subscribed from CSWI. If no 'time-activated control' service is available between CSWI or CPOW and XSWI, the opening and closing commands shall be performed with a GSE message (see IEC 61850-7-2)
LSET	Rte Extended Setting LN

8.3 IEC 61850-Based Substation SCADA/Automation Platform Application Exemplar [6]

The main objective of the work presented here is towards an Under-Voltage Load Shedding (UVLS) and Under-Frequency Load Shedding (UFLS) application implemented in a software-based automation platform used at substation level. The aim was to evaluate and compare the load shedding applications to the traditional methods to determine whether performance requirements can be met. The test system, as shown in Fig. 8.13, developed as part of this investigation had to be designed to allow automated testing of the load shedding applications under different system load scenarios.

The results presented here demonstrate a software-based substation automation platform that supports the integration of time-critical automation functions using IEC 61850 and IEC 61131 can meet the performance requirements of a UVLS and UFLS application, and generally many other time-critical applications. From the

Table 8.7 Static description of LDDJ

Circuit breaker interface (LDDJ)				
LN	DO	CDC	FCS name	Comments
CSWI0	Beh	ENS		
	Pos	DPC		
	OpCls	ACT		Close order send to physical output
	OpOpn	ACT		Open order send to physical output
GGIO0	Beh	ENS		
	Ind1	SPS		Indication of manual closing order of the circuit breaker by switchyard push button
LLN0	Beh	ENS		
	Health	ENS		Health status of LDDJ
	Mod	ENC		
	NamPlt	LPL		
XCBR0	Beh	ENS		
	BlkCls	SPC		Signal CB is blocked in opened state and unable to close
	BlkOpn	SPC		Signal CB is blocked in closed state and unable to open
	Dsc	SPS		CB pole mismatch Direct or calculated acquisition for a separately controlled circuit breaker from the XCBR*.pos of the unit poles Subscribed by the ARS functional group and LDDISCP
	EEHealth	ENS	DF.IN.COM.DJ	
	Pos	DPC	T-ENC	Directly acquired for a circuit breaker with 3 phases control Calculated for a separately controlled circuit breaker poles from the XCBR*.pos of the unit pole Relayed up to CSWI for the power system control Represents the un-filtered states
XCBR*	Beh	ENS		
	BlkCls	SPC		Signal CB is blocked in opened state and unable to close
	BlkOpn	SPC		Signal CB is blocked in closed state and unable to open

(continued)

Table 8.7 (continued)

Circuit breaker interface (LDDJ)				
LN	DO	CDC	FCS name	Comments
	Pos	DPC		XCBR/phase Used for circuit breakers separately controlled per pole Used by XBCR to elaborate the pos value Represents the un-filtered states
XSWI0	Beh	ENS		
	Pos	DPC		Indication that withdrawable circuit breaker is connected or disconnected
LSET0	Beh	ENS		
	OpDlTmms1	ING	T-ENC	Time duration for binary output contact for cb closing command
	OpDlTmms2	ING	T-DEC	Time duration for binary output contact for cb opening command

testing performed, the system load and virtualisation did not appear to have any negative impacts on the function, though ultimately this would need to be tested on the selected platforms and automation function. However, what we have found is that using a statistical analysis of the results we can provide a degree of certainty given the possible variability of GOOSE and Soft-PLC logic cycles.

The 61131-3 logic offers an API that allows generation of the load shedding logic including all the necessary tags from an external source, further reducing the room for error, and saving time and costs when similar UVLS and UFLS functions need to be deployed to different bay-level IEDs at different substations. The use of a standard programming language makes proven logic simple to transfer to alternative platforms, easily duplicated and templated, and testing on a new platform is potentially limited to guaranteeing performance only and not revalidation of the logic itself.

The integration of multiple functions into one system is reducing device count and therefore increasing the overall system reliability. Furthermore, the UVLS and UFLS functions can be added at any time later after the original substation automation system has been commissioned. Redundancy in a hot-hot or hot-standby arrangement can be easily implemented, ensuring that the system can meet availability requirements and avoiding a single-point of failure scenario. The availability of the UVLS and UFLS scheme was further improved by removing the communication latency bottlenecks and having built-in diagnostic capabilities, providing an online diagnostic mode for the tripping logic, the setting parameters and remote access capability.

The benefits of scalability and flexibility were achieved by using an architecture option that supports open standards. The use of IEC 61850 and IEC 61131-3 ensures a high degree of interoperability, enabling the integration of other vendor's products and engineering tools. The software-based automation platforms

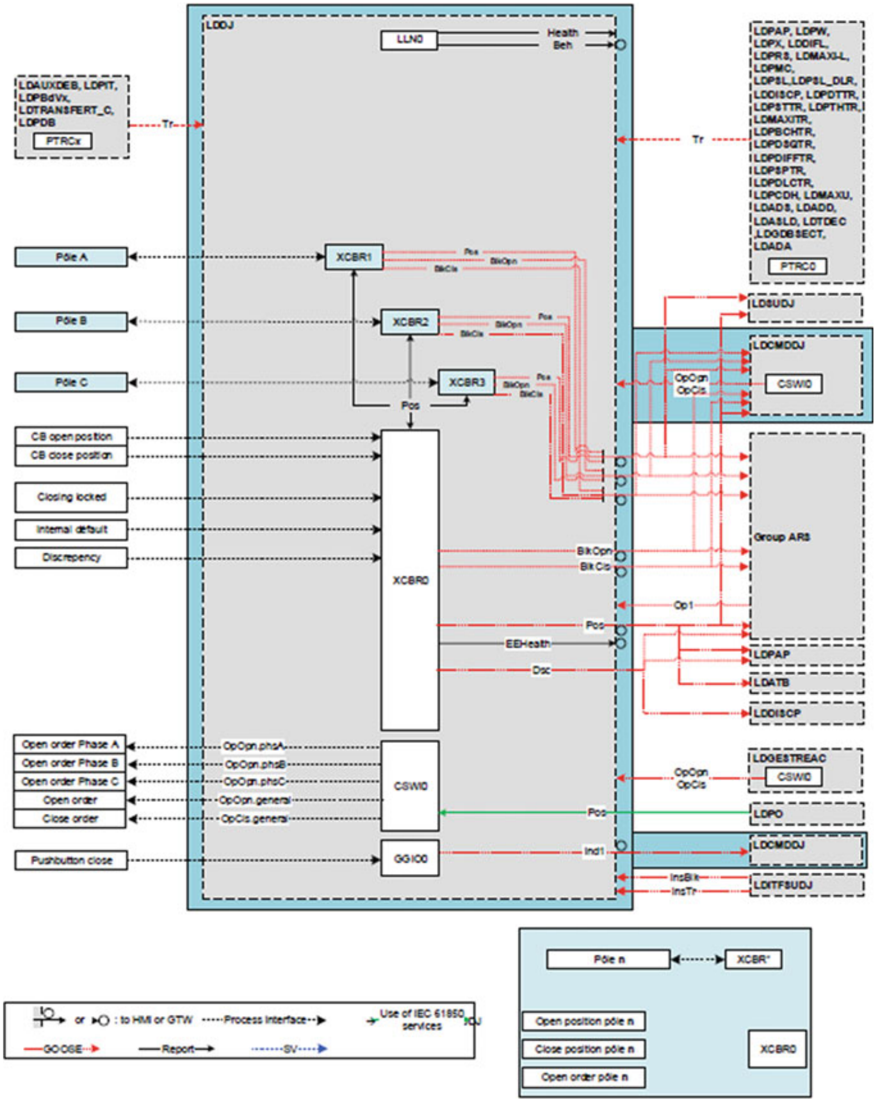


Fig. 8.12 Dynamic description for LDDJ

that support virtualisation allow a high degree of hardware and automation platform independence, reduce maintenance and provide the option to allocate more resources without hardware change, as the configuration and resource requirements change. New functions can easily be added to the existing architecture, removing the need to make changes on the IED level, or replacing IEDs entirely, and new data sources can be integrated quickly into the system. New and more complex

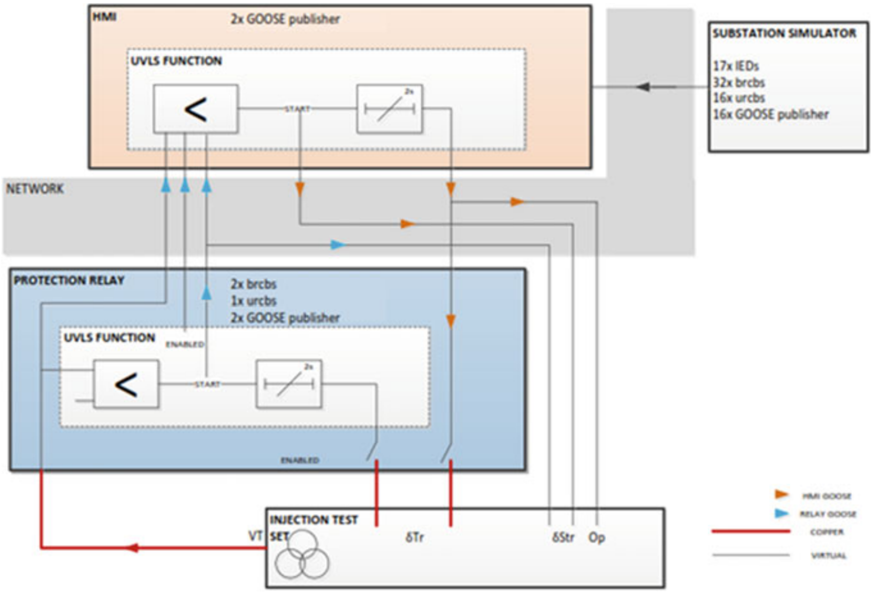


Fig. 8.13 Test system for load shedding scheme

requirements such as the processing of synchrophasor measurements can easily be added to the digital platform.

By leveraging existing station level automation platforms such as HMIs and Gateways, retrofitting these schemes to existing sites would be far cheaper as there would be no need to design or construct new panels and allow for increased battery loads; additional floor or panel space requirements, or learning new relay software and functionality.

It has been demonstrated that substation automation platform products available today will improve the ability to observe and control the power system having a positive impact on the reliability and safety of the electricity networks. New digital platforms can support function integration, provide automated testing and remote diagnostics features, allow virtualisation and when combined with the use of an integrated engineering environment have the potential to significantly reduce cost of engineering, construction, operation and maintenance. Standards-based and hardware-independent automation systems are highly portable, scalable and flexible.

Gaining an understanding of the capabilities of automation products and IEC 61850, along with new distributed automation and control functions required to automate the power system will provide decision makers with the confidence to adopt more capable digital platforms and implement automation functions within and across substations.

The additional complexity introduced with this more integrated approach is justified. However, digital technology products will require organisations to develop specialised skill sets, work processes and procedures to ensure a successful transition to new solutions and architectures. Cyber security is a new emerging issue that needs to be addressed when implementing digital systems.

8.4 Transparent Interlocking Via IEC 61850 Interlocking [7]

A design was done for an IEC 61850-based interlocking scheme at a green-field site which ensures the safe operation of disconnectors and earth switches for all primary system configurations (i.e. operationally transparent) and is in principle extensible beyond the local substation.

The scheme uses switch positions as well as current and voltage information transferred through GOOSE messages. This data is provided to a central interlocking 'controller' which calculates the 'permissions' for each switch using Boolean logic.

The scheme was implemented using the Protection 1 relays and Bay Controllers. The LAN structure used was a simple (non-redundant) star configuration. The 'Central Interlocking Controller' (CIC) subscribes to GOOSE messages provided by each Bay Controller and Protection Relay. These messages contain the relevant disconnector, earth switch, circuit breaker and CT/VT-energised information. The CIC evaluates the information and sends a single GOOSE message containing the 'lock states' for each device. All relays subscribe to this message.

The scheme presently under design is for Transpower's new Pakuranga substation which includes single, double and breaker-and-a-half bay configurations. Information used in the interlocking scheme includes both 33 and 220 kV information (a total of twelve 220 kV bays, three 33 kV buses and around 25 IEDs involved in the scheme).

An 'information processor' relay using IEC 61131 will be used for calculation of the interlocking logic.

This allows use of IEC 61850 naming conventions and decreasing processing times, facilitates future modifications and allows communication of information via other protocols if necessary.

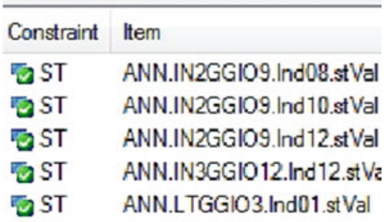
The use of GGIO in any IEC 61850 scheme is highly undesirable as it does not meet the normative concept that data should be named at the lowest possible level and prevents the scheme from being self-documenting.

For upcoming implementation, the manufacturer of the bay controllers and protection relays has provided sufficient flexibility into them that custom logical nodes can be defined to rename generic I/O through editing of the .CID file (Configured IED Description).

A programme was developed to allow the use of a standard template .CID file for each of the three relay types involved in the scheme for Pakuranga. Provided with relay contact and logic mapping data, this programme automatically produced the base CID files for each relay.

In Fig. 8.14, a typical bay controller GOOSE message data set is shown for the Drury implementation using GGIO.

Fig. 8.14 GOOSE message based on GGIO logical nodes

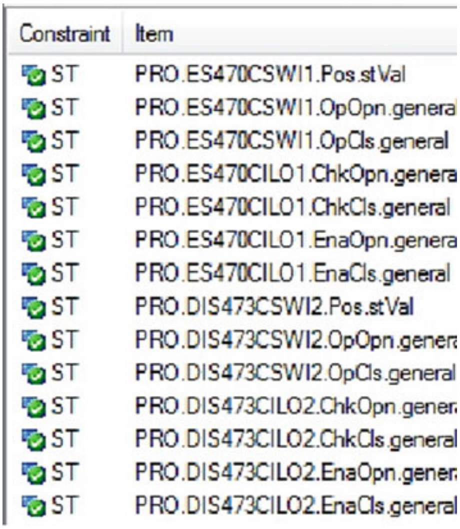


Constraint	Item
ST	ANN.IN2GGIO9.Ind08.stVal
ST	ANN.IN2GGIO9.Ind10.stVal
ST	ANN.IN2GGIO9.Ind12.stVal
ST	ANN.IN3GGIO12.Ind12.stVa
ST	ANN.LTGGIO3.Ind01.stVal

In Fig. 8.15, a typical bay controller GOOSE message data set is shown for the implementation with logical nodes defined. Logical nodes CSWI (control switch) and CILO (control—interlocking) have been implemented. Within the protection relays, PTOV (overvoltage element) and PTOC (overcurrent element) were implemented.

Bay controller logic was designed such that when a disconnector or earth switch open or close command was requested via SCADA or a local pushbutton, a ChkClose or ChkOpen request would be generated from the bay controller. This request would be sent via GOOSE messages to the Central Interlocking Controller (CIC) and operation would be allowed if the corresponding lock point returned via GOOSE message de-asserted within a specific amount of time.

Fig. 8.15 GOOSE message based on custom logical nodes



Constraint	Item
ST	PRO.ES470CSWI1.Pos.stVal
ST	PRO.ES470CSWI1.OpOpn.genera
ST	PRO.ES470CSWI1.OpCls.general
ST	PRO.ES470CILO1.ChkOpn.genera
ST	PRO.ES470CILO1.ChkCls.general
ST	PRO.ES470CILO1.EnaOpn.genera
ST	PRO.ES470CILO1.EnaCls.general
ST	PRO.DIS473CSWI2.Pos.stVal
ST	PRO.DIS473CSWI2.OpOpn.gener
ST	PRO.DIS473CSWI2.OpCls.general
ST	PRO.DIS473CILO2.ChkOpn.gener
ST	PRO.DIS473CILO2.ChkCls.general
ST	PRO.DIS473CILO2.EnaOpn.gener
ST	PRO.DIS473CILO2.EnaCls.general

8.5 IEC 61850 Primary Distribution Substation Functional Application Exemplar: Automatic Bus Transfer Scheme [8]

The case study presented here in this section has been designed and implemented in a distribution utility in New Zealand and has been presented previously during a regional CIGRE conference.

Automatic bus transfer scheme (ABTS) is the practice of transferring a load bus to an alternate source when the normal power supply fails or is tripped thus ensuring continuity of supply. To limit the fault levels, during certain situations, the transformers supplying a primary distribution substation can be run in split instead of parallel operation. This is because during outages if one transformer is lost, overloading of remaining transformers, if it occurs, can be managed. A solution could be designed enabled by digital communications, that if a transformer is lost the bus section circuit breaker (CB) be arranged to be closed automatically after the incomer CB trips. Figure 8.16 illustrates this arrangement.

Bus transfer schemes are well understood for functional implementation for motor bus applications. The time column, as shown in Table 8.8, generally corresponds to the timing evaluation for the motor bus requirements. Slow transfer schemes are usually designed to wait for a predetermined time (hence shown as *X* in Table 8.1), which is normally greater than 0.5 s before connecting the decaying bus voltage to the alternative healthy incomer source.

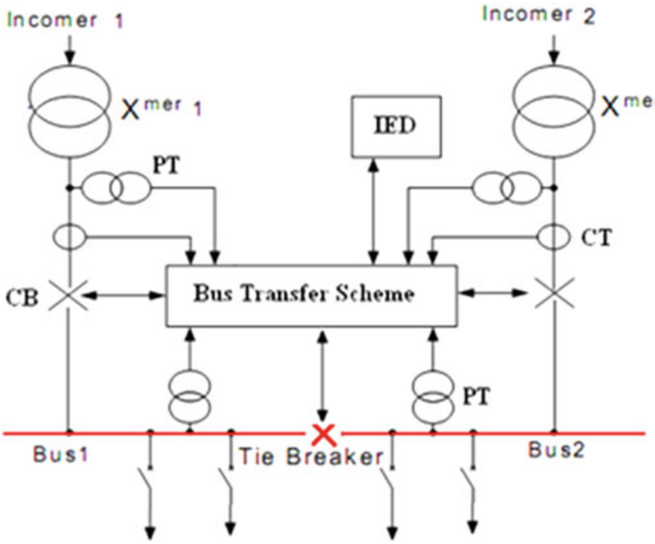


Fig. 8.16 Typical configuration for bus transfer schemes

Table 8.8 Comparative assessment of bus transfer schemes

Transfer	Bus voltage	Cost	Synchroniser	Complexity	Time (s)
Slow	N	Y	N	N	X
Residual	Y	Y	N	N	>0.5 and<3
Fast	Y	N	Y	Y	<0.2
In-phase	Y	N	Y	Y	>0.2 and < 2

Extending the same established principles for motor bus, we can extend the same idea for distribution substation. Figure 8.17 presents the planned configuration of distribution zone substation after its third transformer is installed. Taking into consideration the fault level management, bus section 2-2 is to be run normally open and bus section 1-2 is to be run normally closed. ABTS is the most economic means to adding substation capacity without increasing fault levels but it does not result in any increased revenue for the utility. Other possibilities to be compared include series reactor, neutral earthing resistor and high impedance transformer. The option included in this design is the control and automation of a split-bus scheme. Two cases are considered in the ABTS which requires decision to be made by bus section 2-3's IED.

The proposed ABTS has been implemented in the bus section relay for an 11 kV switchboard in an actual distribution substation where inter-relay communication is based on the IEC 61850 suites of standard. Figure 8.18 shows the configuration of Zone Substation after its third transformer is installed. Bus section 3-1 is to be run normally open, and bus section 1-2 is to be run normally closed. Three cases are considered in the Automatic Bus Transfer Scheme which requires decision to be made by bus section 3-1's IED.

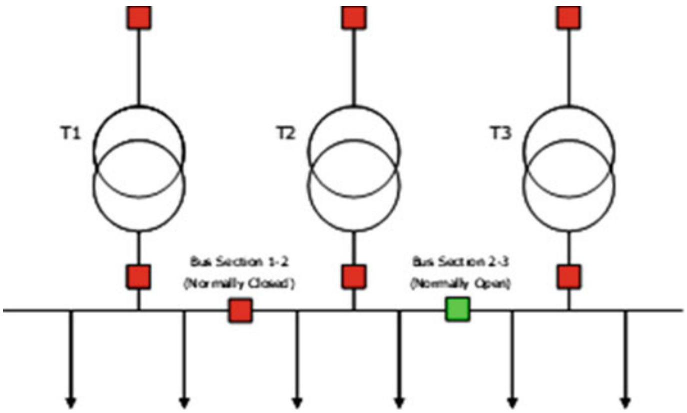


Fig. 8.17 Normal configuration for distribution substation following installation of a third transformer

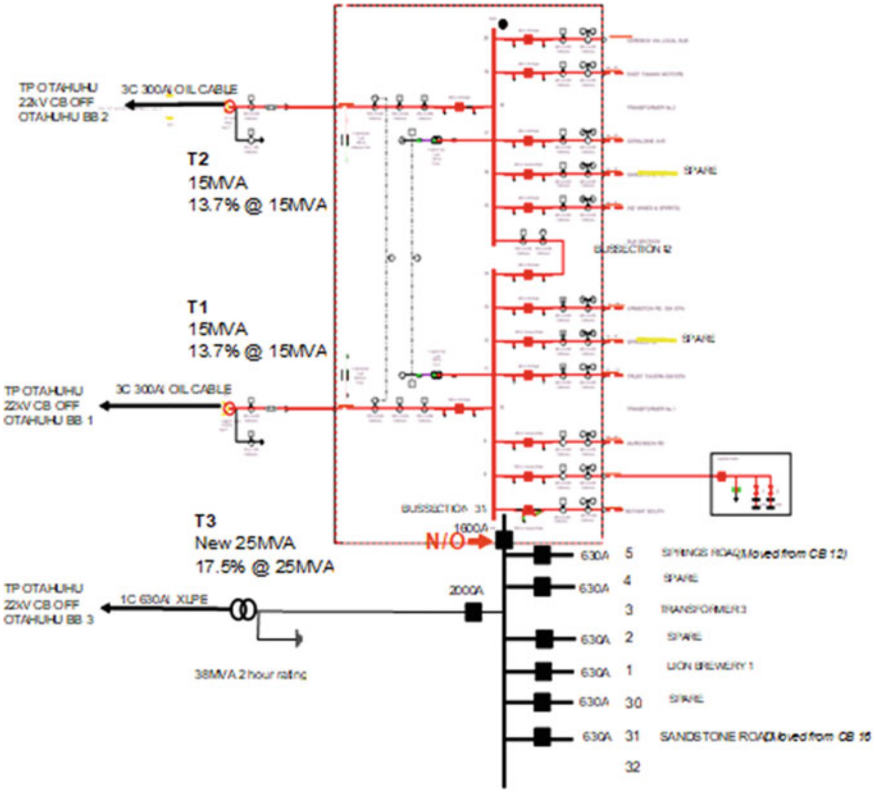


Fig. 8.18 Design of control and protection configuration for distribution zone substation

8.5.1 Overall Functional Scheme Design Philosophy

Case 1: Bus Section 3-1 is open, bus section 1-2 is closed, T3 Trip.

In this situation, feeders connected to T3's bus bar will lose supply. Bus section relay 3-1 will check parameters and if it is safe to do so will automatically close its circuit breaker. Once T3 has been restored the control room operator should ideally open either bus section before the T3 incomer CB is closed, to prevent paralleling of all three transformers.

Case 2: Bus Section 3-1 is open, bus section 1-2 is closed, T1 or T2 Trips.

Overloading of remaining transformer could occur, and loss of any additional transformer will cause loss of supply to feeders attached to that transformer's bus bar. Bus section relay 3-1 will check parameters and if it is safe to do so will automatically close its circuit breaker.

Once both T1 and T2 are both operational again the control room operator should ideally open either bus section before the incomer CB is closed, to prevent paralleling of all three transformers.

Case 3: Bus Section 3-1 closed, section 1-2 is open, T3 or T1 or T2 Trip.

This is an abnormal operating condition. It is up to the control room operator to make control decisions in this case, no logic within bus section 1-2 has been implemented to automatically close its CB, although all the required hardware is available to do so at a future date.

For the three cases listed, the following considerations are required to be satisfied to ensure that the overall scheme operates safely and reliably:

- If an incomer trips due to a bus bar fault or circuit break failure, the scheme will not operate. The scheme will only operate for a transformer bay protection trip (transformer unit protection, transformer Buchholz, tap changer Buchholz, pressure relief protections or a transformer temperature trip).
- If the bus section CB auto switches on to a fault, it will trip instantaneously and lockout. The transfer scheme will not operate if the coupler's circuit breaker is locked out for any reason.
- Paralleling of the three transformers by closing any incomer or coupler circuit breaker is not prevented by interlocking. Instead, an alarm will be raised and a high-set instantaneous overcurrent element will be activated in the bus coupler.
- The scheme can be enabled or disabled either locally or remotely.
- Automatic bus transfer will be disarmed when the coupler is in local control mode.
- If the bus section VT fails, the auto transfer scheme will be automatically disarmed.
- If GOOSE message communications fail, the auto bus transfer scheme will be disarmed and an alarm will be raised.
- The coupler circuit breaker will only be automatically closed if the voltage, frequency and phase angle differences between the buses are within an acceptable range.
- Automatic closing of the bus section CB will occur after a 1.5 s delay to account for downstream distributed generation.

8.5.2 Functional Protection and Automation Scheme Design

Various aspects of this scheme that has been implemented in an actual primary distribution substation in a New Zealand-based distribution network and reported through CIGRE and IEEE conference and journal publications are detailed under through sub-sections.

8.5.2.1 Transformer Bay Protection Trip Detection

Bay trip and circuit breaker status information is sent from all three incomer relays to bus coupler 3-1's relay via GOOSE messaging. The trip messages only relate to transformer unit protection, transformer Buchholz, pressure relief protections or a transformer temperature trip. They are not issued for a HV OC/EF, breaker failure or arc detection trip to prevent an auto closure onto a fault.

For coupler 3-1 to recognise that an incomer CB has opened due to a transformer bay trip, it must receive an indication that both the bay trips have occurred and that the circuit breaker opened within five seconds. For incomers one and two, all bay trips are initiated by an external ‘Master Trip’ relay, and the output of this relay is tied to binary input three of the incomer protection IED to give an indication of the bay trip (The protection ID does not actually issue the trip command.). This indication is assigned to the ‘External Trip—X’ Trip point in the DIGSI system interface.

For incomer three, transformer unit protection is provided by the protection IED and all other transformer bay trips are initiated by individual binary inputs into the protection IED. These individual trips are modelled as logical nodes in the IEC 61850 standard, so are readily available as GOOSE messages for the coupler 3-1 relay to subscribe to.

8.5.2.2 VT Health Monitoring

If a VT failure is detected, the automatic change over scheme is disarmed and an alarm will trigger.

The bus section 3-1 relay has three VT inputs for all phases of the T3 bus and one VT input for the B phase of the T2/T1 bus. The relay monitors the health of these VTs with the VT fuse fail point (function number 170 ‘VT Fuse Fail’ for the IED used) and the auxiliary contacts of the voltage transformer itself (function number 6509 ‘>FAIL:FEEDER VT’ and function number 6510 ‘>FAIL: BUS VT’).

8.5.2.3 Automatic Transfer Scheme Enabled/disabled Control

The automatic transfer scheme can be enabled or disabled via bus coupler 3-1 relay’s function key four on the front panel or remotely through SCADA. It is important to note that ‘Enabled’ does not imply that the scheme is ready to operate. All operating parameters must be satisfied for the scheme to be ‘Armed’ and active. Indication of whether the scheme is enabled and armed is shown on the relay front panel graphical display as shown in Fig. 8.19.

8.5.2.4 Fault Level Protection

Due to fault levels on the 11 kV network, there is a risk to plant and personnel if all three transformers at the substation are run in parallel. To minimise this risk without compromising the distribution network operators’ ability to effectively manage the network, an interlocking scheme to prevent a parallel has not been implemented. Instead, in the event of a parallel an alarm will be raised and a high-set overcurrent protection element is activated in coupler 3-1. The setting for this element (50-1) needs to be specified by the protection consultant, but can be set to operate very low as normally there will be very little current flowing through the bus section and discrimination between bus bar and feeder faults is not required.

The bus section 3-1 relay detects the parallel by subscribing to GOOSE messages of CB position from every coupler and incomer relay. These messages are monitored, and in the event of a GOOSE message failure, the relay will assume

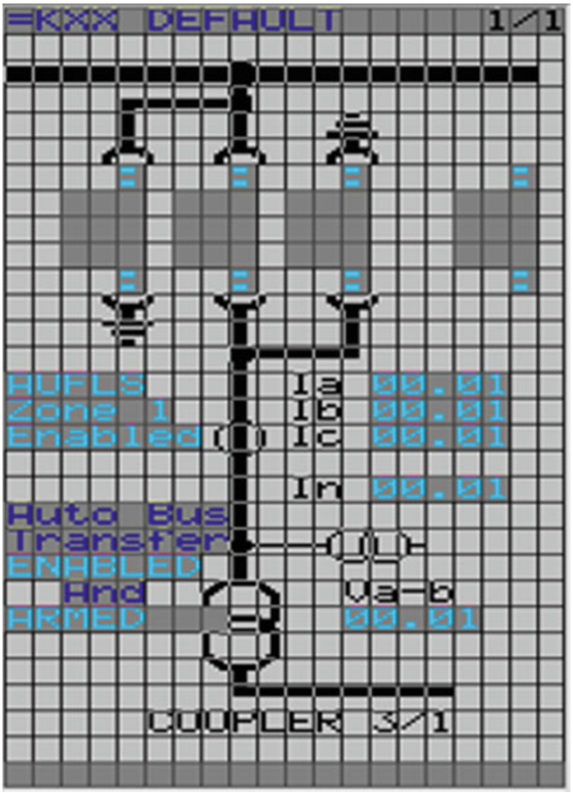


Fig. 8.19 Graphical display for bus section relay 3-1

that the breaker status is closed—this means that it is possible for the high-set element to be activated in the event of a communications failure.

8.5.2.5 GOOSE Message Monitoring

GOOSE messages have been designed to give reliability at least as good as point-to-point wiring so that fast protection messages can be sent over a substation's LAN. Normal Ethernet communication uses acknowledgement messages which ensure that all messages sent reach their destination, but this is done at the expense of transmission speed. GOOSE messages do not use acknowledgements; instead, the message is resent multiple times at increasing intervals once an event occurs to ensure that there is a very high probability of the message getting through to its destination. One of the advantages of GOOSE is the facility to interrogate the status of each transferred message. Where the interruption of a connection cannot be detected with conventional wiring, the signal transmission with IEC 61850 has an integrated continuous monitoring which indicates failure of the connection or the transmitter. The bus coupler relay 3-1 uses the IED's CFC logic block 'SI-GET STATUS' to interrogate GOOSE messages in this way. If a failure is detected, an alarm is raised by the relay.

8.5.2.6 Lockout of Bus Section CB After a Switch Onto Fault

The bus section 3-1 relay is configured to trip instantaneously in the event of a switch onto fault with the 50-2 high-set protection element (function number: '1213A Manual Close Mode'). As part of the logic for the scheme if element 50-2 picks up within five seconds of an auto close command, then the relay is locked out automatically. This will prevent subsequent auto closures from occurring until a 'general relay reset' command is sent, as the schemes' logic ensures that it will always be disarmed whilst bus coupler 3-1's CB is locked out.

8.5.2.7 Voltage and Synchronism Check Before Closing

Before the bus section closes, a check is carried out by the relay to ensure that the voltage, frequency and phase angles on either side of the section are within a preset range. This functionality is implemented using the synchrocheck (25) function of the 7SJ64. If synchrocheck is disabled, then the automatic bus transfer scheme is also disabled.

Before a release is granted, the following conditions must be satisfied:

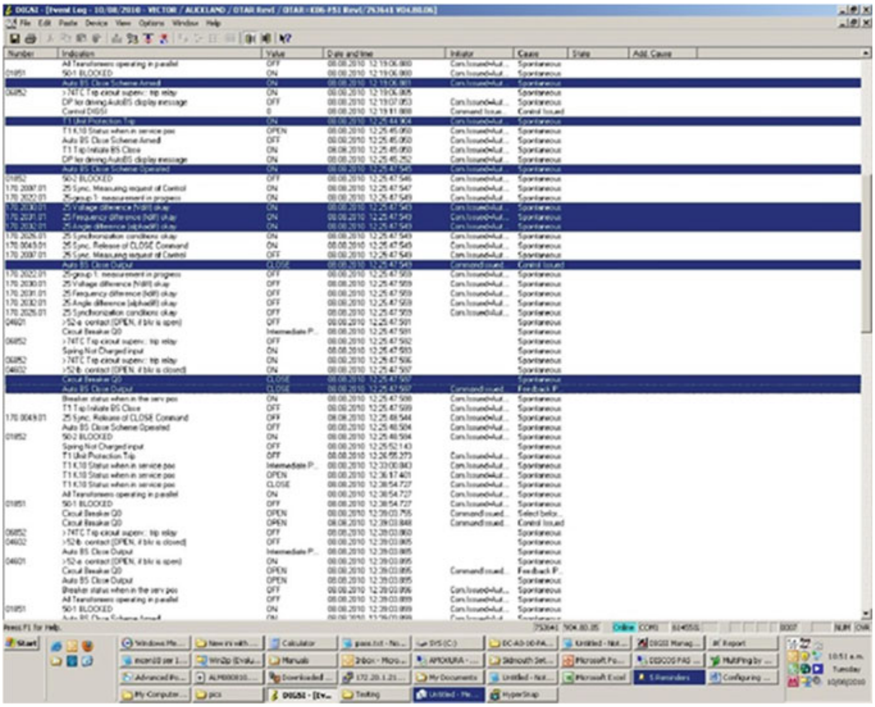
T3's bus voltage is dead (<500 V) and T1's bus voltage is healthy (greater than 9 kV and less than 12.1 kV)
OR—The voltage of both buses is healthy (greater than 9 kV and less than 12.1 kV)
AND—The voltage difference between the two buses less than 200 V primary
AND—The frequency difference between the two buses less than 0.1 Hz
AND—The angle difference between the two buses less than 10°

8.5.2.8 Voltage and Synchronism Check Before Closing

Time delay setting of the scheme:

Consideration has been made for distributed generation in the event of a T3 trip (case one, section three). If there is significant distributed generation connected to bus 3, an island may form and voltage may not immediately drop off to zero. This will prevent the closing of bus section 3-1 by the relay's synchrocheck function.

The distribution utilities' technical standard for the connection of distributed generation requires that the DG ceases to energise the network within two seconds of the formation of an island. The time delay for the scheme is thus set to 2.5 s to allow these generators to disconnect from the network and the bus voltage to fall to below 500 V primary. A screenshot of this scheme in operation is shown in Fig. 8.20.


DIGSI - [Event Log - 10/08/2010 - VECTOR / AUCKLAND / OTAR Rev4 / OTAR - K06-F51 Rev1/ 7SJ641 V04.80.06]
File Edit Paste Device View Options Window Help
Press F1 for Help.
7SJ641 V04.80.05 Online COM1
Start
Windows Me... New in with... Calculator pass.txt - No... SYS (C:) DC-AD-DD-PA... Untitled - Not...
ncom10 per 1... WinZip (Evalu... Manuals Inbox - Micro... APICKURA - ... Sidmouth Set... Microsoft Po...
Advanced Po... ALM00030... Downloaded ... 172.20.1.21... My Documents Untitled - Not... Microsoft Excel
My Computer... pics DIGSI - [Ev... Testing Untitled - Me... HyperSnap
10:51 a.m.
Tuesday
10/08/2010

Number	Indication	Value	Date and time	Initiator	Cause	State	Add. Cause
	All Transformers operating in parallel	OFF	08.08.2010 12:19:06.000	Com.Issued=Aut...	Spontaneous		
01851	50-1 BLOCKED	ON	08.08.2010 12:19:06.000	Com.Issued=Aut...	Spontaneous		
	Auto BS Close Scheme Armed	ON	08.08.2010 12:19:06.001	Com.Issued=Aut...	Spontaneous		
06852	>74TC Trip circuit superv.: trip relay	ON	08.08.2010 12:19:06.005		Spontaneous		
	DP for driving AutoBS display message	OFF	08.08.2010 12:19:07.053	Com.Issued=Aut...	Spontaneous		
	Control DIGSI	0	08.08.2010 12:19:11.000	Command Issue...	Control Issued		
	T1 Unit Protection Trip	ON	08.08.2010 12:25:44.904	Com.Issued=Aut...	Spontaneous		
	T1 K10 Status when in service pos	OPEN	08.08.2010 12:25:45.050	Com.Issued=Aut...	Spontaneous		
	Auto BS Close Scheme Armed	OFF	08.08.2010 12:25:45.050	Com.Issued=Aut...	Spontaneous		
	T1 Trip Initiate BS Close	ON	08.08.2010 12:25:45.050	Com.Issued=Aut...	Spontaneous		
	DP for driving AutoBS display message	ON	08.08.2010 12:25:45.252	Com.Issued=Aut...	Spontaneous		
	Auto BS Close Scheme Operated	ON	08.08.2010 12:25:47.545	Com.Issued=Aut...	Spontaneous		
01852	50-2 BLOCKED	OFF	08.08.2010 12:25:47.546	Com.Issued=Aut...	Spontaneous		
170.2007.01	25 Sync. Measuring request of Control	ON	08.08.2010 12:25:47.547	Com.Issued=Aut...	Spontaneous		
170.2022.01	25-group 1: measurement in progress	ON	08.08.2010 12:25:47.549	Com.Issued=Aut...	Spontaneous		
170.2030.01	25 Voltage difference (Vdiff) okay	ON	08.08.2010 12:25:47.549	Com.Issued=Aut...	Spontaneous		
170.2031.01	25 Frequency difference (fdiff) okay	ON	08.08.2010 12:25:47.549	Com.Issued=Aut...	Spontaneous		
170.2032.01	25 Angle difference (alphadiff) okay	ON	08.08.2010 12:25:47.549	Com.Issued=Aut...	Spontaneous		
170.2025.01	25 Synchronization conditions okay	ON	08.08.2010 12:25:47.549	Com.Issued=Aut...	Spontaneous		
170.0043.01	25 Sync. Release of CLOSE Command	ON	08.08.2010 12:25:47.549	Com.Issued=Aut...	Spontaneous		
170.2007.01	25 Sync. Measuring request of Control	OFF	08.08.2010 12:25:47.549	Com.Issued=Aut...	Spontaneous		
	Auto BS Close Output	CLOSE	08.08.2010 12:25:47.549	Command issued	Control Issued		
170.2022.01	25-group 1: measurement in progress	OFF	08.08.2010 12:25:47.559	Com.Issued=Aut...	Spontaneous		
170.2030.01	25 Voltage difference (Vdiff) okay	OFF	08.08.2010 12:25:47.559	Com.Issued=Aut...	Spontaneous		
170.2031.01	25 Frequency difference (fdiff) okay	OFF	08.08.2010 12:25:47.559	Com.Issued=Aut...	Spontaneous		
170.2032.01	25 Angle difference (alphadiff) okay	OFF	08.08.2010 12:25:47.559	Com.Issued=Aut...	Spontaneous		
170.2025.01	25 Synchronization conditions okay	OFF	08.08.2010 12:25:47.559	Com.Issued=Aut...	Spontaneous		
04601	>52-a contact (OPEN, if bkr is open)	OFF	08.08.2010 12:25:47.581		Spontaneous		
	Circuit Breaker Q0	Intermediate P...	08.08.2010 12:25:47.581		Spontaneous		
06852	>74TC Trip circuit superv.: trip relay	OFF	08.08.2010 12:25:47.582		Spontaneous		
	Spring Not Charged input	ON	08.08.2010 12:25:47.583		Spontaneous		
06852	>74TC Trip circuit superv.: trip relay	ON	08.08.2010 12:25:47.586		Spontaneous		
04602	>52-b contact (OPEN, if bkr is closed)	ON	08.08.2010 12:25:47.587		Spontaneous		
	Circuit Breaker Q0	CLOSE	08.08.2010 12:25:47.587		Spontaneous		
	Auto BS Close Output	CLOSE	08.08.2010 12:25:47.587	Command issued	Feedback P...		
	Breaker status when in the serv pos	ON	08.08.2010 12:25:47.588	Com.Issued=Aut...	Spontaneous		
	T1 Trip Initiate BS Close	OFF	08.08.2010 12:25:47.589	Com.Issued=Aut...	Spontaneous		
170.0043.01	25 Sync. Release of CLOSE Command	OFF	08.08.2010 12:25:48.544	Com.Issued=Aut...	Spontaneous		
	Auto BS Close Scheme Operated	OFF	08.08.2010 12:25:48.504	Com.Issued=Aut...	Spontaneous		
01852	50-2 BLOCKED	ON	08.08.2010 12:25:48.504	Com.Issued=Aut...	Spontaneous		
	Spring Not Charged input	OFF	08.08.2010 12:25:52.143		Spontaneous		
	T1 Unit Protection Trip	OFF	08.08.2010 12:26:55.273	Com.Issued=Aut...	Spontaneous		
	T1 K10 Status when in service pos	Intermediate P...	08.08.2010 12:33:00.843	Com.Issued=Aut...	Spontaneous		
	T1 K10 Status when in service pos	OPEN	08.08.2010 12:36:17.401	Com.Issued=Aut...	Spontaneous		
	T1 K10 Status when in service pos	CLOSE	08.08.2010 12:38:54.727	Com.Issued=Aut...	Spontaneous		
	All Transformers operating in parallel	ON	08.08.2010 12:38:54.727	Com.Issued=Aut...	Spontaneous		
01851	50-1 BLOCKED	OFF	08.08.2010 12:38:54.727	Com.Issued=Aut...	Spontaneous		
	Circuit Breaker Q0	OPEN	08.08.2010 12:39:03.755	Command issued...	Select befor...		
	Circuit Breaker Q0	OPEN	08.08.2010 12:39:03.848	Command issued...	Control Issued		
06852	>74TC Trip circuit superv.: trip relay	OFF	08.08.2010 12:39:03.860		Spontaneous		
04602	>52-b contact (OPEN, if bkr is closed)	OFF	08.08.2010 12:39:03.885		Spontaneous		
	Auto BS Close Output	Intermediate P...	08.08.2010 12:39:03.885		Spontaneous		
04601	>52-a contact (OPEN, if bkr is open)	ON	08.08.2010 12:39:03.895		Spontaneous		
	Circuit Breaker Q0	OPEN	08.08.2010 12:39:03.895	Command issued...	Feedback P...		
	Auto BS Close Output	OPEN	08.08.2010 12:39:03.895		Spontaneous		
	Breaker status when in the serv pos	OFF	08.08.2010 12:39:03.896	Com.Issued=Aut...	Spontaneous		
	All Transformers operating in parallel	OFF	08.08.2010 12:39:03.899	Com.Issued=Aut...	Spontaneous		
01851	50-1 BLOCKED	ON	08.08.2010 12:39:03.899	Com.Issued=Aut...	Spontaneous		
	Auto BS Close Scheme Armed	ON	08.08.2010 12:39:03.899	Com.Issued=Aut...	Spontaneous		

Fig. 8.20 Screen view of the GOOSE-enabled automatic bus transfer scheme

References

1. CIGRE Technical Brochure 540: Applications of IEC 61850 standard to protection schemes. CIGRE WG B5.36. https://e-cigre.org/publication/540-iec-61850-standard-to-protection-schemes (2013)
2. IEC International Standards (IS): https://www.iec.ch/publications/international-standards
3. IEC Technical Specifications (TS): https://www.iec.ch/publications/specifications
4. IEC Technical Reports (TR): https://www.iec.ch/publications/technical-reports
5. RTE Substation Protection Automation and Control Systems: Available from https://assets.rte-france.com/prod/public/2020-08/Contro%CC%82le-commande%20des%20postes%20RTE%20%E2%80%93%20mode%CC%81lisation%20IEC%2061850.pdf (2020)
6. Moulds, D., Schaub, P., Batger, D., Schuiki, B.: Benefits of integrating automation functions into IEC 61850-based substation SCADA/Automation platforms presented at SEAPAC 2019, Sydney, 19–20 Mar 2019
7. Mulholland, D., Sim, S.: Transparent interlocking via IEC 61850 interlocking presented at CIGRE SEAPAC Conference 2011, Sydney, 10–11 Mar 2011
8. Nair, N.K.C., Jenkins, D.L.P.: IEC 61850 enabled automatic bus transfer scheme for primary distribution substations. IEEE Trans Smart Grid **4**(4), 1821–1828 (2013). https://doi.org/10.1109/TSG.2013.2285557

9 Testing of IEC 61850 System Solutions

Alex Apostolov

Abstract

The beginning of this chapter is focussed on the data flow in substations and the different protocols used to improve the network reliability. Their impact on testing over local area networks is later addressed. The following section introduces the testing-related features of the IEC 61850 standard, such as the different modes and the use of simulation. The requirements for testing tools and the different methods that can be used for different types of tests are later described. The end of the chapter is dedicated to testing and security.

Keywords

IEC 61850 • Testing • Testing features • Testing methods • Testing tools

The specialists involved in the testing of protection, automation and control systems are familiar with a physical isolation of the object under test based on the use of connectors or test switches that allow on one hand to open the circuit that trips the breaker and at the same time to replace the analogue signals from the secondary of the current and voltage transformers with signals coming from the test equipment.

The replacement of part or all of the hardwired interfaces with communication links requires the development and implementation of methods and tools that maintain the same level of security during the testing process, while at the same time taking advantage of all the benefits that IEC 61850 provides.

This chapter will help readers to understand details of the methods and tools required for the functional testing of complete digital substation at any stage of its life cycle. It provides detailed description of the testing-related aspects of IEC 61850 Edition 2, followed by the testing methods and tools for the different types of tests and the description of different use cases. The requirements for isolation—one of the key issues related to the testing of digital substations—depend mainly

A. Apostolov (✉)
OMICRON Electronics, Los Angeles, USA
e-mail: alex.apostolov@omicronenergy.com

P. Bishop and N.-K. C. Nair (eds.), *IEC 61850 Principles and Applications to Electric Power Systems*, CIGRE Green Books, https://doi.org/10.1007/978-3-031-24567-1_9

on what is being tested and the purpose of the test. This chapter highlights in which cases the test should be performed using normal operating configuration and when we should use the different operating modes that support virtual isolation. The requirements for functional testing of devices and distributed functions also determine the methods for testing of both types of systems are proposed based on the following order of system components tests:

- Functional testing of individual IEDs used in the scheme,
- Functional testing of distributed functions within a substation.

The testing of the protection, automation and control functions for any substation or other electric power system component plays a very important role in ensuring its reliability and security.

9.1 Data Flow Management of Ethernet-Based Networks [1]

In order to understand the requirements and determine the methods for testing of IEC 61850-based devices and systems, we need to consider the data flow within the network. In a PACS architecture, both station bus and process bus will use Ethernet-based networks as the communication path for data message exchange between devices. Ethernet-based networks are managed networks, in order to provide both reliability and performance.

Reliability is considered as the requirements that messages will always successfully pass between devices connected to the network.

Performance is considered as the requirement that the network introduces no time delays incompatible with functional requirements while passing messages.

Reliability and performance are balanced together in the communication network design. It is important to remember that network reliability and performance are about passing messages across the communication network, not what is the content of the actual message.

One method to manage data flow on a network is to use VLANs. Network ports are configured to only pass messages assigned to specific VLANs associated with the port. Messages are assigned to be transmitted across specific VLANs, with specific priority. In this way, specific messages are limited to specific parts of the network, reducing the bandwidth utilisation for the entire network.

A second way to manage data flow is to use MAC address filtering. Ports on an Ethernet switch can be configured to forward only messages with specific destination MAC addresses. All other messages will be blocked.

The fully digital substations take advantage of Ethernet networks. Managing data, data sets and data messages from PACS IEDs and from test equipment is a complicating factor for testing of the fully digital substation.

The example of Fig. 9.1 illustrates some of these considerations. Data will be outputs of specific logical nodes and inputs to specific logical nodes. A logical

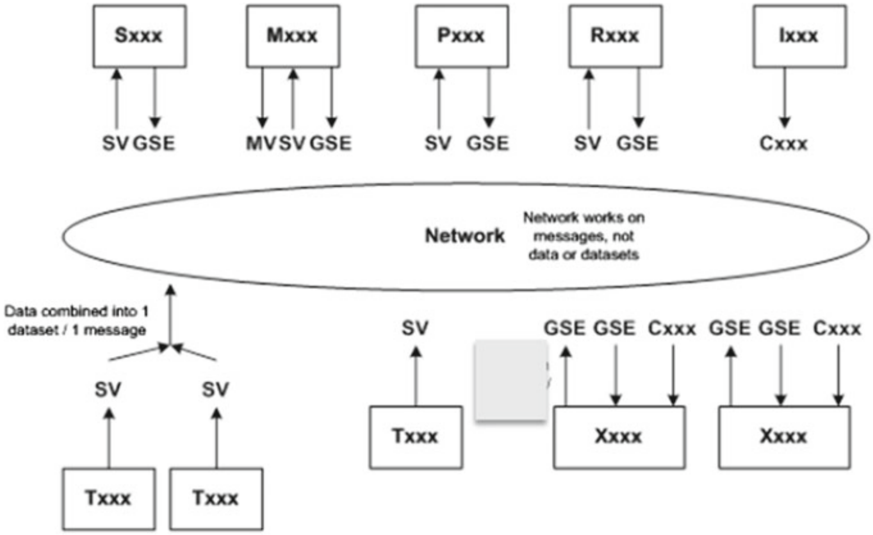

Sxxx
Mxxx
Pxxx
Rxxx
Ixxx
SV GSE
MV SV GSE
SV GSE
SV GSE
Cxxx
Network
Network works on messages, not data or datasets
Data combined into 1 dataset / 1 message
SV
SV
Txxx
Txxx
SV
Txxx
GSE GSE Cxxx GSE GSE Cxxx
Xxxx
Xxxx

Fig. 9.1 Data flows in a fully digital substation

device may combine the data outputs of multiple logical nodes into one data set or place the output of one logical node into multiple data sets. Also, one logical node may accept inputs from different data sets.

Testing at its most basic is the creation of simulated inputs to a function or device to verify the operation and performance expectations taking into account the type of test and the traffic on the communication network. When testing a fully digital substation, it is necessary to create simulated data as inputs to specific logical nodes or logical devices. The condition for this simulated data for testing to pass through the network is that they are placed in a data message that the network accepts and transmits successfully. This requires that the test system publishes messages based on the definitions of the SCL file describing the PACS. There is also the need for a test system to accept, record and analyse messages published by PACS devices.

The most basic requirement in terms of data flows and testing is that test messages, especially if these messages are created by test devices, need to pass successfully through the network and reach the target logical nodes and logical devices that are receiving the test data in the messages. Therefore, the format of the test message must be identical to the entire normal message, including the VLANs and priority levels. If MAC address filtering is used, test messages may need to duplicate destination MAC addresses in some cases, or switch ports may need to be configured to accept test messages with specific destination MAC addresses. This means that it is not enough to only consider the output of a logical node and it is necessary to create an entire test message.

Network data management therefore influences where the test device can be connected to the network in both a physical and virtual sense. This also means that the PACS has to be engineered to support connection for test devices and the testing process.

9.1.1 Considerations for VLANs

GOOSE and SV frames may be configured to specific VLANs and therefore be limited to portions of the network.

Figure 9.2 shows a simplified network configuration with a VLAN. Device 1 and Device 2 normally published data to each other across a specific VLAN. A test device will create test data messages, with these messages assigned to the same VLAN as Device 1 and Device 2. The test device must be connected to the network in such a way that test data messages, with this specific VLAN setting, will be passed through its Ethernet switch ports. Members of the test system have to be configured to simulate messages belonging to the different VLANs.

The simplest way to accomplish this is by the method illustrated in Fig. 9.2. A switch port on one of the switches that will be connected to the specific VLAN may be left unconnected as a physical access port to the test device. Note that cyber security practices may require the enabling and disabling of this port as devices are physically connected and disconnected. This switch port is configured to be part of the same specific VLAN as the operating devices under test. This method works if the test device is publishing test messages and subscribing to test messages. This method absolutely requires that the communication network design is fully provisioned for the connection of test devices to be able to perform all required test scenarios.

Passing VLAN data between individual Ethernet switches requires the use of trunk ports between these switches. Trunk ports pass all data from active VLANs on the switch, unless specific VLANs are excluded by configuration. It is therefore

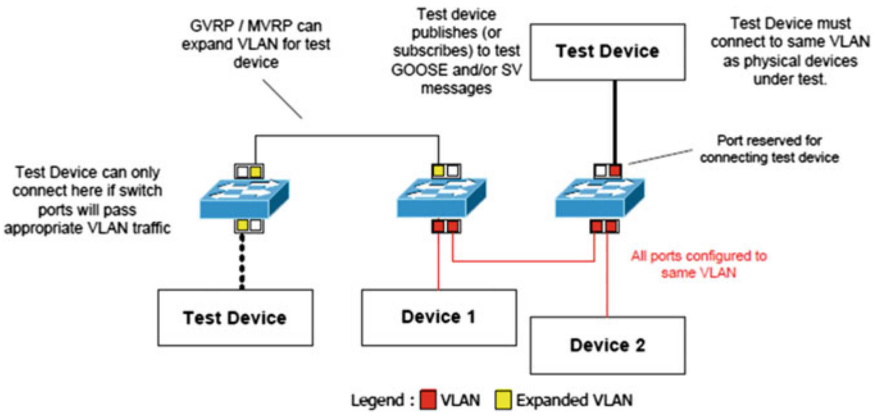

GVRP / MVRP can expand VLAN for test device
Test device publishes (or subscribes) to test GOOSE and/or SV messages
Test Device
Test Device must connect to same VLAN as physical devices under test.
Port reserved for connecting test device
Test Device can only connect here if switch ports will pass appropriate VLAN traffic
All ports configured to same VLAN
Test Device
Device 1
Device 2
Legend : 🟥 VLAN 🟨 Expanded VLAN

Fig. 9.2 VLAN and test devices

possible to connect a test device to a third switch and assign test data to the appropriate VLAN. This requires careful communication network design.

The IEEE 802.1Q standard defines the use of GVRP (GARP VLAN Registration Protocol) or MVRP (Multiple VLAN Registration Protocol) through the IEEE 802.1ak amendment to dynamic expand VLANs through trunk ports. Connecting a GARP or MVRP aware test device publishing or subscribing to data on a specific VLAN will dynamically expand the VLAN across the network. Either of these methods expands the VLAN across a larger portion of the network and should be considered in the communication network design. This also applies in the cases of MAC multicast filtering.

This leads to additional requirements for the PACS and for the test equipment.

9.2 Considerations for Network Reliability and Testing [1]

This section is about the influence of network reliability on protection and control testing. Testing of communication network reliability and performance is not covered. Network reliability methods in common use include RSTP, PRP and HSR. When the topology is an Ethernet ring (RSTP or HSR), this needs to be considered during testing as it can affect network data flow along with VLANs and MAC address filtering. However, PRP and HSR influence how test devices can be connected to the network. Details of RSTP and PRP are covered in detail in Chapters 4 and 7 of this GREEN book.

9.2.1 Rapid Spanning Tree Protocol (IEEE 802.1w RSTP)

RSTP improves the network reliability by enabling Ethernet switches to be connected with multiple paths, such as in a typical ring or mesh topology. RSTP automatically determines the best path that spans the entire physical network and logically opens one or the ports involved in any physical loops. Without RSTP, any broadcast frames received on Ethernet switches connected in a ring topology would flood the network. In the event of a link failure, the network is reconfigured to determine a new path that spans the entire physical network. The time required to detect the fault and find an alternative path is typically referred to as the convergence time. See Fig. 9.3 for a simple example of how this protocol works.

It is important to note that RSTP does not consider how specific VLANs may be configured or impacted. Care should be taken to ensure that required VLANs are available at network switches under various network configurations. This must also include consideration for connection of any test device.

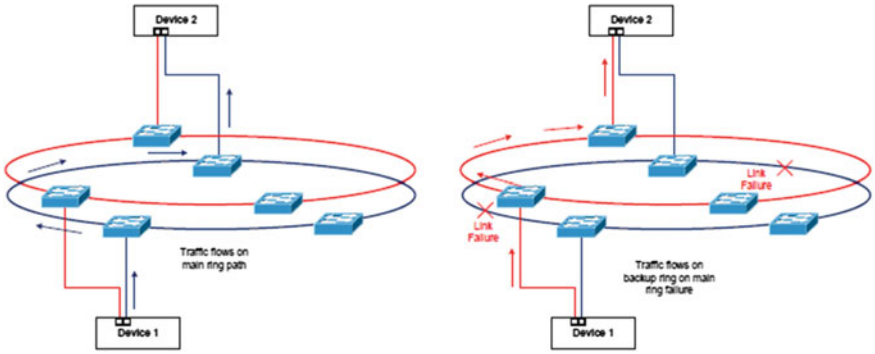

Device 2
Device 1
Traffic flows on main ring path
Device 2
Link Failure
Link Failure
Traffic flows on backup ring on main ring failure
Device 1

Fig. 9.3 RSTP network example with reconfiguration after link failure

9.2.2 Parallel Redundancy Protocol (IEC 62439-3 PRP)

PRP provides network reliability by publishing the same message to two redundant networks. The end device accepts the first instance of this message and discards the second instance. PRP allows devices to be a singly attached node (SAN), or a dually attached node implementing PRP (DANP). A SAN device is connected to only one of the redundant networks and can only communicate to devices connected to the specific network. A DANP is a device connected to both networks implementing PRP. A RedBox allows a natively SAN device to be connected to a PRP network as a DANP device.

This means that there are several possibilities for connecting a test device to a PRP network to publish or subscribe to test messages.

Test device as Single Attached Node.

The simplest method is to connect the test device as a SAN on one of the PRP networks. This allows communications to any device connected to this network. This includes SAN devices connected to this network, and all devices connected as DANP devices to both networks. This connection allows full functional testing of all elements. However, it does not test the performance of messaging over PRP; it allows the injection of test messages in a simple manner. Also, this method can only test devices connected to the same network segment as the test device (Fig. 9.4).

Test device as Double Attached Node implementing PRP.

The test device can also be connected as a DANP (Fig. 9.4). This provides a true verification of the system, including the PRP messaging aspects. Test messages will be PRP messages, published to both networks, and all devices will treat these test messages as PRP messages. If the test device has fully implemented PRP, this is simply a matter of connecting the device to both networks as appropriate. Alternatively, the test device can be connected to both networks through a RedBox.

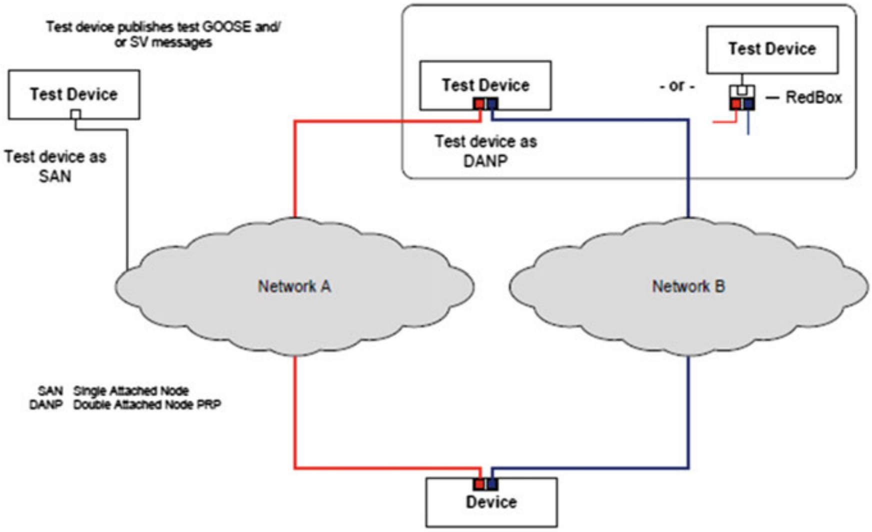


Fig. 9.4 PRP and test device

It is also possible to test SAN devices connected to only one of the networks with a DANP test device.

PRP networks support data flow management exactly the same as traditional networks, including using VLANs and possibly MAC address filtering. Therefore, connecting test devices to the network, either as a SAN or a DANP, still requires considerations for network configuration, data message configuration and physical port connections.

9.2.3 High-Availability Seamless Redundancy (IEC 62439-3 HSR)

HSR networks consist exclusively of Double Attached Nodes implementing HSR (DANH) devices connected in one continuous ring. A device publishes the same message in both directions around the ring. When a connected device receives one copy of the message, it automatically discards the other copy. All devices must be DANH devices: no SAN devices are possible. A typical HSR network looks like Fig. 9.5.

The DANH-only configuration of the HSR network presents a challenge for testing. Test devices must be connected to the network as DANH device. This requires that the test device has HSR capabilities, or the test device must be connected to the network through a so-called Redundancy Box (RedBox), as shown in Fig. 9.6. The strong recommendation is that the test device should be permanently connected as part of the network. The temporary connection of a test device during testing requires breaking of the communication ring, installing additional

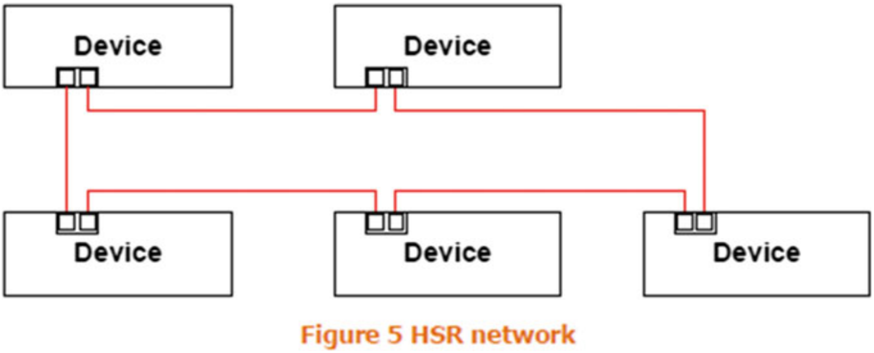


Fig. 9.5 HSR network

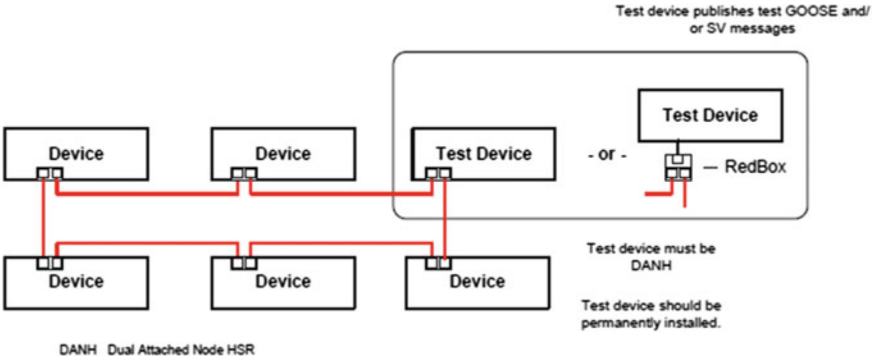

Test device publishes test GOOSE and/ or SV messages
Device
Device
Test Device
- or -
Test Device
RedBox
Device
Device
Device
Test device must be DANH
Test device should be permanently installed.
DANH Dual Attached Node HSR

Fig. 9.6 HSR network with test device

cables to connect the test device and restore the ring. A permanently installed test device simply becomes another node on the network that will pass HSR messages. It is also possible to implement a permanent RedBox to connect temporarily a test device as single node.

HSR networks do not support traditional data flow management techniques like VLANs or MAC address filtering. Every message must travel completely around the network. Therefore, a test device may be connected at any point between any two nodes of the network and can test any device on the network.

9.2.4 Combined PRP and HSR Networks

PRP and HSR technologies may also be combined in PACS using an Ethernet-based network (Fig. 9.7). For example, a bay may use HSR to connect devices without any additional Ethernet switches, while using PRP at the station level to

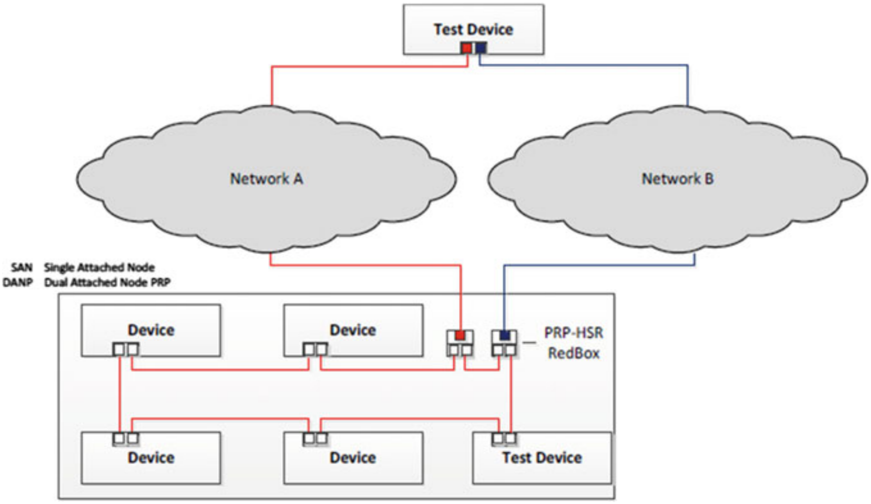


Fig. 9.7 PRP/HSR network with test device

better manage data flow. This approach can be practical as it limits the size of an HSR network, thereby reducing the bandwidth required for each device on the HSR network.

As previously indicated, a test device can be connected between two nodes on the HSR network or to the PRP network. A test device can also be connected to the PRP network if the network is designed with port trunking to pass the required VLAN traffic. It is also possible to use test equipment connected to the PRP network to test devices on the HSR network. However, the impact on network performance should be considered since this requires the PRP network to be capable of handing the additional messages.

9.2.5 Network Bandwidth Considerations

Data flow management techniques as well as the network topology must be considered when determining Ethernet network bandwidth requirements.

Devices connected on a HSR network must have the capacity to handle every message passed around the ring. Devices connected to a PRP network (either as a SAN or DANP) only require sufficient bandwidth to handle traffic for the specific device. The Ethernet switches must have the capacity to pass all traffic on the switch and trunk ports.

The use of test devices has to be taken into account when engineering the communication network from the point of view of bandwidth consideration. This includes the verification that test devices can be operated without notably affecting other functions during maintenance when the substation is in operation.

Managed switches, the system and communication system architecture, the communication protocols RSTP/PRP/HSR and Cyber Security have an impact on the data flow concerning testing. These issues are covered in detail in IEC TR 61850-90-4 [2].

9.3 Features in IEC 61850 Related to Testing [1]

Functions in PACS are not performed by a single function element (logical node), but implemented through an interaction of multiple logical nodes, each contributing its specific functionality. The different functions may be accommodated in different logical devices, even hosted by different Physical Devices, which imposes the usage of agreed-upon basics:

- standardised functional and communicational behaviour of LN,
- evaluation of the information received in a predictable manner,
- exchange of information of a common semantic.

While during normal operation the information flow is defined by the communication scheme, testing may require a user interference into this scheme prior to the test, to avoid inadvertent reactions onto information created during testing. Disconnecting of a device under test is not the appropriate way of doing, moreover as this device may require information from the other components of the system to perform its function.

The above-mentioned basics of IEC 61850 are used for testing purposes to functionally isolate a definable structure of functions in a system environment without disturbing the components in normal operation. The following chapters will present the principles of how functional isolation is achieved.

9.3.1 Test Features Defined in IEC 61850

Some of the features described in this section are not mandatory and, therefore, may not be available in all IEDs which conform to IEC 61850. It is therefore recommended that the users explicitly indicate in their specification if they require such a feature.

9.3.1.1 System Configuration Language (SCL)

IEC 61850 part 6 (Configuration description language for communication in electrical substations related to IEDs) is a key part of the standard that allows engineering tools to create files that are used to describe the capabilities of the IEDs, the functions that are in use and the communication between various functions that are implemented in these IEDs. These files are used with test systems to configure the test devices. The file with the .SCD extension (Substation Configuration Description) contains the information of all IEDs in the system and their communication configuration. This file will also contain information about IEDs that may be physically missing. Some IED configuration tools export only files with extension ≪.CID≫ (Configured IED Description) that contains the configured functions, messages to be received by the IED and the communication parameters of the IED. The test system configuration tool reads the SCD file (or multiple CID files) to get all information about the IEDs in the system or parts of the system to be tested.

9.3.1.2 Simulation

At the IED level, the option to set the logical node LPHD data ≪Sim.stVal≫ to TRUE or FALSE allows the IED to select the multicast signals that will be processed. In order to use this feature to test an IED, ≪Sim.stVal≫ is set to TRUE and the test simulation device has to inject GOOSE messages with the simulation bit in the header set to TRUE. The same behaviour applies to a Sampled Value stream.

The simulation flag of reports is not addressed in the standard, and it might be useful to be able to use the SIM setting in nested or multiple LD levels (and not only physical device level).

Figure 9.8 shows IED1 receiving simultaneously two similar GOOSE messages (GOOSE 1). The GOOSE message from the test simulation device has its message header simulation bit set to TRUE while the other GOOSE 1 message coming from the configured nominal source has its simulation bit set to FALSE. The IED1 with its physical device logical node LPHD1 data ≪Sim.stVal≫ also set to TRUE will process only the GOOSE 1 message from the test device. If the data ≪Sim.StVal≫ is set to FALSE, it will process the GOOSE 1 message from the actual device that has the simulation bit set to FALSE. The actual GOOSE

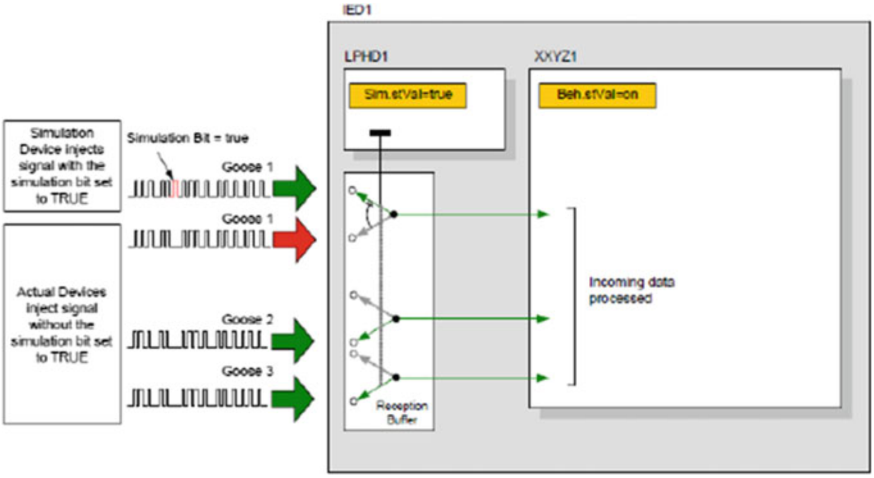

IED1
LPHD1
XXYZ1
Sim.stVal=true
Beh.stVal=on
Simulation Device injects signal with the simulation bit set to TRUE
Simulation Bit = true
Goose 1
Goose 1
Actual Devices inject signal without the simulation bit set to TRUE
Goose 2
Goose 3
Incoming data processed
Reception Buffer

Fig. 9.8 Data used for receiving simulation signals (IEC 61850-7-1 Fig. 40)

1 signal will continue to be not processed until the LPHD1 data ≪Sim.stVal≫ is reset to FALSE.

While LPHD1 data ≪Sim.stVal≫ remains TRUE, two other GOOSE messages from actual devices, GOOSE 2 and GOOSE 3, with simulation bits FALSE will still be processed according to IEC 61850 as shown in Fig. 9.8 as there are no other GOOSE 2 or GOOSE 3 messages on the network that have the simulation bit set to TRUE. As soon as there will be a GOOSE 2 or GOOSE 3 that have the simulation bit set to TRUE, the device will subscribe to this/these GOOSE.

Messages with simulation bit set to TRUE can only be published by test systems. All in service IEDs belonging to the PACS always publish all messages with simulation bit set to FALSE.

The simulation is thus not completely equivalent to the use of a traditional 'test handle' diverting all input data associated with a conventional IED, since not all input signals systematically come from the test tool. Also, when designing the test cases and test scenarios, the effects of GOOSE coming from the system under operation have to be taken into account. Depending on the test aim, it might be preferable to combine the use of SIM and the test mode.

9.3.1.3 Mode and Behaviour of Functions

In IEC 61,850, each function, represented by a logical node or a logical device, can adopt one of five different modes resulting in five different functional and communicational behaviours (cf. IEC 61850-7-4, Annex A):

on, blocked, test, test/blocked, off

If the resulting behaviour is '**on**', the application of a function is operative, all communicating features are in service.

The featured difference between the '**on**' and the '**blocked**' behaviours is that '**blocked**' can only be used by functions which have a direct interaction with the process (i.e. no other intermediate LN). For these boundary logical nodes, the outputs through contacts or analogue ports can be blocked. This means that these outputs are not changed for the duration of the blocking. All communicating features are in service.

Testing shall not impact other functions in normal operation. Therefore, a function which is set to '**test**' is operative, but indicates information as being produced under test conditions. It reacts only on control commands with a test flag set from a client (HMI, telecontrol gateway, etc.).

The output to the process of a function in '**test**' can be blocked in a similar way to '**blocked**' using the '**test/blocked**' behaviour, blocking the output contacts or analogue ports. The application indicates information as being produced under test conditions, and it reacts on control commands with a test flag set.

A function can be set to '**off**', which disables its application. As the application does not work, it neither processes the inputs nor produces physical outputs, and communication output is provided with data quality 'invalid'. Control commands from a client are rejected with negative responses.

Table 9.1 LD/LN Mode/Beh inheritance [IEC 61850-7-4, Table 10: Beh]

LNMode or nested LDMode	LDMode	LNBeh (read only)
XXXX.Mod	LLN0.Mod	XXXX.Beh
on	on	on
on	blocked	blocked
on	test	test
on	test/blocked	test/blocked
on	off	off
blocked	on	blocked
blocked	blocked	blocked
blocked	test	test/blocked
blocked	test/blocked	test/blocked
blocked	off	off
test	on	test
test	blocked	test/blocked
test	test	test
test	test/blocked	test/blocked
test	off	off
test/blocked	on	test/blocked
test/blocked	blocked	test/blocked
test/blocked	test	test/blocked
test/blocked	test/blocked	test/blocked
test/blocked	off	off
off	on	off
off	blocked	off
off	test	off
off	test/blocked	off
off	off	off

The behaviour of a function is controlled jointly by its superior hierarchical level as well as through its controllable object ‘Mod’. To reach a definite behaviour among these two access variants, the states are ordered by priority, where ‘off’ has priority over ‘test’ which has priority over ‘on’. Example: If the superior logical device is set to ‘test’, logical nodes or nested logical devices on a lower hierarchical level may only be varied into ‘test/blocked’ behaviour or switched ‘off’, never be set to ‘on’ (Table 9.1).

Regardless of the status of a function, the communication service to control its behaviour is always in service, even in ‘off’ status.

For testing purposes, ≪Mod≫ can be set to test; to allow ‘processing as valid’ of a control service command with a test flag set to TRUE or a GOOSE data signal with ≪q.test≫ value of TRUE as shown in Fig. 9.9.

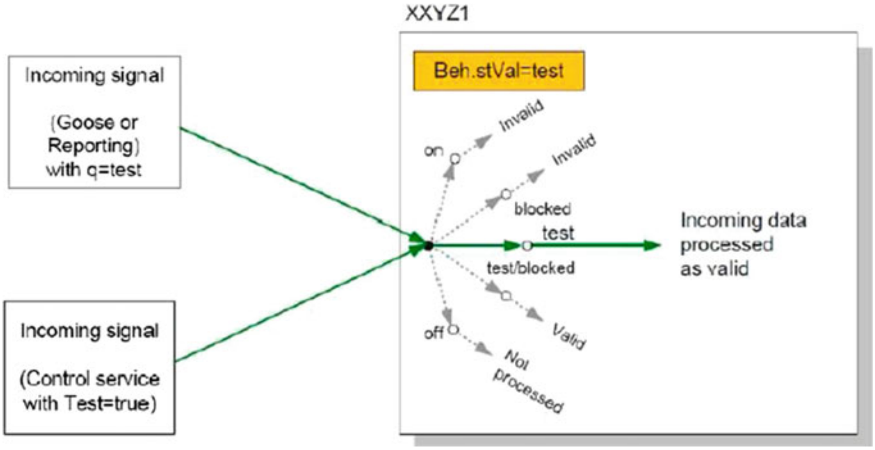


Fig. 9.9 Modes of logical nodes [IEC 61850-7-1, Fig. 42]

A command with test value of FALSE to a LN with ≪Beh≫ = test will not be processed. When Mod is set to test/blocked, it will behave as in test but the result of the processed reactions will not be issued as physical output to the process. IEC 61850-7-4 Annex A (cf. Table 9.2) provides a detailed explanation of the behaviour for various settings of the data object Mod.

9.3.1.4 Logical Device Management Hierarchy

The management of logical nodes according to Edition 2 of IEC 61850 is based on the functional hierarchy represented by the nesting of logical devices. Logical devices are used to represent a group of typical automation, protection or other functions. The functions are defined as groupings of function elements represented by logical nodes in the IEC 61850 object model. The logical nodes are contained and managed in logical devices.

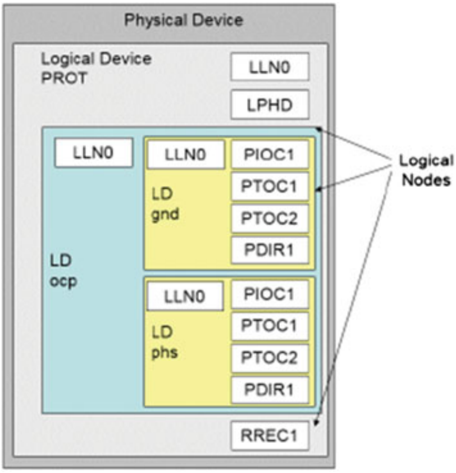
In a multifunctional protection IED, we typically have several main functions:

- Protection
- Automation
- Control
- Measurements
- Recording
- Condition monitoring
- Other

Depending on the type of protection IED, each function may contain several subfunctions. For example, in a distribution feeder protection IED we may have:

- Overcurrent protection

Fig. 9.10 Nesting of logical devices representing the functional hierarchy



- Overvoltage protection
- Underfrequency protection

Figure 9.10 shows an example of a protection logical device PROT which contains a nested logical device ocp, representing the overcurrent protection sub-function. PROT is called the ‘root’ logical device.

The *LD ocp* contains two more logical devices—gnd and phs, which accordingly represent the ground and phase overcurrent protection sub-functions.

LLN0 of the logical device *LD ocp* contains a setting data named GrRef whose common data class is ORG (‘object reference setting group’). The referenced value of GrRef in *LD ocp* is PROT, meaning that the logical device function refers to the functional group represented by the logical device PROT. Likewise, LLN0 of *LD gnd* refers to the functional group represented by the logical device *LD ocp*. In other words, LNs in *LD gnd* are sub-functions of *LD ocp*.

The use of the object reference GrRef is shown in Fig. 9.11. The management of the behaviour within a logical device is based on the Mod setting of its LLN0, which contains common information for the LD like health, mode, behaviour and name plate. The hierarchy determines how the mode (e.g. on, off, test) of these functions and sub-functions is managed. The referenced value of GrRef is PROT, meaning that the logical device function refers to the functional group represented by the logical device PROT. The hierarchical management of the mode and behaviour is shown in Fig. 9.11. The mode of the LNs in LD gnd may be changed individually or globally by means of LLN0 of *LD gnd*.

Their mode may also be changed either by means of LLN0 of *LD ocp* or by means of LLN0 of *LD PROT*. For example, if the mode of the functional group *LD ocp* is set to ‘off’, it not only sets the behaviour of all logical nodes in *LD ocp* to ‘off’ but also the behaviour of all logical nodes *in LD gnd*. Switching the mode of *LD PROT* will affect the behaviour of all logical devices and logical nodes

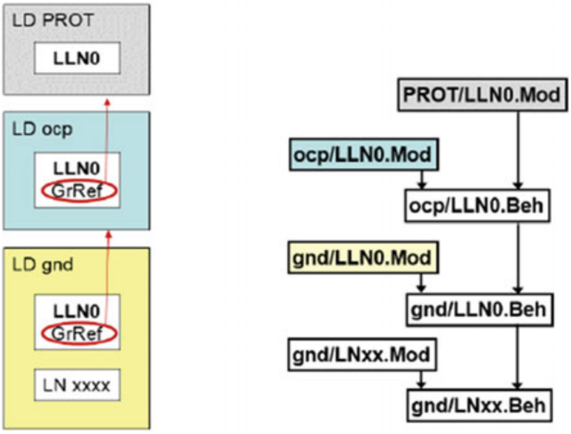


Fig. 9.11 Use of GrRef

belonging to the functional group *LD PROT*, i.e. all logical nodes in *LD PROT, LD ocp*, and *LD gnd* and *LD phs.*

Such hierarchical management of the mode and behaviour allows a very efficient control of the different functions and sub-functions implemented in a multifunctional IED. This is designed in particular to enable testing at different levels.

9.3.1.5 Processing of Attributes of Input Data

Information is transmitted between a publishing function and a subscribing function, including the status value or measurement value of a data object. The publishing function is also expected to convey additional information, such as data quality and time stamps. This information of the value is necessary for the correct understanding and processing of the value by the subscribing function. Different data attributes can be used as inputs for the subscribing function which define how to handle the value in an application-specific way.

If the test bit in the quality attribute of a data object is different from the behaviour (Beh) of the subscribing function, the application deals with the input in a way which reflects the definitions in the IEC 61850-7-4 Table A2 ([05]), Fig. 9.12.

For a function which is ‘on’ or ‘blocked’, the user expects that its processing is not affected by information published by another function under test. Commands marked as ‘test’ are not considered for processing by functions operating normally. Therefore, the application of a function in ‘on’ or ‘blocked’ state must ignore input data with ≪q.test≫ set to TRUE.

Logical nodes publishing states of physical inputs can also be in test mode. This can be used by the operators to indicate that tests are performed.

- with a test set representing the primary equipment,
- on the primary equipment itself,
- on the secondary equipment.

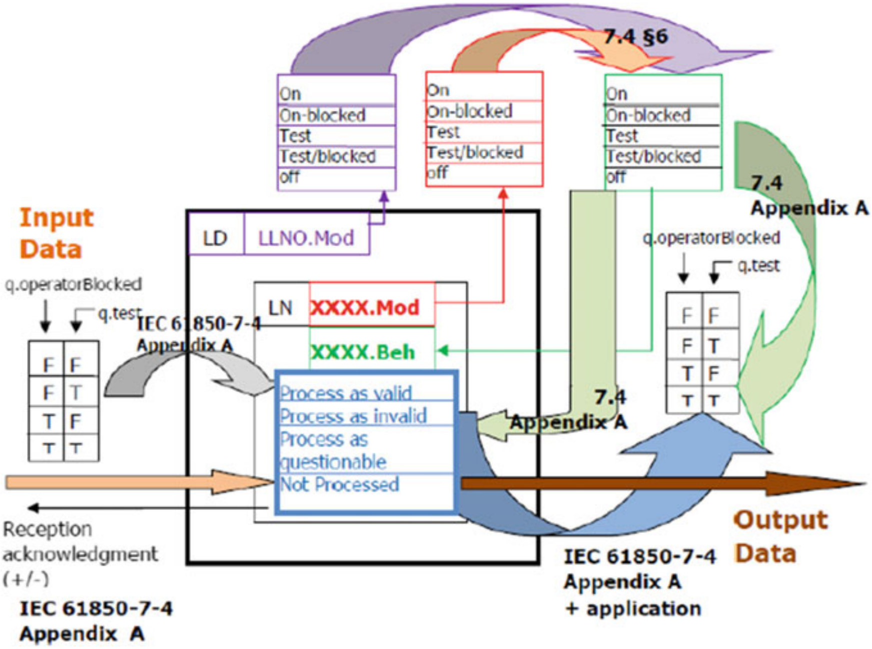


Fig. 9.12 Processing of the data by a LN depending on the LN mode and the quality of the input data

Since the test bit (e.g. XCBR.Pos.q.test) will be set to TRUE for these tests, these inputs have to be processed accordingly.

A function which is set to 'test' or to 'test/blocked' processes 'as valid' all messages with ≪q.test≫ = FALSE and messages with ≪q.test≫ = TRUE (cf. Table 2), ≪q.validity≫ = GOOD assumed. This characteristic has an important impact on the test methodology. Table 9.2 summarises the processing principles expressed in various chapters of the standard. These principles are needed to secure the interoperability of functions in the way the user expects applications to work.

The 'invalid' indication is typically known in conjunction with measurement values, but not limited to. Stronger than with an indication 'questionable' where a processing of the value is conceivable (depending on the application), 'invalid' unambiguously indicates that a value is not to be used. In the subscribing function, the communication services note that information was received, but the application does not consider the value for its processing. For a better understanding why a value is ranked 'invalid' or 'questionable', detailed quality identifiers are provided. Overflow, Out of Range, Bad Reference, Oscillatory and Failure lead to an indication 'invalid', and Out of Range, Bad Reference, Oscillatory, Old data, Inconsistent and Inaccurate lead to an indication 'questionable'. The subscribing function can evaluate the detailed quality identifiers to derive the most appropriate way of processing of the information. This expected behaviour of the subscribing

Table 9.2 IEC 61850-7-4 Ed 2.1 Annex A Table A.2

Mode/behaviour	on	blocked	test	test/blocked	off
Function behind LN	ON	ON	ON	ON	OFF
Output to the process (Switchgear) via a non-IEC 61850 link for example wire (typical for $X\ldots$,$Y\ldots$ and GGIO LNs)	YES	NO	YES	NO	NO
Output of FC ST, MX (issued independently from Beh)	Value is relevant q is relevant	Value is relevant q is relevant	Value is relevant q.test = true	Value is relevant q.test = true	Value is irrelevant q.validity = invalid
Response to (normal) command from client (a+ / a− acknowledgement)	a+ pos. ack.	a+ pos. ack.	a− neg. ack.	a− neg. ack.	a− neg. ack.
Response to TEST command from client (a+ / a− acknowledgement)	a− neg. ack.	a− neg. ack.	a+ pos. ack.	a+ pos. ack.	a− neg. ack.
Incoming data with validity = good AND test = false AND operatorBlocked = false	Processed as valid	Processed as valid	Processed as valid	Processed as valid	Not Processed
Incoming data with validity = questionable AND test = false AND operatorBlocked = true	Processed as questionable	Processed as questionable	Processed as questionable	Processed as questionable	Not Processed
Incoming data with validity = good AND test = true AND operatorBlocked = false	Processed as invalid	Processed as invalid	Processed as valid	Processed as valid	Not Processed
Incoming data with validity = questionable AND test = true AND operatorBlocked=true	Processed as invalid	Processed as invalid	Processed as questionable	Processed as questionable	Not Processed

(continued)

Table 9.2 (continued)

Mode/behaviour	on	blocked	test	test/blocked	off
Incoming data with validity = invalid AND test = don't care AND operatorBlocked = don't care	Processed as invalid	Processed as invalid	Processed as invalid	Processed as invalid	Not Processed
Non-IEC 61850 binary (relay, contact) inputs and analogue (instrument transformer) inputs	Processed	Processed	Processed	Processed	Not Processed

functions upon reception of invalid or questionable data should be specified and included in the test scope.

It is worth noting that more than one quality indication may be set to TRUE at the same time.

As a rule, a dataset using Function Common Data Attributes (FCDA) shall also include the quality information associated with a status value or measurement value. The Function Common Data (FCD) includes this information in their structure.

9.3.1.6 Blocking of Information

In Fig. 9.13, the different possibilities to intervene into a given communication scheme of functions are shown. The activation of physical outputs (contacts, analogue ports) of functions which have a direct interaction with the process can be blocked by setting the function to 'blocked' or 'test/blocked' status using the control service on the controllable object 'Mod'. The status evaluation of physical inputs can be influenced by an oscillation suppression feature, if implemented in the application. This feature is defined by the configuration.

Blocking of communication inputs.

The acceptance of commands can be prohibited by activating 'CmdBlk'. This blocking affects simultaneously all controllable objects of the logical node, except for the data object 'Mod' which is always accessible. If 'CmdBlk' is activated, access through control services is rejected.

Application example: This feature can be used to prevent from inadvertent triggering of a function (e.g. commanding of a switchgear). The function processes the other input data normally and publishes the output data normally.

Blocking of communication outputs.

The operator is able to block communication outputs by setting 'blkEna' to TRUE. This intervention is done on data level, i.e. on the individual information produced by a function. Upon activation of 'blkEna' on a certain data object, the update of

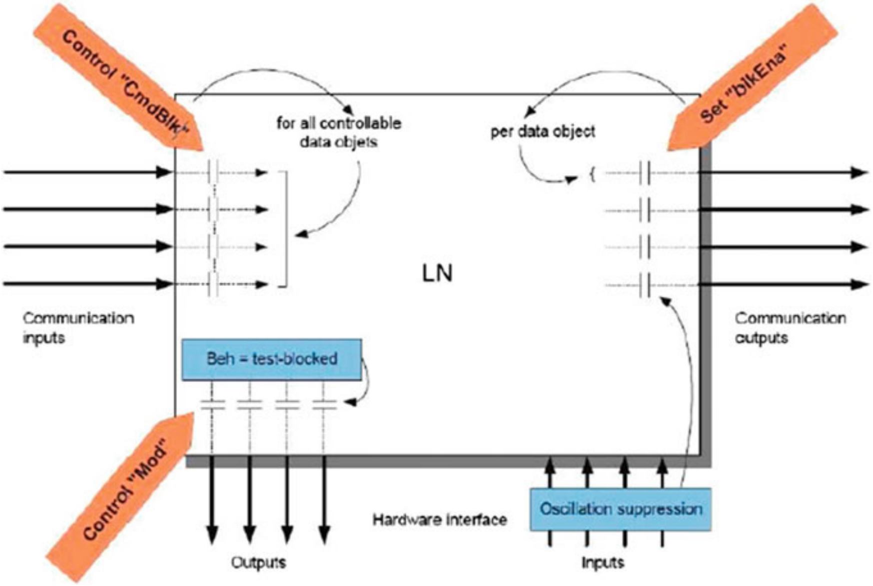


Fig. 9.13 Data used for logical node inputs/outputs blocking ([05]) [IEC 61850-7-1, Fig. 39]

this data is stopped and the indications ‘operatorBlocked’ and ‘oldData’ are set to the associated data quality, as the value is no longer updated.

‘blkEna’ has effect on data object level and, therefore, is different from the logical node modes ‘blocked’ or ‘test/blocked’, which affect the physical process outputs of the functions.

9.3.1.7 Changing the Information Source (InRef) for Testing

The input signals to an LN can be switched between process signals from other functions and tests signals from functions dedicated for testing (even from testing devices) defined through the data object InRef as shown conceptually in Fig. 9.14. This does not depend on the Behaviour of the logical node, and the data is processed and published according to the Behaviour.

Data attribute ≪setSrcRef≫ specifies the object reference to the input that is normally used as input while ≪setTstRev≫ specifies the reference to data object used for testing. By setting the data attribute ≪tstEna≫ to TRUE, the application will use the test signal referred to by ≪setTstRef≫ instead of the data object referenced by ≪setSrcRef≫ used for normal operation. A function LN can have multiple instances of ≪InRef≫ for multiple inputs.

By means of switching over the input reference from the process signal, which may be not accessible or cannot be modified, to a signal which can be easily modified (tstEna set to TRUE), an application can be isolated on the input side from the process and fed with test signals (value and data quality information). This

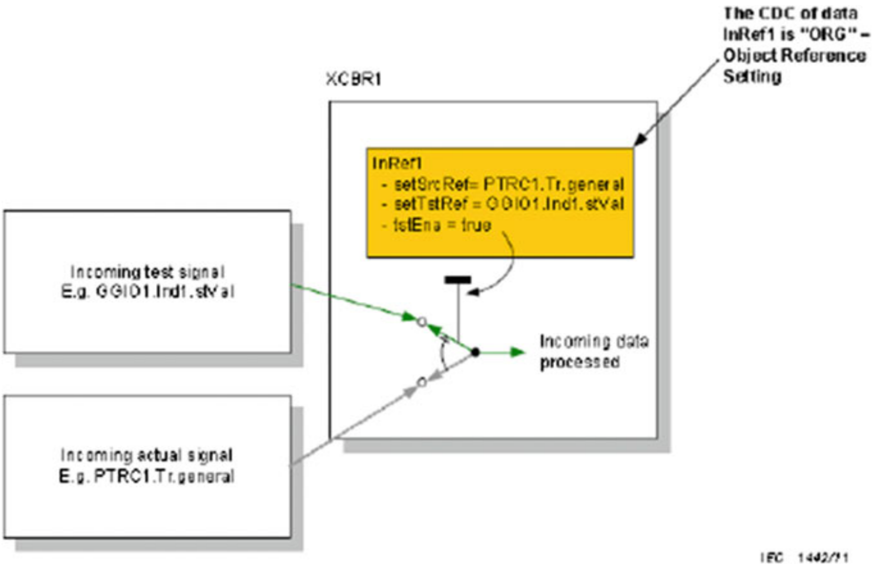


Fig. 9.14 Example of input signals used for testing (IEC 61850-7-1, Fig. 41)

feature requires to have an extra function at hand which allows a controlled generation (e.g. from a front panel pushbutton) of these signals. In case this function is hosted in a device external to the IED under test, the data flow has to be prepared (e.g. GOOSE subscription) in the device configuration. InRef is applicable to all types of Data Objects including Sampled Values.

This feature is different from the use of the Simulation mode which affects the entire IED and is limited to GOOSE communication, while 'tstEna' has effect on the information sourcing of a single input (Fig. 9.15).

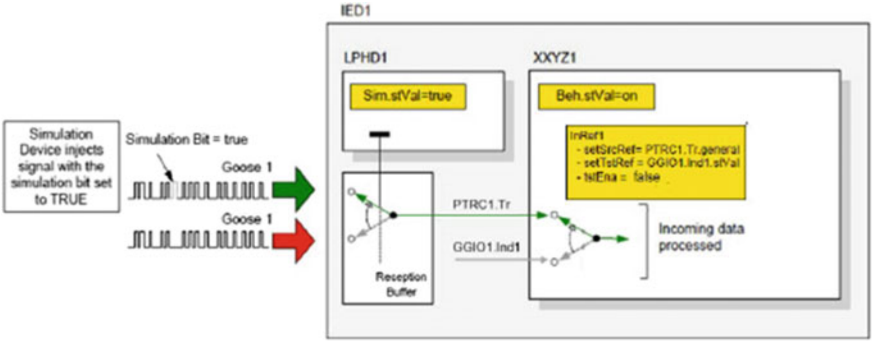


Fig. 9.15 Use of InRef by simulation mode [IEC 61850-7-1, Fig. 40]

Some signals subscribed by LD under test may be not strictly necessary for the tests (e.g. SF6 pressure of CB, etc.). Ideally, the test set should be capable to generate all these input signals and the LN should be defined with an individual TstEna for every single input. This has to be included in the system design in the engineering phase.

Consequence of this would be an ‘automatic’ configuration of the test set depending on the characteristics of the feeder. Normally, all information can be found in the SCD file.

9.4 Application and Implementation of IEC 61850 Test Features [1]

As stated in Sect. 9.3, the application of the test features proposed by IEC 61850 ed2 implies a verification of the status of the incoming data. The status of the published data depends on the status of the input data and on the status of the logical node. In this context, IEC 61850 Ed2 has some requirements concerning the processing of the data, namely IEC 61850-7-4 Annex A. For the quality attribute, these requirements are represented in Fig. 13 of IEC 61850-7-4 Annex A.

As a matter of interoperability, functions must be provided with an implementation of the data quality processing rules as given in the standard. These requirements are however quite general and need clarification in the context of an implementation or a PACS specification. Only if all functions participating in a scheme are processing data quality with the same understanding, an effective isolation and testing of a function can be reached.

A special attention is required for the definition of the expected behaviour of LN processing heterogeneous data, i.e. data with inconsistent simulation or quality tags.

9.4.1 Use of Simulation

The simulation described in the standard is applicable in the LPHD at the level of the Physical Device and defines the processing of the data by the communication processor of the Physical Device. This somehow limits the use of Simulation for maintenance tests, as logical devices cannot be tested independently from other LD in the same IED who may have to stay operational.

If the implementation of Sampled Values Control Blocks in Merging Units allows publishing of more than one data stream of the same content (identified by different SVCB and identifiers) and the processing capability of the subscribing IED allows to subscribe to a number of SV streams simultaneously, then individual functions could be assigned different SV streams to subscribe to. For testing, this permits to continue feeding parts of the IED functionality with data coming from the process, while the functions under test can be fed from a simulation device.

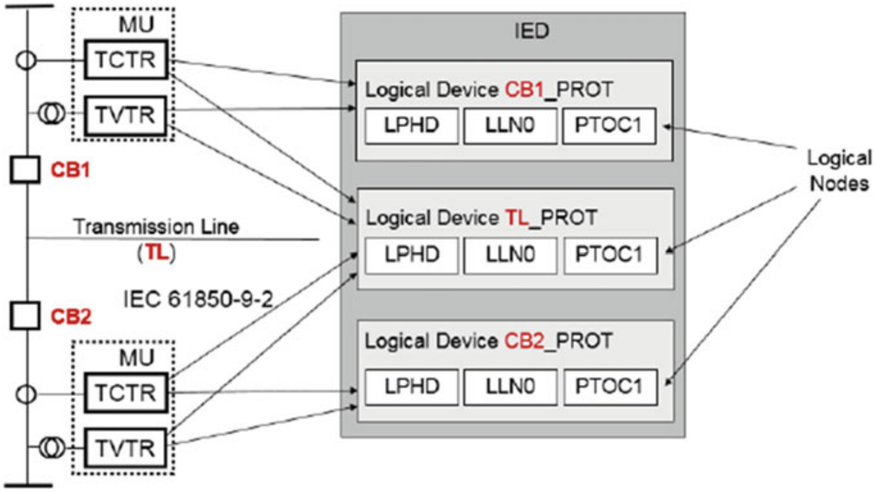


Fig. 9.16 IED with multiple process interfaces

This concept requires an in-depth knowledge of the IED architecture and may not be suitable for being applied by all users.

Figure 9.16 gives an example of the use of multifunctional IED for the transmission line protection in a breaker and a half or ring bus configuration.

In this case, a single IED requires separate interfaces with the merging units on each of the individual breakers (CB1 and CB2). If we are to test, for example, a PTOC function element tripping CB1, we will need only sampled values simulation for CB1.

If we are to test a PTOC function element tripping CB2, we will need only sampled values simulation for CB2.

The simulation as defined in IEC 61850 may still work, since the switch to using simulated values starts only after receiving the first message with the Simulation parameter set to TRUE.

The use of Simulation flag may however be an appropriate way to test IED containing only one function or a homogenous group of functions, as this is often the case up to now for protection relays. The principle is illustrated in Fig. 9.17.

In order to use the simulation flag, LPHD.Sim of the receiving Physical Device must adopt the value ‘TRUE’ and the simulation bit in the message from the test device also must be ‘TRUE’, according to IEC 61850 parts 7-2 and 7-4. This message is generated by a test device and not by an IED of the PACS.

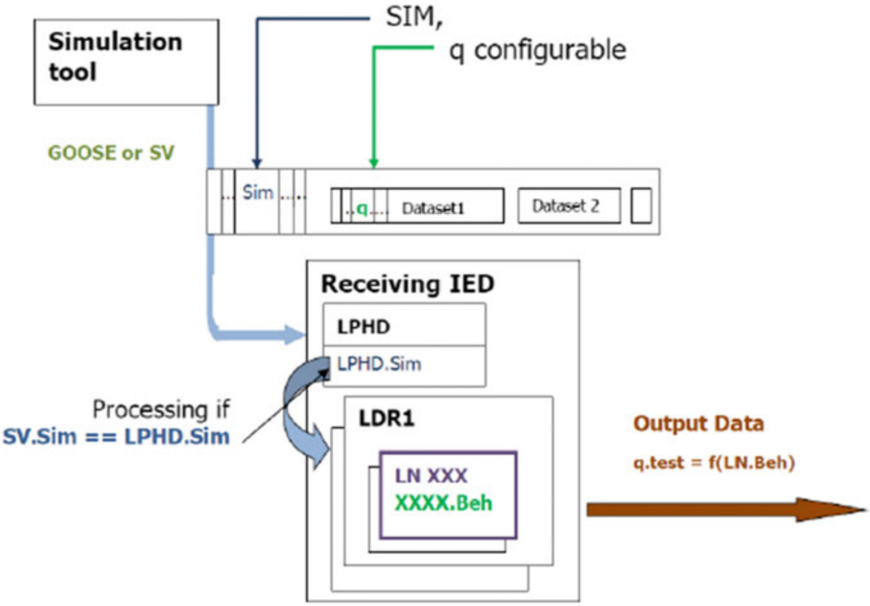


Fig. 9.17 Scheme of the application of simulation on processing of data

9.4.2 Case of Heterogeneous Quality Attributes in Input Data

When performing tests in an operating PACS, there will be at the same time.

- operating LD in 'on' mode which has to continue to interact with the process in a nominal way.
- LD under test with quality data attributes different from nominal state and/or SIM parameter set.

There will thus be operating logical devices receiving so-called heterogeneous data. It is important to specify the expected behaviour of these logical devices. It is possible that different behaviours are required, depending on the function.

It is thus recommended to define a generic behaviour in the specification describing the implementation of IEC 61850 test features and to leave the possibility to define a specific behaviour for each function if the generic behaviour is not convenient. This means that the expected behaviour for each function (each LD) has to be established and validated. This is a prerequisite for the testing of such schemes.

An example for LD receiving heterogeneous quality attributes is given in Fig. 9.18, where the LD called ATB has to process two streams coming from two different Merging Units. If one of the two MU is in test mode (SAMU2), e.g. because of a test performed on LD PX also shown in Fig. 9.22, LD ATB will be

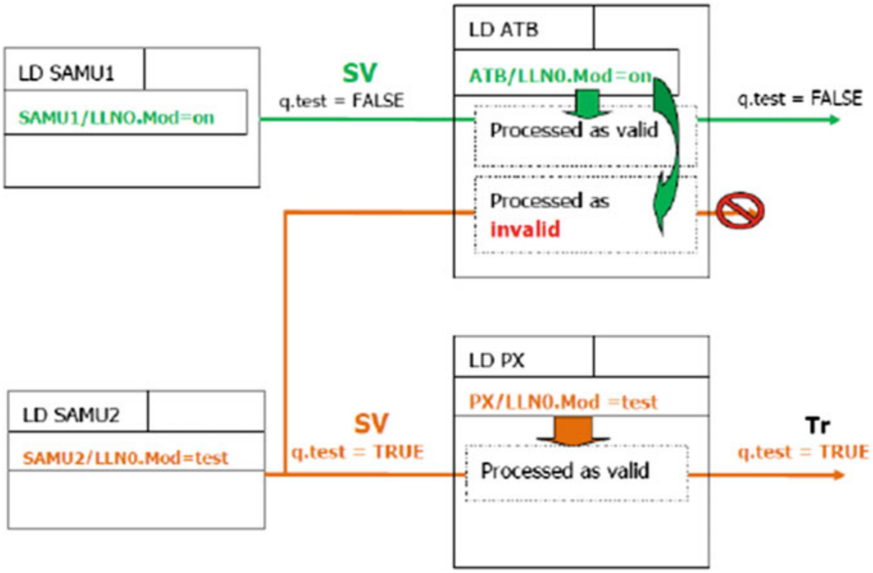


Fig. 9.18 LD receiving heterogeneous quality attributes

faced with a SV stream coming from SAMU1 in normal mode (q.test = FALSE) and another stream coming from SAMU2 in test mode (q.test = TRUE). This is one example for LD subscribing input data with heterogeneous quality attributes.

Since LD ATB itself is in normal operation, it has to process the SV stream coming from SAMU2 as invalid according to IEC 61850-7-4. What this means in particular for the function ATB has to be specified by the user.

Specifications should take into account the following statements when describing the implementation of IEC 61850 test features:

If not indicated otherwise in the specification of the application, heterogeneous input data are processed as follows:

- **test**: If LN.Beh = on or blocked, then data with attribute q.test = TRUE has to be ‘processed as invalid’. The function continues to work without taking into account these entries. The way to do this has to be clarified for each function in the specification. The data are published with q.test = FALSE.

  If LN.Beh = test or test/blocked, then data with attribute q.test = FALSE has to be processed as valid according to IEC61850-7-4 Table A2. The operation of the function is nominal, and the data are published with q.test = TRUE.
- **operatorBlocked**: The way to handle Incoming data with attribute q.operatorBlocked = TRUE has to be clarified for each function in the specification. The outgoing data are published with a value for q.operatorBlocked according to the behaviour of the LN.

- **Source**: The value of q.Source of the published data has to be clarified for each function in the specification.
- **validity**: For each function, the specification should describe how incoming data with attribute q.validity = INVALID has to be processed.

The way to handle incoming data with q.validity = QUESTIONNABLE has to be clarified for each function in the specification.

The definition of the impact of these quality attributes on the behaviour of function elements is considered out of scope of this Technical Brochure. However, it has to be clearly specified for the design of the functions and has to be tested as part of the type testing of the developer and of the acceptance testing of the user.

9.5 Support of Testing-Related Features [1]

To allow testing, especially maintenance testing, where it is essential to functionally isolate the object (function, physical device) under test, the IEDs must have the appropriate IEC 61850 implementation. It is the intended testing philosophy for the PACS which dictates the requirements towards the implementation. So, already in the design phase of a project the testing concept must be defined, as it impacts the selection of the IEDs.

For the selection of the PACS equipment, the user needs to know the capabilities of the following:

- testing-related features as given in IEC 61850,
- communication services,
- control blocks and datasets (for additional test-related messaging),
- data streams of Sampled Value subscription,

In addition, understanding of the IED internal architecture, i.e. the functional hierarchy and the interactions of functions, is required to know where to apply the IEC 61850 testing-related features.

The user can retrieve information from the following sources to understand the level of support in the IED implementation:

- **Technical brochure, user manual**
  The testing-related features supported in an IED must be listed in the technical brochure of the device. Their full description must be given in the user manual.
- **Model Implementation Conformance Statement (MICS), typical content**
  The typical content of a MICS presents the data model of an IED rather than the testing-related element provided by the IED. This document does not provide the required level of information to learn about the implementation of testing-related features.
- **Protocol Implementation Conformance Statement (PICS)** The typical content of a PICS presents the supported communication services of an IED.

This document provides the required level of information to learn about the implementation of testing-related features.

- **Protocol Implementation eXtra Information for Testing (PIXIT) document** Since the ICD describes all information elements implemented in an IED, only sparse information about the implementation of testing-related features can be found in the PIXIT. This document does not provide the required level of information to learn about the implementation of testing-related features.
- **IED Capability Description (ICD)** The ICD is the machine-readable engineering artefact for the IEC 61850 implementation of an IED software. It describes the data model and the supported protocol services as well as the numbers of various elements (report control block instances, datasets, e.g.) available.

  In the ICD, the user can also detect on the data object instance the elements which are needed for a service (for blocking of an output, e.g.). If an element is there, then the associated service is supported; vice versa, if the element cannot be detected, then the service is not supported.

  As it is understood that not all the users are experts enough to scrutinise SCL in order to conclude on the capabilities of an IED, UCAIug provides a software tool which creates a full Model Implementation Conformance Statement (MICS) document out of an ICD. In such a MICS, the required service elements are shown.

While the ICD describes the information elements existing in an IED, it does not state the functional support for each of them. Additional information has to be provided by the manufacturer, preferably in a machine-readable format for being processed in tools. SCL files should contain all sections defined in IEC 61850-6.

9.6 Requirements for Testing Tools [1]

This section describes requirements for test tools. Beyond the requirements described in this section, the test tools also have to produce a test documentation which corresponds to user requirements.

9.6.1 Requirements for the Device Injecting Test Signals

One of the main issues covered in IEC 61850 Part 4 System and Project Management is the quality assurance process which requires that the manufacturer and the system integrator should establish and maintain a quality system in accordance with ISO 9001.

The stages of quality assurance as a responsibility of the manufacturer and system integrator as defined in the standard are shown in Fig. 9.19.

The document defines several types of tests that should be covered as part of the system's life cycle, as well as the requirements for the test system to be used.

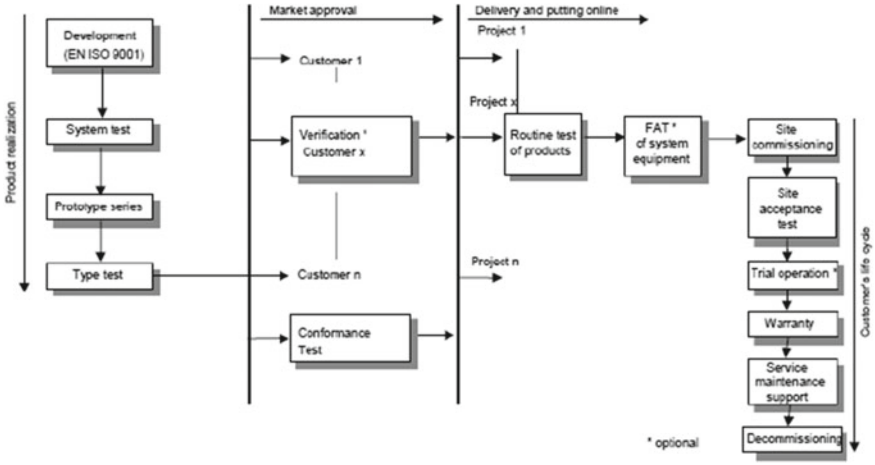


Fig. 9.19 Quality assurance process ([05]) [IEC 61850–4, Fig. 7]

According to IEC 61850 part 4, the test equipment includes all equipment that is required for the acceptance test and commissioning. It is used to provide the verification of all inputs and outputs of the primary equipment, the communication with the network control centre and the functionality of the individual IEDs of the automation system, such as protection and control.

It is considered that the test system may consist of several test devices and/or software tools.

Additionally, the test system is necessary to prove the behaviour and the performance characteristics of the automation system and its components. With respect to the functionality and performance requirements, the test system is divided into three categories:

- normal process simulation,
- transient and fault process simulation,
- communication check and simulation.

The test equipment used to simulate the Normal Process, in its simplest form, must be able to provide all alarms and position indications for the control system, enable the simulation of measured values (including overrange) and be able to display all commands from the automation system.

More complex test equipment must be able to simulate reactions of the switchgear in real time. Such test equipment can be used to check dynamic processes such as switching sequences or synchronisation. There is a need to be able to generate various conditions for the reactions, for example to produce intermediate positions of switchgear or to simulate an earth fault on one busbar section during a switching sequence.

Test equipment should also be capable of generating a large quantity of data traffic in a short time or intermittent data traffic on a regular basis.

The test equipment should be capable of injecting simulated or replayed transients of voltages and currents in a three-phase power system, simulating many types of faults or other abnormal processes such as power swing, saturation of current transformers and others. It also should be capable of producing simulated faults, thus producing disturbance records.

The communication test equipment is used for performing tests at all communication channels for:

- internal links of the automation system
- telecommunication

The communication test system should be a convenient and efficient tool which enables the performance of the following functions at all required levels (network control centre, substation, bay and process level):

- simulation of a server, simulation of a client, monitoring of the data traffic;
- quality analysis of the data traffic (e.g. the quality of electrical signals, time breaks, jitter, latency, etc.).

In addition to the above-defined requirements for the test system, it is necessary to define some requirements specific to the testing of IEC 61850-based digital substation protection, automation and control systems:

- The test system should be compliant with the testing-related features defined in IEC 61850 Edition 2,
- The test system should be capable to act as a IEC 61850 client,
- The test system should be configurable using IEC 61850 SCL files,
- The test system should be capable of operating in a normal mode (simulating the normal operation of an IED with Sim = FALSE) or in simulation mode (Sim = TRUE),
- The test system should be capable of configuring all individual parts of the quality attribute as required by the test case (e.g. validity, test, source, etc.),
- The test system should be capable of checking the Test bit in the quality attribute if TRUE or FALSE as required by the test case,
- The test system should be capable of time synchronisation based on IEEE 1588 and PTP defined in IEC 61850-9-3-related standards including the possibility for the user to choose the value of the synchronisation data attribute (GLOBAL, LOCAL, NOT SYNCHRONISED),
- The test system should be capable of simulating or causing loss/alteration of SV/GOOSE.
- The test system should be capable of analysing the performance of the system under test and generate a test report including the test conditions and reflecting the results of this analysis.

- The test system should be capable of testing both client and server functionality.
- The test system should be capable of supporting automated testing based on the capabilities of the system under test. This may include the possibility to change settings of functions, enable or disable sub-functions of functional elements or other as necessary.

9.6.2 Implementation Considerations for the Test System

It is considered to be a good practice to separate the control of the test system from PACS under test. This means that the test system components are only connected to the PACS for injection of test signals and monitoring test responses. This also means that the control between test computer and test devices should use a separated network segment (Fig. 9.20). For remote testing, the test computer has to be connected to the cloud.

The test system components can be divided into two main groups:

- Hardware,
- Software

The hardware of the test system may include different types of devices depending on the requirements of the test:

- Computers
- Test devices with one or more of the following interfaces
  - communications interface (e.g. direct injection of SV and GOOSE)
  - binary I/O
  - low-level analogue signals interface (e.g. for systems with Rogowski coils)
  - secondary level analogue signals interface (1A or 5A, 100 V corresponding to a conventional test device, e.g. for SAMU)
  - primary values or pseudo primary values (e.g. for testing of LPIT)
- Amplifiers converting low-level analogue signals interface to secondary analogue signals interface (e.g. to interface network simulators to the system under test)
- Communications equipment—switches and routers

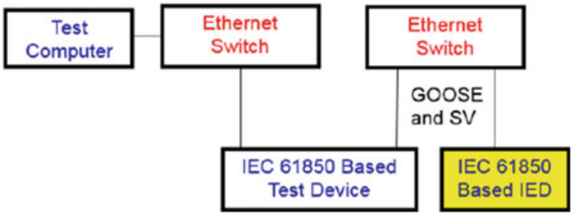


Fig. 9.20 Single test device testing system architecture

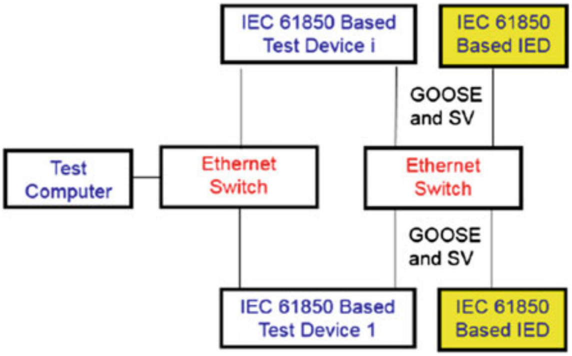


Fig. 9.21 Distributed testing system architecture

- GPS antennas and receivers
- Clocks

The hardware architecture of the system also depends on the requirements of the test and the capabilities of the components of the test system. If the test object is a single IED or a combination of merging unit and IED, a single test device may be sufficient for the testing as shown in Fig. 9.20.

However, if the test includes End-to-End Testing, the test system may need to include multiple test devices synchronised using IEC 61850 9-3 in different physical locations controlled by a test computer as shown in Fig. 9.21.

The second component of the test system is the software. The software can be of three kinds:

- Embedded in the test devices,
- Applications running on computer hardware,
- Applications running in a cloud.

The software performs different functions, such as:

- Normal and abnormal conditions simulation as defined by the testing requirements
- Control of the mode of the test object,
- Monitoring the performance of the test object,
- Documenting the results from the test.

During testing, the status changes inside an IED must be monitored. Typically, there are three ways to capture live data of an IED: reporting, GOOSE messaging and MMS reading. The configuration of an IED has to be prepared to support testing, in order to enable the IED to report to a test client. The test device may subscribe to information published by the Device Under Test (DUT). The piece of information needed during testing has to be included in the GOOSE dataset.

In order to access information, the test system must be equipped with one or more of the following features:

- **MMS Browser** to actively read out data elements from the DUT by means of MMS Read, either in single-shot mode upon request or continuously acquired ('polling') to update dedicated views.

In case the IED configuration was prepared to support testing, then it can be sufficient to.

- **Writing** (trigger options, option fields and report enable) **to Report Control Blocks for testing**

and/or.

- **Writing** (GOOSE enable) **to GOOSE Control Blocks for testing**

In special cases, if the IED configuration was not prepared in the engineering phase, the following additional features are required. It is however not recommended to use this approach in an operational system without prior testing:

- **Creation of datasets for testing**

  which reference the desired information. To save the resources of the DUT, the type 'non-persistent' can be chosen, if supported by the DUT.
- **Writing to Report Control Blocks for testing**

  to configure the RCB, submit reporting options and to enable the reporting.
- **Writing to GOOSE Control Blocks for testing**

  to configure the GoCB and to enable the GOOSE publishing.

Depending on the test scenario, the analysis of the test results may require access to recordings of the monitoring system during the test. It also may be required to add additional features to the HMI of the PACS that support the testing process.

The HMI of the test system should include the following features:

- Support import of SCL files.
- Configuration and management of test scenarios
- Assignment of test devices to simulate primary and secondary components according to test scenarios.
- Display and export of test report.

9.6.3 Features Required to Support Remote Testing

If testing tools are connected to the PACS on a permanent basis, the next logical step would be to perform tests remotely. This can be useful in case of a large distance between the substation and the base of the test staff.

The following features of the PACS and the testing tool are required in order to undertake remotely controlled testing:

1. The possibility to remotely configure and operate the test tool. The remote access of the testing tool should be independent of the PACS to be tested. This means that an independent communication link has to be provided. PACS process and station bus should not be used to operate the testing tool since this could have unwanted effects on the test results.
2. The possibility to remotely retrieve the test results. This includes recordings of the test tool itself, recordings of additional monitoring equipment connected to the PACS (e.g. Ethernet Traffic Analyzer) and recordings of the PACS itself (COMTRADE or COMFEDE files). As mentioned above, the test and monitoring tools should use communication channels which are independent of the tested PACS.
3. The possibility to put the PACS itself remotely in the expected initial state required by the test procedure. This may include to put the IED or LD of the functions to be tested in SIM or test mode.

The remote testing concept can be implemented using different methods. One of these options is shown in Fig. 9.22.

The test system in the substation includes several components:

- Test computer which runs the testing software supporting IEC 61850 Edition 2 testing features and the required functional testing tools.
- Test devices performing simulation and evaluation of the results from each test.

It is necessary to have the capacity to accurately measure the performance of all components of the tested scheme within the real communications architecture of the PACS. For this reason, the test system has to be physically located in the substation.

The interface to the test computer is recommended to be established over a private cloud and requires the use of cybersecurity technology available for remote access from the engineering station by an authorised and authenticated user, which should include role-based access.

Depending on the requirements for maintenance testing that needs to be performed, the logical nodes, logical devices or complete IEDs are set in the required mode in order to ensure their virtual isolation. It is evident that the remote testing procedure itself has to be properly tested and validated. The operating staff has to have reasonable confidence in the remote test devices and procedures.

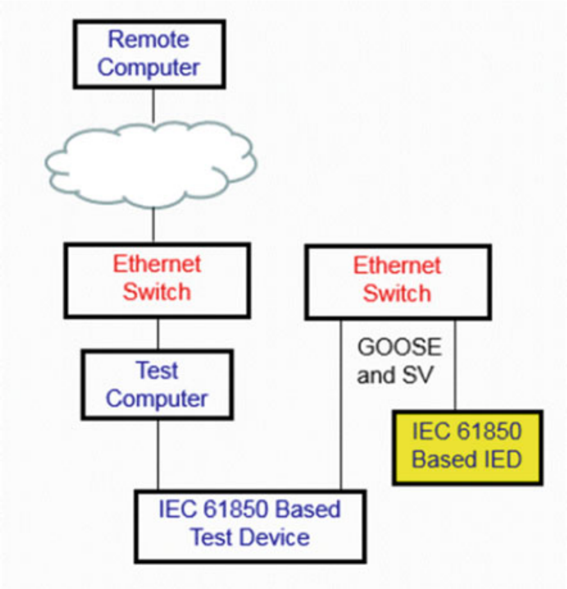


Fig. 9.22 Remote testing system components

In order to avoid risks related to the communication link, it is recommended to download a test script into the test device and remotely launch the test sequence. This approach does not require a permanent and stable communication link during the test sequence. The PACS should have the ability to exit from a remote test and autonomously recover to a defined known state (e.g. a PACS state captured before the start of the test sequence) in case of timeout or unpredictable events during the test and loss of control of the test system.

Remote testing can be envisaged during the following situations:

- after replacement of an IED by local staff and remote or on-site configuration of the new IED.
- after a maloperation or a failure to operate.
- after remote or on-site updates of parameters, settings or configuration of an existing IED.
- after modifications of equipment connected to the process-bus interface of the PACS.

The corresponding tests should be designed in order to verify that all functions concerned by the modifications are operating correctly and are properly interfaced with the PACS.

9.7 Test Methodology and Assessment [1]

Functional testing methods can be divided into several categories. They are related to the complexity of the functionality of the individual devices being used in the different levels of the hierarchical system, as well as the types of distributed functions implemented in it. This requires the selection of the right testing method for the specific type of test, as well as the use of testing tools that can automate the testing process.

From this point of view, the following are the more commonly used testing types:

- Functional element testing
- Integration testing
- Function testing
- System testing

A function in this case can be considered as a sub-system with a different level of complexity, for example a system monitoring function, while the system is the complete redundant protection system.

Regardless of what is being tested, the test object needs to meet the requirement for testability. This is a design characteristic which allows the status (operable, inoperable, or degrade) of a system or any of its sub-systems to be confidently determined in a timely fashion. Testability identifies those attributes of system design which facilitate the verification of the behaviour of components that affect system performance. From the point of view of testability, a functional element in a protection system is the unit that can be tested, because it is the smallest element that can exist by itself and exchange information with its peers in the protection system.

Another consideration is the purpose of the test. It also needs to be clarified if the tests are performed in relation to acceptance of a new product or function, the engineering and commissioning of a substation component or the complete protection system or its maintenance. From that perspective, different testing methods can be implemented even in the testing of the same functional element or function.

For example, the testing of a system monitoring function during the user acceptance phase may focus on the testing of the measuring element characteristic using search test methods, while during the commissioning the operating times for different system conditions are the important ones achieved through transient simulation methods.

The knowledge of the internal behaviour of the test object or more specifically the logic or algorithms implemented determine how the tests are being executed. The most commonly used test methods from this point of view are as follows:

- Black box testing
- White box testing

An important aspect that needs to be considered during the testing is the availability of redundant devices performing the different protection system functions.

The following sections discuss in more detail the different testing methods listed above.

9.7.1 Black Box Testing

Black box testing is a very commonly used test method where the tester views the test object as a black box. This means that we are not concerned with the internal behaviour and structure of the tested function. Test data are derived solely from the specifications without taking advantage of knowledge of the internal structure of the function (Fig. 9.23).

Black box testing is typically used for:

- functional element testing
- PACS factory testing
- PACS site acceptance testing

Since functional elements are defined as units that are the smallest that can exist independently and are testable, black box testing is usually the only method that can be used for their testing.

The response of the test object to the stimuli can be monitored by the test system using the operation of physical outputs, communications messages or reports.

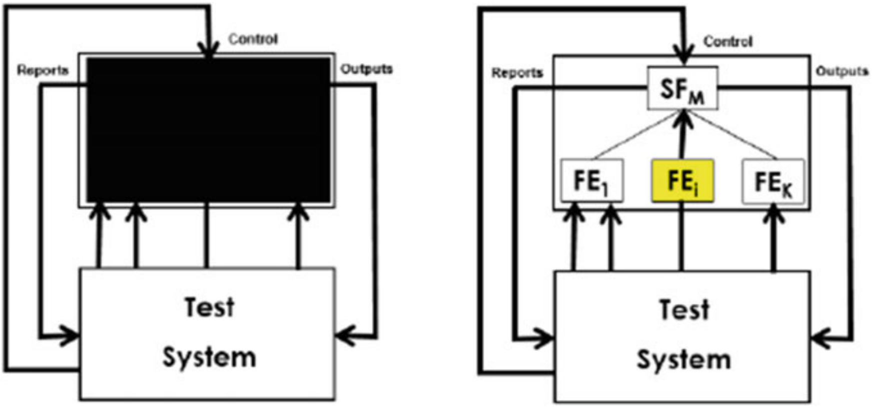


Fig. 9.23 Black box and white box testing

9.7.2 White Box Testing

White box testing is a method where the test system is not only concerned with the operation of the test object under the test conditions, but also views its internal behaviour and structure. In the case of a protection system, it means that it will not only monitor the operation of the system at its function boundary, but also monitor the exchange of signals between different components of the system (Fig. 9.23).

The testing strategy allows us to examine the internal structure of the test object and is useful in the case of analysis of its behaviour, especially when its test failed.

In using this strategy, the test system derives test data from examination of the test object's logic without neglecting the requirements in the specification. The goal of this test method is to achieve high test coverage through examination of the operation of different components of a complex function and the exchange of signals or messages between them under the test conditions.

This method is especially useful during the test of distributed functions based on different logical interfaces. The observation of the behaviour of the sub-functions or functional elements is achieved by monitoring of the exchange of messages between the components of the test object.

The test scenarios however do not have to be different from the ones used under black box testing.

In IEC 61850-based systems, white box testing is fairly easy to achieve using the subscription to GOOSE messages whose data sets contain data attributes representing the status of all function elements that are used in the implementation of the tested function.

9.7.3 Top-Down Testing

Top-down testing is a method that can be widely used for a PACS, especially during site acceptance testing, when we can assume that all the components of the system have already been configured and tested.

Top-down testing can be performed using both a black box and a white box testing method.

The testing starts with the complete system. If the test fails, a new test is performed at the next lower functional level. The process continues down the function hierarchy until the reason of the failure is identified, including sub-function testing and if necessary functional element testing.

In the case of factory acceptance testing, when not all components of a system or sub-system are available, it is necessary for the test system to be able to simulate their operation as expected under the test scenario conditions. In this case, the test system has to represent functions or functional elements that are not yet available.

Each functional element is tested according to a functional element test plan, with a top-down strategy.

If we consider a PACS implementation in IEC 61850 for testing using a top-down approach, we will start with the definition of the function boundary.

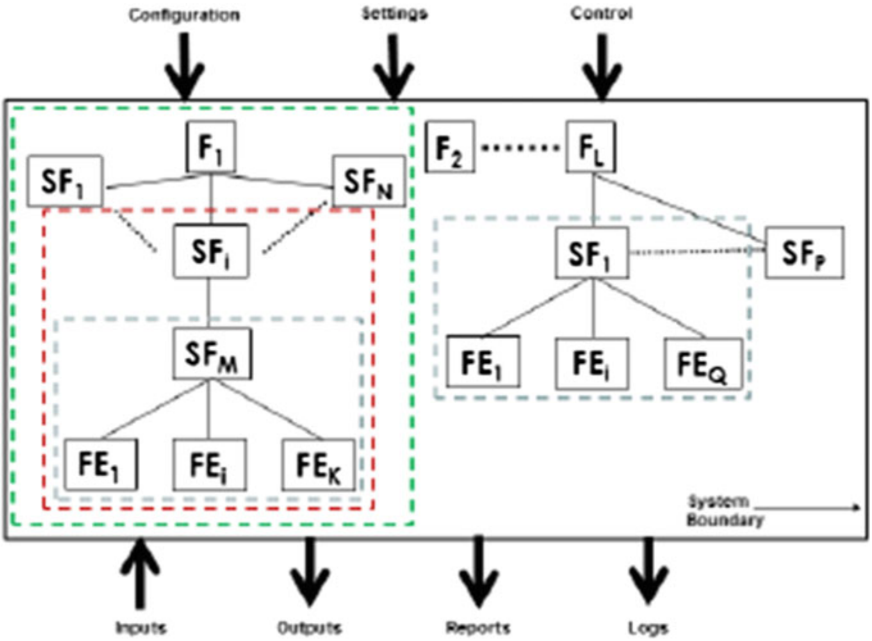


Fig. 9.24 Top-down testing of a system monitoring function

The testing of the individual components of a system function might be required in the case of failure of a specific test, which is shown in Fig. 9.24. The function boundary for each of these tests is different and will require a different set of stimuli from the test system, as well as monitoring of the behaviour of functional elements using different signals or communications messages.

9.7.4 Bottom-Up Testing

Bottom-up testing is a method that starts with lower level functions—typically with the functional elements used in the system—for example PTOC.

This method is more suitable for type testing by a manufacturer or acceptance testing by the user.

When testing complex multilevel functions or systems, the test system must be able to simulate any missing component of the system when performing, for example, factory acceptance testing.

There are many similarities in the test scenarios used in the bottom-up, compared to the top-down method. The main difference between the two methods is the order in which the tests are performed and the number of tests required.

The bottom-up approach involves a higher number of tests which are necessary to ensure that everything is working as designed.

9.7.5 Positive and Negative Testing

Positive testing is a testing process where the system is validated against expected input data. In this testing, the tester always checks if an application behaves as expected with expected inputs.

Negative testing is a testing process where the system is validated against unexpected input data. A negative test checks if an application behaves as expected with unexpected inputs. The tester has to determine which unexpected inputs are meaningful for the tested functions.

9.8 Testing and Security [1]

When using a test set for testing in a Security Domain, during the test, the test set needs to become part of the Security Group being tested and must know the Symmetric Key for the group for a period of time. During the time when the test set is interfacing with the Security Group, it is known as a Temporary Cyber Asset or TCA (see Fig. 9.25).

When connected to the Security Domain, the test set requires that it be loaded with a certificate that identifies it as being a member of the Security Domain under test. The certificate can be created with a limited life that expires in a day or a week or as long as needed.

On start-up, the TCA will request the Symmetric Key for the group in which it will be performing testing. Upon validation of the certificate loaded into the TCA, and upon request of the TCA, a Symmetric Key will be provided to the requesting TCA. Once given the key, the TCA can then participate in the Security Group and encode/decode test data as per the test configuration and policies set by the KDC.

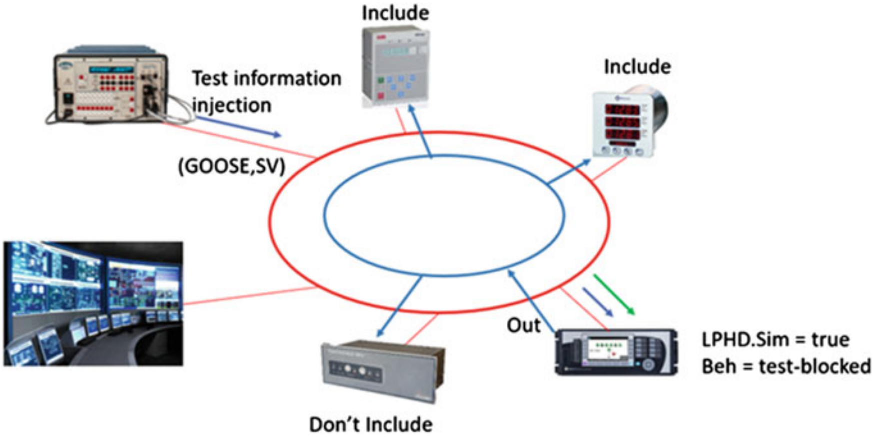


Fig. 9.25 Interface of a temporary cyber asset into a security group

9.9 Installation Test

The previous sections and sub-sections have outlined the methods, procedures and techniques for IEC 61850-based systems.

These installation tests for substations are true for all technologies of IEDs, and in the context of IEC 61850, this is applicable as well. These need to align with typical utility installation test procedures, which are highlighted below to complete this chapter.

The first stage of field testing is to verify the correct implementation of the physical installation. This means verifying the correct connection of the primary signals, and the local communication infrastructure, the Ethernet network in the yard of the process level and the station level in the control room.

The procedures in this sense involve the certification of the optical connections infrastructure. This phase should be carried out in compliance with utility guidelines which detail all procedures, test reports and required handover certification. As these tests are typically not carried out by the commissioning staff, there should be a formal handover with acceptance criteria. The amount of tests can be significantly reduced if routine tests and factory acceptance tests have been carried out.

The following tasks are carried out during this phase: The tests should be documented by the utility in a site pre-commissioning test document. Such a document would be created for each relay/scheme type.

Verification that all correct equipment is installed as per system design:

- AC and DC systems (Batteries, distribution boards, polarity tests)
- Instrument transformers (primary\secondary ratings, burdens, class, etc.)
- Verification that all equipment is installed correctly as per installation design
- No infringement on safety clearances
- Polarity orientation, earthing, etc.
- Verification that the earth grid is installed correctly and that all connections are compliant
- Verification of equipment nomenclature
- Verification that all wiring is installed and terminated as per installation design
- All cabling and termination complete as per design,
- Quality compliance cable types, terminals, shorting\isolation facilities
- Verification that all local communication is installed and terminated as per installation design
- LAN complete as per design,
- Optical and wiring communication cables
- Cabinet/panel wiring installed as per detailed design
- Powering up of all relays/control unit
- Formal certified handover to the utility

Some tests are visual tests to ensure that the correct equipment is installed in compliance with the design. Others are checks for signal continuity. And we also have those that refer to equipment configurations, such as switches.

References

1. CIGRE Technical Brochure 760: Test strategy for protection, automation and control (PAC) functions in a fully digital substation based on IEC 61850 applications. CIGRE WG B5.53. https://e-cigre.org/publication/760-test-strategy-for-protection-automation-and-control-pac-functions-in-a-fully-digital-substation-based-on-iec-61850-applications (2019)
2. IEC TR 61850-90-4:2020: Communication networks and systems for power utility automation—part 90–4: Network engineering guidelines. https://webstore.iec.ch/publication/64801

Vendor Interoperability of IEC 61850 Systems

10

Priyanka Mohapatra

Abstract

This chapter focuses on addressing interoperability aspects from utility perspective and through real-life applications of IEC 61850 standard and associated protocols in multi-vendor substations. It sets out the main expectations of utilities and end-users regarding multi-vendor interoperability; and then discusses the challenges faced by utilities while implementing digital substations based on IEC 61850. There are recommendations provided for both utilities and vendors, on how to improve the specification, engineering, implementation and testing of multi-vendor digital substations.

Keywords

SCD • SSD • ICD • CID • IEC 61850 • Specification • Engineering • Testing • Interoperability

10.1 Introduction

Interoperability is the ability of two or more intelligent electronic devices (IEDs) from the same or from different manufacturers, to exchange information in such a way that a correct functional co-operation between information producer and information recipient is achieved.

To achieve this goal, the standard provides the following key elements:

- Standardised class-oriented data modelling method to describe each possible data in its functional context which each tool and component in the system can

P. Mohapatra (✉)
Scottish Power, Glasgow, Scotland
e-mail: priyanka.mohapatra@web.de

P. Bishop and N.-K. C. Nair (eds.), *IEC 61850 Principles and Applications to Electric Power Systems*, CIGRE Green Books, https://doi.org/10.1007/978-3-031-24567-1_10

understand and process (as long as both sides are using the same common data class)
- Standardised file format for the data model description and the device capabilities between tools of different manufacturers
- Standardised communication procedures called services to facilitate system wide interaction between components of different manufacturers to act as a complete system
- Standardised mapping on a network to use unique communication and hardware layers
- Test methods definition to verify an interoperable behaviour of all system components during testing

Note: IEDs in this chapter refer to protection, control, monitoring IEDs and where applicable substation Ethernet switches as well.

10.2 Interoperability

Since its inception, IEC 61850 has been targeted to achieve interoperability in recognition of the engineering difficulties associated with a huge proliferation of varying data models and protocols. In classical terms, interoperability can be generally defined according to IEC 61850-1 as follows:

> Interoperability is the ability of two or more IEDs from the same vendor, or from different vendors, to exchange information and use that information for correct execution of specified functions.

This definition includes two important aspects. They are information exchange and correct interpretation of the information exchanged. Figure 10.1 below depicts the concept of interoperability.

There are many instances of system implementation where the utilities and asset owners have chosen a particular vendor as the equipment supplier for the entire system, or perhaps in duplicated redundant systems as one vendor for system “X” and one for system “Y”. A utility substation can consist of multiple vendor IEDs. In an ideal IEC 61850 implementation the multi-vendor IEDs must comply by the following two key aspects of interoperability:

1. Real-time communication interoperability between devices over the LAN.
2. Engineering interoperability during different engineering stages and between different engineering tools.

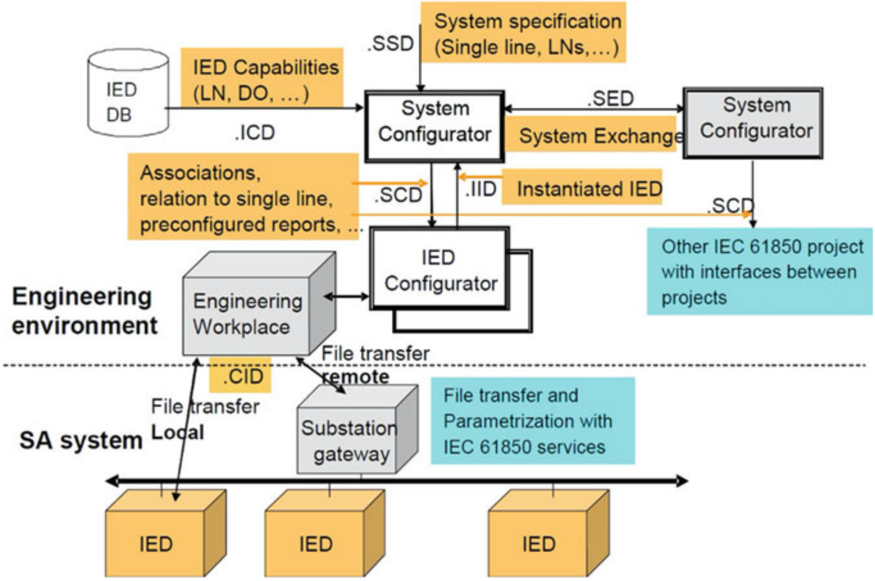

.SSD
System specification (Single line, LNs,...)
IED DB
IED Capabilities (LN, DO, ...)
.ICD
System Configurator
.SED
System Exchange
System Configurator
Associations, relation to single line, preconfigured reports, ...
.SCD
.IID
Instantiated IED
.SCD
Other IEC 61850 project with interfaces between projects
Engineering environment
Engineering Workplace
IED Configurator
File transfer remote
.CID
File transfer Local
SA system
Substation gateway
File transfer and Parametrization with IEC 61850 services
IED
IED
IED

Fig. 10.1 Reference model for information flow in the configuration process (*source* IEC 61850-6:2009 Figure 1)

10.2.1 Interoperability Versus Interchangeability

The IEC 61850 standard was developed with the goal of providing interoperability as a key component. Although the standard has a clear definition of what is meant by interoperability, end-user interpretation may exceed this definition and interoperability is sometimes understood as interchangeability or even plug-and-play. As described later in the brochure, interoperability is expected not only between IEDs of a digital substation but also between engineering and testing tools [1]. Therefore, it is important to understand the basic differences between interoperability and interchangeability at the outset of this chapter. Approaching the subject of interoperability from an informed and reasonable view of its requirements and limitations allows any utility and/or system integrator to create a set of specifications and establish processes that can be met by commercially available IEDs and will indeed deliver efficiencies through roll-out of IEC61850 substations.

Interoperability between multi-vendor IEDs according to various IEC 61850 and related standards requires the IEDs to be able to configured using a common language with engineering tools (which includes IED configuration tool), tested with any test tool with ability to interpret the common language and communicate to exchange information over an Ethernet-based network in real-time independent of the original manufacturer.

Interchangeability in pure sense requires a vendor IED to be replaced with another vendor IED during operation and maintenance without any requirement for IED specific re-engineering and testing. Interchangeability is not specified or required by the IEC 61850 standard and also inhibited by many factors in the IEC 61850 compliant implementation, some of which are listed below:

1. IED interface tools are proprietary for all vendors. This requires re-engineering of the IED based on the IED configuration definition (ICD) of the new file.
2. Performance, functional and application considerations of IEDs require retesting of IEDs during replacement of IEDs.

This chapter focusses only on the interoperability aspect between multi-vendor devices only and does not discuss interchangeability.

10.3 Standardisation Committees and Working Groups Enhancing IEC 61850 Interoperability

ENTSO-E Europe has done significant research and explained the utilities expectations on those regards in its statement and related documents published in 2012 [2]. This statement was an important trigger for all stakeholders to join efforts at the standardisation level, e.g. in IEC TC57 (Power system control and associated communications) WG10.

Currently, the Osmose 1 project and its sub-task 7.1 "Interoperability" is an advanced R&D project aiming to demonstrate the effectiveness of standardisation work and notably the full multi-vendor interoperability of the top-down engineering process, with an industrial demonstrator in two configurations combining products from several vendors including IEDs, system and device tools. To achieve top-down engineering process, the concept of virtual IED was introduced as an update to the IEC 61850 engineering cycle to support the specification and system configuration stages. It is an IED specification (a planned IED/LN) template that can be used during the system configuration stage, allowing later mapping to actual devices to be performed after system configuration is complete (validated or even simulated). This template can be represented by an IED Specification Definition (ISD) file which can be used to create an system specification description (SSD) file based on these virtual IED templates. A device ICD file can then be compared to the ISD file to ensure compatibility before creating the system configuration definition (SCD) file. This enables a layer of engineering interoperability between system design and implementation, also further supporting the procurement and selection of different IEDs for the same system build-up. In IEC TC 57, there is ongoing work to introduce the concept of doing, e.g. a specification in system configuration language (SCL) using virtual IEDs for a future release of Technical Report IEC 61850-6-100.

This report being inherently relevant to the recommendations and experiences in multi-vendor interoperability in IEC 61850, parts and diagrams from the report have been referenced to throughout this chapter.

10.4 Business Case for Multi-vendor Interoperability

There are number of reasons why an electric utility may want to benefit from interoperability. These may include the following ([1]):

1. leveraging features across different product lines within the same vendor or from multiple vendors;
2. reduction of common mode of failure by using different vendor products in protection schemes;
3. benefitting from leading edge features from different vendors;
4. management of device obsolescence requiring usage of newer devices within existing installations;
5. optimisation of asset management.

In the following sections, we will analyse some of these drivers in detail.

10.4.1 Functional Requirements

In power system substations, IEDs perform multiple functions. These range from analogue to digital conversion performed by merging units (MUs), stand-alone merging units (SAMUs) and switching control units (SCUs), protection and control and system monitoring. There are multiple vendors that offer IEDs specific to each of the functions. There are global vendors that have a bigger product portfolio and they can offer a range of products that can perform all the functions as per the requirements specified by the utility. However, in most cases different functions in the same substation are performed by IEDs from multiple vendors. Individual utility criteria for selection of substation devices often qualify devices from different vendors.

In a conventional substation, multi-vendor interoperability is limited to the requirement of functional interoperability. In IEC 61850-based digital substations the requirement for multi-vendor interoperability extends to engineering design and communication level. Such approach tends to avoid discrepancies about where any problems need to be resolved. However, it is rare that any one vendor has a complete range of IEDs to suit the complete system functional requirements. Equally, due to the life of the substation automation system, it would be rare that the system integrator at the outset is likely to be the same system integrator at every addition, refurbishment or system replacement.

10.4.2 Regulatory Requirements

The operational regulations in many countries require some critical functions in high-voltage substations to be duplicated, sometimes with constraints as with two different vendor devices and/or over different platforms. The requirement is in place to avoid single type and/or point of failure in critical protection IEDs. In all high-voltage substations under such regulatory requirements, protection functions are either duplicated or separated over multiple vendor platforms. One of the main requirements of transition to digital substations is to maintain the same level of redundancy and availability as in a conventional substation. The same two principles of multi-vendor interoperability apply to comply by the requirement of multi-vendor IEDs in digital substations.

10.4.3 Serviceability

Operations and maintenance requirements in substations require IEDs to be easily serviceable and replaceable. Utilities often stock up spare IEDs to prepare for such situations. It is important that vendors maintain firmware versions which are backward compatible with older models of the IEDs. Additionally, it is important that utilities should be able to replace one vendor IED with that from another vendor offering the same functionality with the required changes to the engineering design and with proper steps taken during testing in commissioning. While interchangeability is not required by the standard itself, interoperability between a newly replaced IED and existing IEDs as well as the Substation Automation System (SAS) is crucial.

10.5 Role of Standardisation in Ensuring Multi-vendor Interoperability

Within the overall structure of IEC 61850, Part 10 is “Conformance testing”. This sets out the requirements for claiming IEC 61850 compliance in respect of the core interoperability related parts of.

- Part 6: engineering process file exchange
- Part 7-1: data model
- Part 7-2: data model
- Part 7-3: data model
- Part 7-4: data model
- Part 8-1: communication services as required
- Part 9-2: communication services as required

Conformance testing was added to verify that the implementations of IEC 61850 into devices and tools of different manufacturers are conformant to this standard. Running a set of predefined test procedures, proof is given of the correct data modelling, implementation of services, provision of description files and documentation.

This testing only proves that there is no inconsistency between the data model, the description files and the documentation. The validation of which functional objects are modelled and how they are modelled is out of scope of conformance testing.

It is important to understand that "compliance" does not imply implementation of every possible feature of IEC 61850. There are many options in all aspects if IEC 61850 specifically to enable systems to be created as needed in the most efficient and economical manner.

In that respect sheer "compliance" does not in itself guarantee any degree of "random interoperability" for the specific function required to be implemented. Indeed the format of certificates states precisely the reverse of absolute compliance:

"The device has not been found to be non-compliant."
We would generally interpret that as meaning "whatever has been implemented has been done correctly".

It remains a responsibility of the asset owner and systems integrator to confirm that the various components of the system actually work interoperable to fulfil the functional requirements.

Part 10 however does provide a key starting point in that to obtain such Certification, the vendor must have provided key documentation about the IED:

- PICS: Protocol Implementation Conformance Specification
- MICS: Model Implementation Conformance Specification
- PiXIT: Protocol Implementation eXtra Information for Testing
- TICS: TISSUES Implementation Conformance Specification
- ICD: IEC Capability Description file

It is these pieces of information that enables the asset owner/systems integrator to begin the process of choosing IEDs that are indeed interoperable for the specific implementation.

Note that "compliance" of IEDs sometimes refers to compliance to the physical and environmental capabilities of the IED according to IEC 61850-3.

10.6 Ensuring Interoperability Through System Specifications

Multi-vendor IED interoperability is the fundamental requirement for successful engineering design of IEC 61850 substations. In such a conceptual model, as shown in Fig. 10.2, the capability of maintaining a single IEC 61850-based system model throughout the lifecycle (also known as the "virtual system") is deemed most important. Such a model can be accessed and manipulated by different tools of different vendors at different points in time for different engineering purposes—a true IEC 61850 tool environment across the lifecycle. This reinforces model-driven approaches, based on system configuration language (SCL) files with digital models automatically processable by tools (including IEC 61850

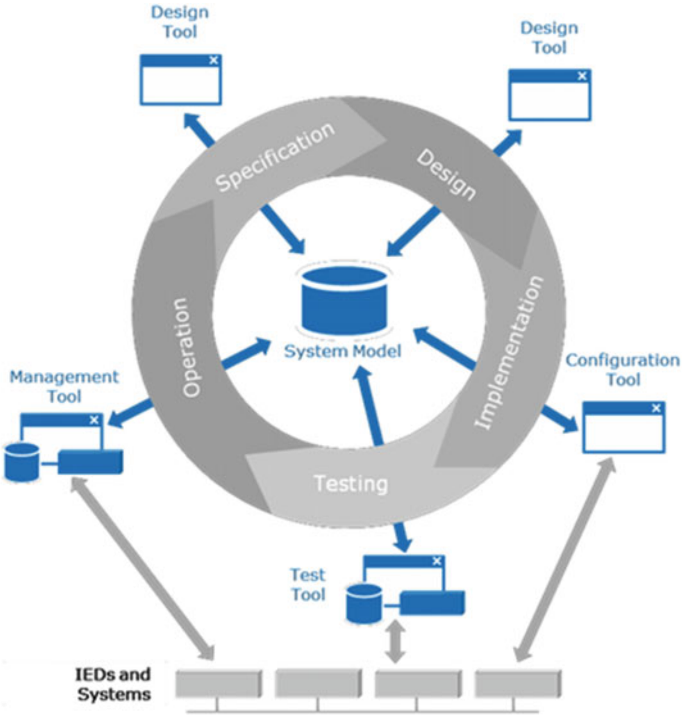


Fig. 10.2 System model and SCL-based lifecycle management process (*source* [1])

models, CAD models or other progressively integrated digital models), in favour of traditional document-driven processes, mostly processable by humans.

10.6.1 Multi-vendor Engineering Environment and Single System Model Across the Life Cycle

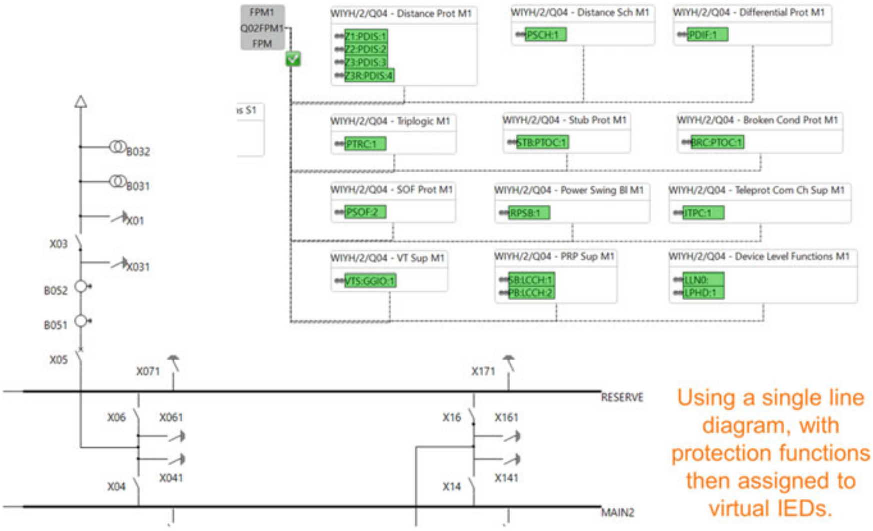
During the engineering design phase both with the bottom-up and top-down approach, multi-vendor IEDs need to be configured using the standard defined IED capability definition files (ICD) to produce system configuration definition (SCD) using IEC61850 defined SCL. The approaches taken in top-down engineering also require interoperability between the vendor IED configuration tool (ICT) and system configuration tool (SCT) and system specification tool (SST). Note: both SCT and SST could be the same software/tool. This section will look into some of the requirements for interoperability requirements and considerations while selecting a vendor independent SCT for engineering design of a multi-vendor substation based on utility specifications.

10.6.1.1 System Specifications

The SSD file is usually an utility specific specification file that defines the substation model and functions required for the utility template or specific substation specification—Fig. 10.3. The SSD file is based on individual company polices and requirements. The SSD file should contain of list of logical nodes and logical device structure that translates the conventional substation design to an IEC 61850-based specification. The definition of SSD file and compliance check of vendor IEDs by the SSD file ensures the first level of interoperability between vendor devices through qualification of functional elements in multi-vendor IEDs. The provision for Virtual IED and ISD in future SSD files enabled by the standard will also allow utilities to qualify individual IEDs against the specific functional requirements.

The key interoperability considerations during definition of system specifications. SSD file and device qualification are the following: (two additional requirements have been expressed by ENTSO-E [1]).

1. System engineering efficiency
   a. the possibility to define key primary system data (e.g. CT or VT ratio) and link them to other Data Object elements inside the SCL file that are dependent of it (e.g. global variable inherited through the SCL structure), ensuring therefore data consistency in an efficient way;
   b. the possibility to specify and maintain within the SCL file, the overall system functional requirements as logical nodes (or ANSI/IEEE C37.2 code



Using a single line diagram, with protection functions then assigned to virtual IEDs.

Fig. 10.3 .ssd file definitions (*source* SP Energy Networks) numbers) together with data regarding the number and type of modelling functions related to that code number; and

c. to enhance the efficiency of the engineering/purchasing process, gaps need to be identified to fully support the formal description of IED requirements. For example, Buffered Report Control Blocks capabilities, disturbance recording capabilities, accuracy, temperature ranges for monitoring purposes.

2. Communication Network Description
   a. the complete description of the communication network, including topology, characterisation of the network nodes (switches and routers), VLANs, etc. This would allow a seamless integration of a Network Engineering Tool, capable of importing a SCD file (see IEC 61850-90-4, clause 12.4). The configuration of the switches and routers would then be automatic from the SCD file.

10.6.1.2 System Specification Description (SSD) and Virtual IEDs

The process of defining SSD file will enable an automatic comparison between configuration files against specification files. This will accelerate the whole procurement process and provide higher transparency. Comparison tool should be developed on the market in order to facilitate this comparison process. There is a clear need for several comparison stages. For some users, the output of the SST could be an SSD with or without virtual IED's—depending on the user requirements on physical allocation—and it will be up to the system integrator (that can be the user himself) to choose ICDs to cover all functions and signals of the SSD. An SCD will only be created after first selecting the ICDs, and will not be available in a first comparison stage (for choosing the IEDs) of the process. A comparison between SSD/SCD is useful, for example, as a part of the SCD validation stage further in the engineering process in order to validate a configuration against a specification. Figure 10.4 illustrates this.

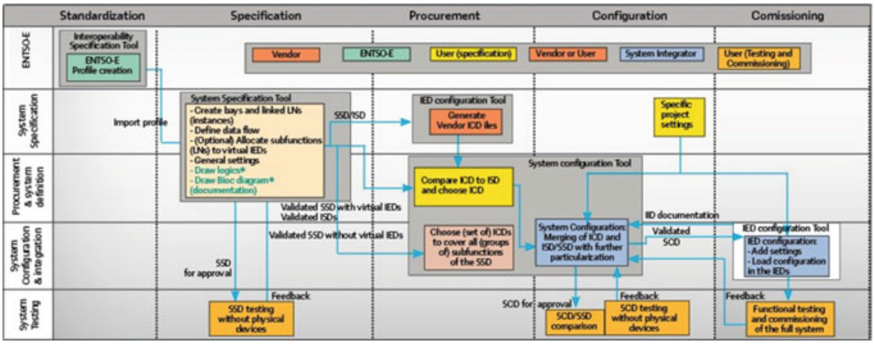

Standardization
Specification
Procurement
Configuration
Comissioning
ENTSO-E
System Specification
Procurement & system definition
System Configuration & integration
System Testing
Interoperability Specification Tool
ENTSO-E Profile creation
Vendor
ENTSO-E
User (specification)
Vendor or User
System Integrator
User (Testing and Commissioning)
Import profile
System Specification Tool
- Create bays and linked LNs (instances)
- Define data flow
- (Optional) Allocate subfunctions (LNs) to virtual IEDs
- General settings
- Draw logics*
- Draw Bloc diagram* (documentation)
SSD/ISD
IED configuration Tool
Generate Vendor ICD files
Specific project settings
System configuration Tool
Compare ICD to ISD and choose ICD
Validated SSD with virtual IEDs
Validated ISDs
Validated SSD without virtual IEDs
Choose (set of) ICDs to cover all (groups of) subfunctions of the SSD
System Configuration: Merging of ICD and ISD/SSD with further particularization
IID documentation
Validated SCD
IED configuration Tool
IED configuration: -Add settings -Load configuration in the IEDs
SSD for approval
Feedback
SSD testing without physical devices
SCD for approval
SCD/SSD comparison
Feedback
SCD testing without physical devices
Feedback
Functional testing and commissioning of the full system

Fig. 10.4 Extended engineering process with virtual IED definition and IED selection (*source* PAC World Magazine)

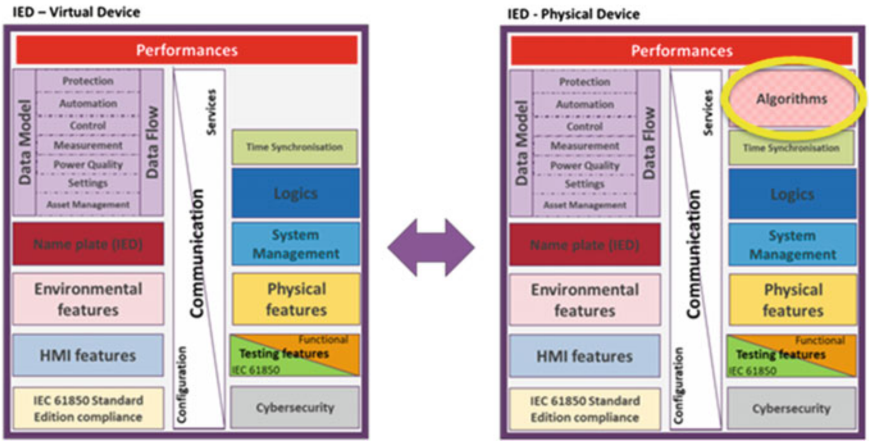


Fig. 10.5 Virtual device versus physical device (*source* PAC World Magazine)

The first requirement of creating System Engineering Efficiency is enabled through the extended engineering process depicted in Fig. 10.4 above. The concept of virtual IED compared to a real device is shown in Fig. 10.5. Communication wise, the virtual IED “looks” practically the same as a real IED, but it does not consist of the internal algorithms (at the upper right corner of the figure, marked with yellow), which determine the control or protection functionalities of the IED. The definition of virtual IED and comparison with physical IEDs ICDs is a key step in ensuring multi-vendor interoperability between the real physical devices during engineering and commissioning of digital substations. Inclusion of logical nodes as defined by the standard to exactly match the utility design specification. In the case of a particular functional and/or application requirement not modelled in the IEC 61850 standard, a query should be made to the standard for future consideration to expand logical node definitions. The use of flexible nodes or GGIOs should be limited to special applications. Utilities can enforce interoperability by strictly adhering to the standard. It will allow system specifications to be used across substations and with multi-vendor IEDs.

10.6.1.3 Flexible Product Naming

IEC 61850-5 Edition 2.1 introduces the concept of flexible product naming (FPN) which allows utilities to define user defined prefixes for standard IEC61850 logical node definitions. FPN allows the data model of an IED to be modified up to a certain level to reflect the hierarchy/structure defined by the overall scheme. The user, in control of the naming details is able to arrive at installation specific, manufacturer independent IED data model conventions. The data model definitions can be applied to all IEDs supporting this facility, to modify their Product Naming into data models which are conformant and relevant to both the site and customer specific conventions. Based on this customised data model, all relevant data can

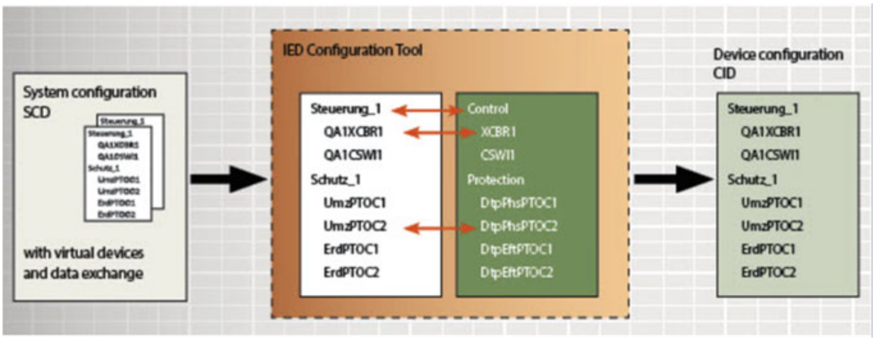


Fig. 10.6 Example for flexible product naming (*source* PAC World Magazine)

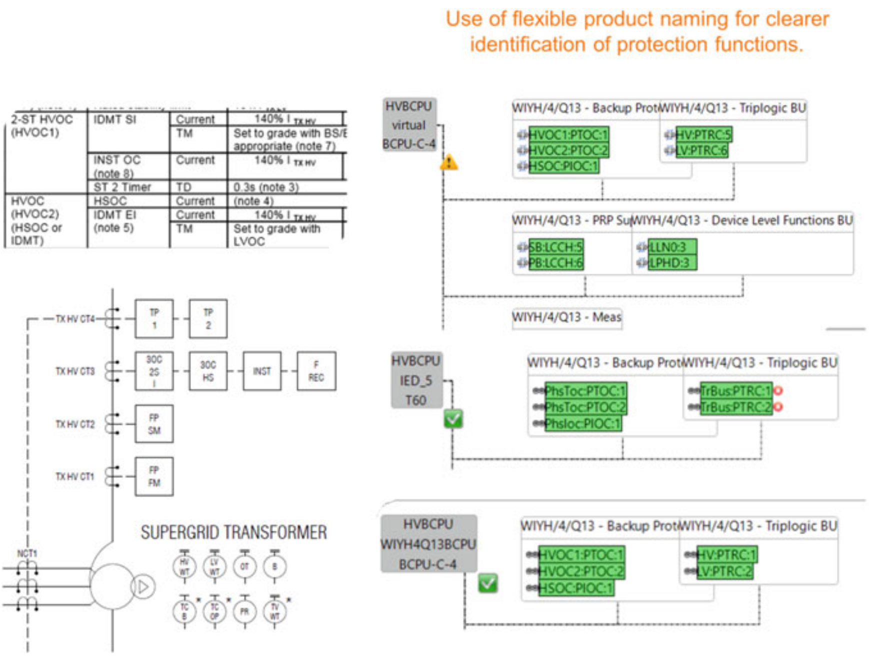
be exchanged between the IED and its communication peers in an interoperable way.

To reach any level of interchangeability, it is required to align the data models in the IEDs to have the same naming and semantic of all data exchanged. IEDs that allow to modify and to customise parts of the whole data models, provide "Flexible Product Naming" functionality. The vendor IEDs available commercially should support FPN. Utilities can make use of FPN to harmonise engineering designs across substations. FPN when used properly aids in on boarding of engineers more conversant with conventional substation design on to the IEC61850 terminology. As a recommendation, FPNs should be defined as per the conventional naming conventions.

When using the method of modifying the IED data model, the logical node instances (representations of the functions) can be renamed by changing the logical node prefixes or suffixes or both of them. The logical node classes and the data object names cannot be changed. LDname, a concatenation of IEDname and LDinst, can be changed as shown in the Figs. 10.6 and 10.7.

10.6.1.4 Template IEDs for Efficient Engineering

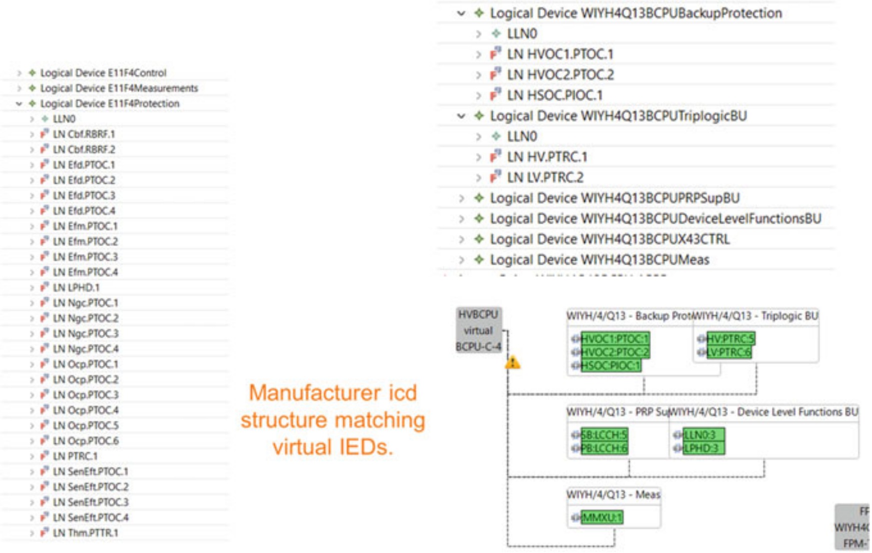
Asset owners can also create their template designs and libraries for typical type of power system bays and feeders to increase efficiency in design of future substations. These template designs and libraries should however be regularly updated to ensure that they are up to date with the changes in the standard. Utilities should also consider updating designs keeping in pace with multi-vendor products as vendors adapt to the changes to the standard for engineering design process in short term. It means that even as the standard introduces new concepts and features, it is important that utilities conduct regular market reviews and work collaboratively with vendors to create specifications that can be met by existing range of vendor products. Utilities however at the same time should specify future requirements according to developments in the standard to encourage vendors to upgrade IEDs according to the latest specifications. This interaction among the vendors and utility is captured through Fig. 10.8.



Use of flexible product naming for clearer identification of protection functions.

2-ST HVOC (HVOC1)	IDMT SI	Current	140% $I_{\text{TX HV}}$
		TM	Set to grade with BS/E appropriate (note 7)
	INST OC (note 8)	Current	140% $I_{\text{TX HV}}$
	ST 2 Timer	TD	0.3s (note 3)
HVOC (HVOC2) (HSOC or IDMT)	HSOC	Current	(note 4)
	IDMT EI (note 5)	Current	140% $I_{\text{TX HV}}$
		TM	Set to grade with LVOC

Fig. 10.7 Illustrates how a utility can choose to represent clearer identification of protection functions through the use of flexible product naming (*source* SP Energy Networks)



- Logical Device E11F4Control
- Logical Device E11F4Measurements
- Logical Device E11F4Protection
  - LLN0
  - LN Cbf.RBRF.1
  - LN Cbf.RBRF.2
  - LN Efd.PTOC.1
  - LN Efd.PTOC.2
  - LN Efd.PTOC.3
  - LN Efd.PTOC.4
  - LN Efm.PTOC.1
  - LN Efm.PTOC.2
  - LN Efm.PTOC.3
  - LN Efm.PTOC.4
  - LN LPHD.1
  - LN Ngc.PTOC.1
  - LN Ngc.PTOC.2
  - LN Ngc.PTOC.3
  - LN Ngc.PTOC.4
  - LN Ocp.PTOC.1
  - LN Ocp.PTOC.2
  - LN Ocp.PTOC.3
  - LN Ocp.PTOC.4
  - LN Ocp.PTOC.5
  - LN Ocp.PTOC.6
  - LN PTRC.1
  - LN SenEft.PTOC.1
  - LN SenEft.PTOC.2
  - LN SenEft.PTOC.3
  - LN SenEft.PTOC.4
  - LN Thm.PTTR.1

Manufacturer icd structure matching virtual IEDs.

- Logical Device WIYH4Q13BCPUBackupProtection
  - LLN0
  - LN HVOC1.PTOC.1
  - LN HVOC2.PTOC.2
  - LN HSOC.PIOC.1
- Logical Device WIYH4Q13BCPUTriplogicBU
  - LLN0
  - LN HV.PTRC.1
  - LN LV.PTRC.2
- Logical Device WIYH4Q13BCPUPRPSupBU
- Logical Device WIYH4Q13BCPUDeviceLevelFunctionsBU
- Logical Device WIYH4Q13BCPUX43CTRL
- Logical Device WIYH4Q13BCPUMeas

Fig. 10.8 Manufacturer's adopting ICD files to utility specification (*source* SP Energy Networks)

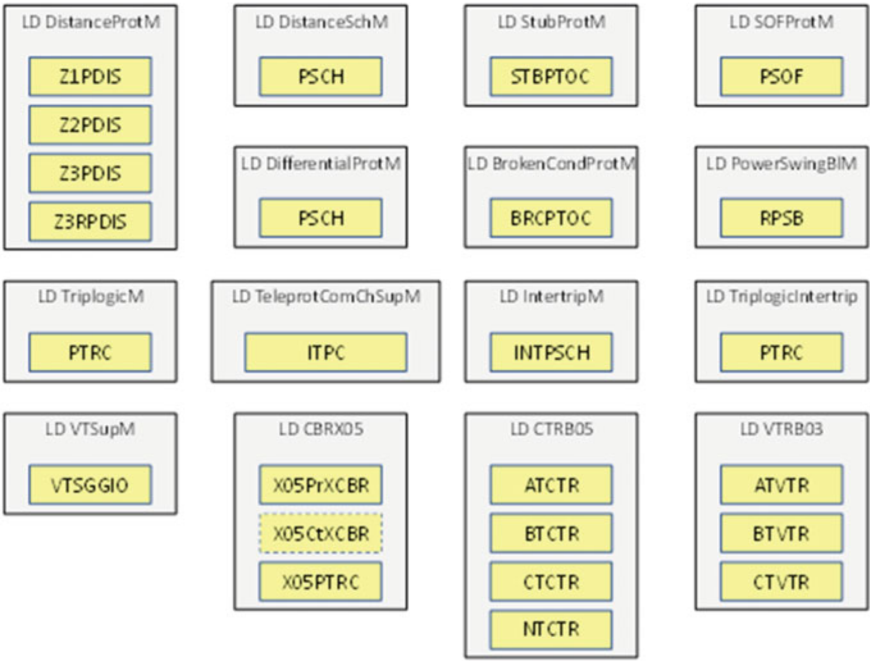


Fig. 10.9 Definition of number of logical node instances (*source* SP Energy Networks)

The substation design and definition of substation equipment should also be a part of the system specification definition. Utilities can assign various functional elements and logical nodes directly to the substation equipment and create dependencies for functions which cater for multiple bays. This allows for specification of right number of functional and logical node instances as illustrated in Fig. 10.9 for a particular utility implementation. It also ensures during the actual substation design phase utilities do not have to design tailor-made logics to make up for the shortage of functional instances in the IEDs.

10.7 System Configuration

The system configuration of multi-vendor substations can be carried out using two established methods: top-down and bottom-up engineering.

The bottom-up engineering process is mostly performed using the vendor ICTs then the configured IED description (CID) files are combined to create the substation SCD file. This is one of the approaches of achieving bottom-up engineering design. There are also methods of creating configurations for individual bays using multiple vendor ICTs and combining each of the bay SCD files to create the final SCD file.

In top-down engineering usually a SCT either 3rd party vendor independent or of one IED vendor is used to configure the whole substation which may consist of multi-vendor IEDs. The top-down engineering process especially in a multi-vendor application is more onerous on the system integrator and interoperability between multi-vendor IEDs ensures successful configuration of the substation. The SCD file produced through the top-down engineering process needs to be correctly parsed by the multi-vendor ICTs to successfully configure the IEDs. The top-down engineering process is currently not as smooth and ideal as the standard intends it to be. There are improvements required in this area especially around standardisation between the SCTs and multi-vendor ICTs to create a seamless top-down engineering process.

10.7.1 SCD Engineering

The overall SCD engineering using vendor independent SCT focusses mainly on creating GOOSE, SV publishing and subscription and report creation over MMS and establishing server–client relationship for each report. The final SCD should be a combination of substation elements inherited from the SSD or created in the SCD, vendor ICDs, configured GOOSE and reports.

The interoperability issues between an SCD created using a vendor independent SCT and the multi-vendor ICTs arise when the ICT cannot successfully interpret the SCD. This leads either to failed or partial configuration of the IED. There are many reasons why such a scenario could arise. In many cases, the errors are simply due to erroneous engineering. There are also cases where the compatibility or interoperability between these tools needs to be addressed in future requirements from the standard.

An example where the standard and vendors could ensure better interoperability is definition of enumerators (enums) and namespaces that get adopted from the SCT itself. The vendor ICTs need to be flexible to accept these parameters as per the requirements of the standards rather than individual definitions. Similarly, handling of private fields should not be a requirement on the SCT rather the ICT should ensure all private fields required by the finally configured IED are restored or updated before generating the IID file and uploading it to the individual IEDs. These challenges are not uniform across the ICTs. Utilities and system integrators often have to figure out the requirements as they configure individual IEDs.

The size of the substation designed using top-down engineering process can also pose challenges during the configuration phase. As the standard does not regulate the size of the ICDs. The actual size of the ICD file can vary in range of few kBs to few MBs. This poses a real challenge to the hardware and software memory requirements and processing power requirements for the computer used for the purpose of engineering. Interoperability can also be enhanced through limitation of information in the ICD files to that requested by the utility. It then allows the utility to procure IEDs, computer platforms and SCTs that can cope with the design memory and processing requirements. This is important, as reliability and usability of the top-down engineering process is essential to successful design of digital substations.

10.7.2 GOOSE Engineering

GOOSE engineering especially in a top-down engineering process should be straightforward as to linking a published GOOSE to an internal address or node of the recipient device. There are many challenges with this process that poses some of the key interoperability challenges between devices.

Vendor IEDs deploy GOOSE engineering in many different ways since the vendor itself mostly uses its own ICT to configure the IED. The ICT itself ensures all necessary assignments and bindings are completed to ensure GOOSE messages will be published or received as intended. There is limited experience of trial of independent SCTs to configure multi-vendor IEDs on a large scale among vendors and utilities alike.

There are some examples of how a certain vendor IED expects a received GOOSE to be configured. Many vendors expect the GOOSE to be mapped to the system logical node LLN0, and the actual handling of the GOOSE is done within the logic of the device. Some vendors expect the use of later binding and ExtRef fields to be filled by the SCT to assign the GOOSE to an internal address. However, not all vendors provide a list of internal addresses within the ICD file itself.

The vendors in some cases also provide a list of internal address to which the GOOSE can be mapped on to which allows the user to create the final logic of communication between functional elements of the multi-vendor IEDs at the SCD level itself. This is a recommended method for GOOSE engineering however not a common place among the commercially available multi-vendor IEDs.

10.7.3 Report Engineering

Report engineering between multi-vendor IEDs and SAS is fairly interoperable. There are various challenges encountered during engineering of reports over MMS. The client/server communication over TCP/IP is a widely tested service which is easily engineered in configured.

The limitation in terms of multi-vendor interoperability arises in cases where the server IED has some of its clients reserved for its own preparatory SAS. In such cases, the system integrator needs to be aware of the challenge of configuring MMS to dedicated clients for the vendor SAS which can result in failure in the server–client communication to be successfully established.

The number of clients configurable for each server IED can also pose challenges during engineering, testing and actual operation of the final design. There needs to be provision for additional clients to be configured to allow test equipment to simulate server/client communication during testing and commissioning phase.

In general, multi-vendor IEDs can be successfully configured using the top-down engineering process.

10.8 Interoperability Requirements for Testing and Commissioning

The interoperability requirements for testing and commissioning are derived from the need of enabling multi-vendor testing devices, tools and procedures to successfully test a fleet of multi-vendor IEDs in a digital substation. The methods of testing a digital substation have similarities with conventional substations, however fundamentally different on the aspect of testing the communication network. Successful testing of communication network in a digital substation largely relies on interoperability of the IEDs with the testing tools which are also designed according to the IEC 61850 standard.

An example to explain the kind of issues utilities will face while ensuring interoperability during testing is use of LGOS node. At the time of writing of this chapter the use of LGOS to monitor GOOSE communication is only available in certain vendor IEDs. A test device from an independent test tool vendor relies on the information derived from the LGOS parameter to inform the test engineer regarding the status of the GOOSE. In this particular case, the functionality provided by the test tool is only of limited use as the IED manufacturer does not yet provide this function. Interoperability issues during testing and commissioning can also be addressed during the system specification phase. This particular example cites the logical nodes dedicated to monitoring the quality of communication in a digital substation the likes of LTRK, LGOS, LSVS are important to be supported by IEDs to ensure interoperability during testing and commissioning phase.

One of the key business benefit case for digital substations is that it enables outage-less maintenance. Introduction of Ed2.0 simulation flag and test mode allows utilities to test and commission IEDs on a live system without the requirement to take an outage on the network. Almost all vendors provide both parameters in their range of digital substation IEDs. This enables test tools to be connected to the LAN within the substation to simulate faults and trips on the system while testing one or a series of IEDs while the power system and primary equipment are still protected by a redundant system. One of the challenges with interoperability with Ed2.0 simulation flag and test mode is that; they are currently implemented in different ways by the multiple vendors.

The standard does not specify the settings structure for the IEDs that enable or disable these parameters within the IED. It also does not specify whether there should be further security around enabling and disabling of these parameters. That implies whether the test engineer can enable and disable these parameters remotely and does the engineer need special permission to do so. The outage-less maintenance features are powerful tools for testing; however, they can also pose challenges if the test engineer does not follow the steps correctly or is not familiar with a particular IED. Harmonisation of implementation of this critical feature

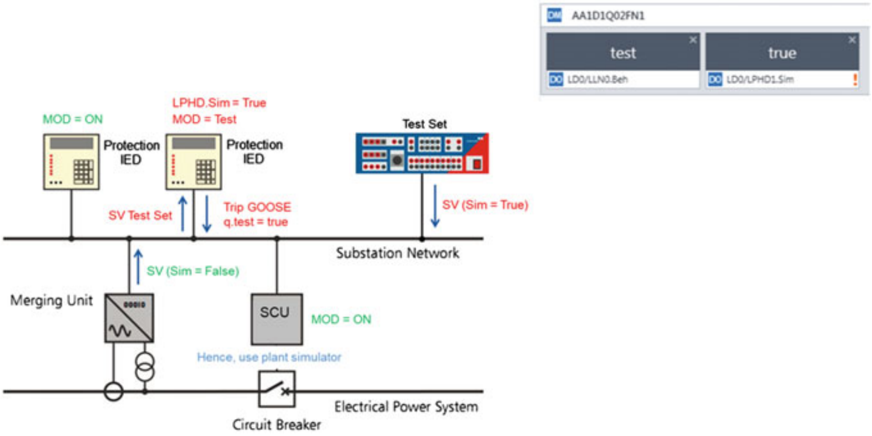


Fig. 10.10 Interoperability in testing using simulation flag and test mode (*source* OMICRON electronics GmbH)

by vendors will allow utilities to develop standard test procedures and allow test engineers to confidently use this feature without disconnecting the IED(s) and/or taking outage on the network. Figure 10.10 illustrates this discussion.

The SCD file is important to successfully test the communication network in a digital substation. The test tools use the SCD file to configure test procedures and simulate test GOOSE, SVs and client/server communication. It is therefore of paramount importance in order to ensure interoperability between the IEDs and test tools that a complete configuration SCD file is available. The SCD file should also be version controlled and there should be methods and tools to check the final configuration against the actual communication on the network. Interoperability is only possible when all IEDs are reliably tested against the final design and a repetition of the test routine without any changes on the system on a later date produces the exact same result. This testing arrangement is illustrated in Fig. 10.11.

Overall comprehensive testing of multi-vendor IEDs using 3rd party tools are critical to ensuring interoperability and reliability of digital substations. Figure 10.12 shows a typical SCL-based testing result view.

10.9 Interoperability Requirements for Operation and Maintenance

Multi-vendor interoperability is an absolute necessity for successful operations and maintenance of digital substations. In general terms, interoperability ensures that all functions designed for the substation perform and communicate between multi-vendor IEDs reliably in real time. It also means that after proper testing and successful commissioning of the substations, the multi-vendor IEDs can protect, monitor and control the network as designed.

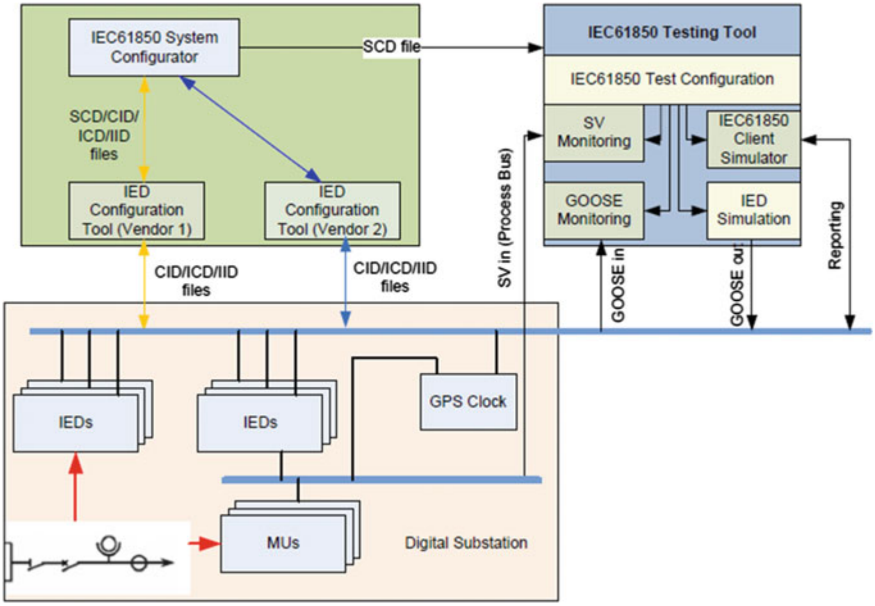
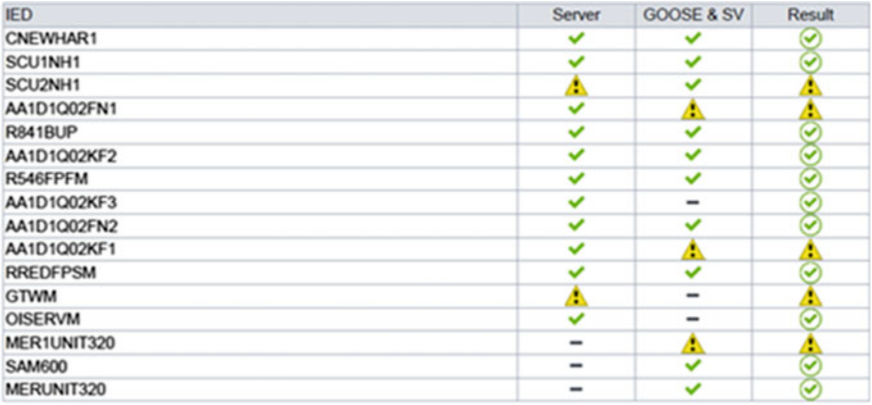


Fig. 10.11 Testing arrangement (*source* [1])

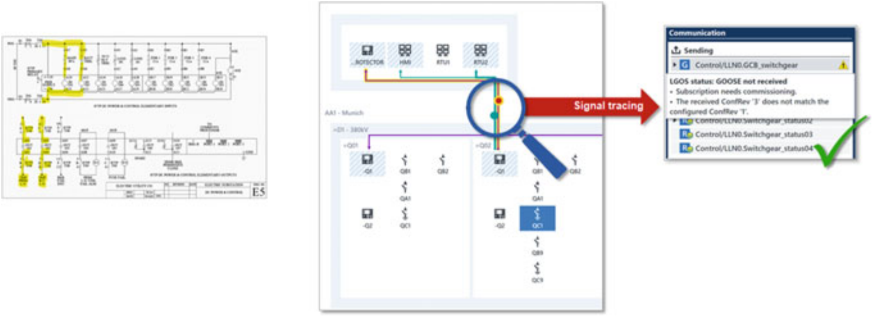


IED	Server	GOOSE & SV	Result
CNEWHAR1	✓	✓	✓
SCU1NH1	✓	✓	✓
SCU2NH1	⚠	✓	⚠
AA1D1Q02FN1	✓	⚠	⚠
R841BUP	✓	✓	✓
AA1D1Q02KF2	✓	✓	✓
R546FPFM	✓	✓	✓
AA1D1Q02KF3	✓	–	✓
AA1D1Q02FN2	✓	✓	✓
AA1D1Q02KF1	✓	⚠	⚠
RREDFPSM	✓	✓	✓
GTWM	⚠	–	⚠
OISERVM	✓	–	✓
MER1UNIT320	–	⚠	⚠
SAM600	–	✓	✓
MERUNIT320	–	✓	✓

Fig. 10.12 SCL-based system testing [1]

10.9.1 Monitoring Requirements

In real-time operations scenario, there will also be failures in IEDs. IEDs can have hardware failures, firmware issues and/or develop error codes and will need troubleshooting, repair and in extreme case replacement. In conventional substations as faults develop on IEDs the operational engineers would perform a series of



Control/LLN0.GCB_switchgear

LGOS status: GOOSE not received
- Subscription needs commissioning.
- The received ConfRev '3' does not match the configured ConfRev '1'.

Control/LLN0.Switchgear_status02
Control/LLN0.Switchgear_status03
Control/LLN0.Switchgear_status04

Fig. 10.13 Use of LGOS logical node for functional monitoring (*source* OMICRON electronics GmbH)

tests including wiring tests, troubleshooting events and logs and system integrity tests. In a digital substation scenario, the same approach applies, however since the communication is over the substation LAN there is no possibility to perform wiring tests. There are needs for functions enabling port supervision such as IEC 61850 objects LCCP or supervision over SNMP to ensure that all physical communication channels are healthy. The next requirement will then be monitoring information regarding individual messages and signals over LTRK, LSVS and LGOS logical nodes as described in the section above. If multi-vendor IEDs do not provide these standard features, then troubleshooting a digital substation during a communication failure will be a real challenge for utilities. Figure 10.13 illustrates this functional monitoring arrangement.

Independent vendor test tools and devices can only provide useful information to the maintenance engineer if the monitoring functional elements (logical nodes) are standardised and interoperable among multi-vendor IEDs.

10.10 Backward Compatibility

One aspect of ensuring interoperability in future is to account for backward compatibility which allows for interoperability with an older legacy system. The same is true for future extensions. Ideally a substation specification should not only be backward compatible but also allow for expansion of the substation in future. A well-perceived specification ensures that vendors align their current and future firmware versions to be backward compatible with older products. This requirement can also be built in the tendering phase to ensure utilities do not have to change the whole substation design during operation and maintenance phase.

One of the major expectations of the users regarding IEC 61850 is that the digital substation products would be easily implemented and interoperable indifferent of their time of installation. This means that any substation extension or modification to an existing substation should be possible to implement with new IEDs that can operate together with the existing IEDs without any compatibility problems arising. Especially if a period of time from original commissioning date has elapsed, the new IEDs will most probably be of a new version (new firmware, maybe even fully new IED model) and require use of new versions of the tools. The expectation on new IEDs added to the system is that they should support the use of both the current edition of the standard but also older editions. The minimum expectation is that it should be possible in the IED configuration tool to select which edition of IEC 61850 to use in the specific case. But the most desirable solution is that the IEDs and their configuration tools should support several versions simultaneously at least starting from Ed2.0 of the standard.

The new IEDs to be added to an existing system usually require new versions of the system integration tools and, most likely, also new versions of device configuration tools. Any modification of the Substation Automation System (SAS) will much probably lead to some configuration changes in the existing IEDs. It is strongly recommended that these changes can be made with the same set of system integration and configuration tools as the new IEDs are handled with. This means that the tools should be capable of configuring both new versions and old versions of the IEDs. This applies also for the case, where the existing IEDs are compliant with older editions of IEC 61850 and the new ones are compliant with later editions. End-user expectation is that there are no compatibility issues due to such version differences or incompatibilities in the IEDs, independent of the vendor of these IEDs.

Also, the configuration tool is expected to give clear visibility on the versioning of the different firmware and the standard version applied in each IED. This is an important piece of information to the system integrator and system designer. Also, the tool itself should be backwards compatible to configure earlier versions of IEDs.

10.10.1 Upgrading of System Software

Over the lifetime of the digital substation it may happen that errors are found in the software used to run the digital substation. This software (SW) is known as the "*system software*", which is here understood as the software platform including operating system and main Protection and Control application software. Similarly, the SW platform of IEDs are called "*firmware*". Due to some errors it may be necessary to upgrade the system software with a newer version. As a result of hardware replacement the new hardware may no longer be compatible with the system, resulting in a newer drivers or operating system having to be installed. Generally, the upgrading of the system can be completed in two ways:

1. Installation of software patches on the existing
2. Complete re-installation of newer

It needs to be noted that system SW problems and their upgrade needs are not strictly related to the IEC 61850 standard solutions. They are independent of general issues common to any DSAS solutions. However, they are still challenging for the end-users and therefore worth mentioning also in this Technical Brochure.

Generally, utilities are cautious about installing new software or patches on systems or IEDs that have been installed, commissioned and in-service. Therefore, vendors should ensure that the following are adhered to:

- The new software is compatible with all other SAS software and data;
- A backup process and installation procedure allow for the re-installation of previously deployed system software and configuration data;
- Complete installation instructions are provided;
- Details of the errors in the previous version and how these issues were resolved;
- Implications of installing the software; and
- Define all testing to be completed so as to ensure that the system is fully functional and ensuring no new problems were introduced as a result of the installation.

10.10.2 Communication Network Interoperability

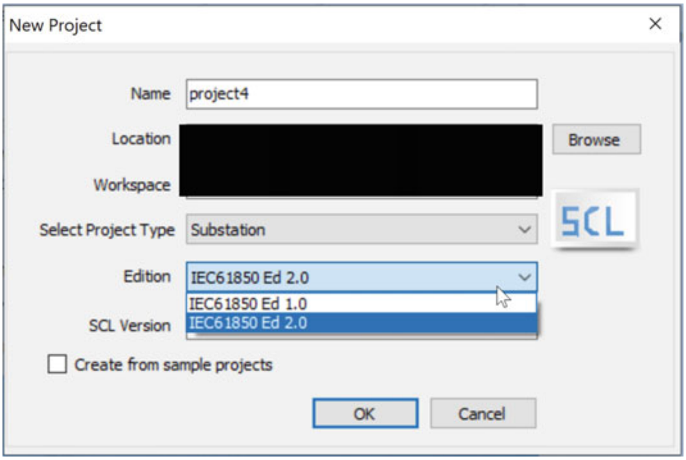
In general, all requirements above are also valid for the communication bus equipment used in the substation such as the switches and the routers. Specifically, the LAN topology of the substation should accommodate for all SAS configuration changes. Communication protocols like PRP or HSR should continue to work when any new devices are added to the network during the whole lifecycle of the substations, independent of the employed version of the communication protocol.

In the same manner, the DSAS should support also IP version evolution (e.g. IP v6).

10.10.3 Replacement of IEDs

Replacement of IEDs has posed serious challenges especially in a substation with a mixture of Ed1.0 and Ed2.0 IEDs. The interoperability and backward compatibility between same vendor IEDs across the editions especially in aspects engineering design and testing remains a challenge and requires special handling. For example, 3rd party design tools and ICTs need to support both editions and be able to create SCDs in all editions of the standard to be compatible with the IED. For example, the introduction of release parameter in IEC61850 namespace Ed2.1 requires SCTs to be able to handle this parameter to be able to parse files.

In the current range of available products some IEDs to provide this parameter in Ed2.1 ICD files whereas in the same substation other Ed2.0 IEDs do not provide this parameter. Although, the changes between editions can be minor however the pace at which multi-vendor IEDs and vendor independent design and



New Project

Name: project4

Location: [redacted]

Workspace:

Select Project Type: Substation

Edition: IEC61850 Ed 2.0

SCL Version

□ Create from sample projects

Fig. 10.14 SCT compatible with different editions and versions (*source* SCL Manager, ASE Systems)

test tools adapt the standard can vary from months to years. This poses a challenge for utilities delivering, operating and maintaining project with multi-vendor IEDs. Backward compatibility remains a challenge in ensuring full-interoperability in digital substations. Figure 10.14 shows interface view of managing different edition and version following replacement cycles of IEDs.

10.11 Review of Miscellaneous Aspects of Multi-Vendor Installations

10.11.1 Architecture: HSR and PRP

Network redundancy, from an operational, maintenance and testing perspective, while using multi-vendor IEDs requires special considerations. It is important that IEDs support the chosen protocol PRP or HSR or both, for the final system architecture.

As a next step, the network bandwidth and port speed requirements should be accounted for to ensure multi-vendor interoperability. The HSR redundancy protocol seems to align itself better to the concept of sharing data in a unified format, i.e. GOOSE, MMS and SV on the same network with 1 GBPS network bandwidth used to cater for the network load, the PRP type of network on the station/bay level and completely segregated process buses on the process level offers a clear demarcation between station data and critical process data—more in line with the concept of segregation of station functions from the critical process related data, as in any conventional systems. In the current market as there are limited IEDs than can be a part of 1GBPS HSR network without requiring an additional PRP/HSR interface device. Selecting multi-vendor IEDs in a HSR architecture with sampled values requiring a larger bandwidth is challenging in terms of ensuring multi-vendor interoperability in system architecture.

10.11.2 Data Streams and Functional Interoperability

In general, there is no known issues between correctly configured IEDs during real-time operation, as far as unencrypted GOOSE, client/server and SV communication is concerned. Interoperability does not cater for accuracy and quality of the data streams. The general experience is once multi-vendor IEDs are correctly configured, they reliably communicate over GOOSE, client/server and SVs. In order to improve monitoring and checking of the data received by the IEDs, logical nodes such as LTRK, LSVS and LGOS should be deployed, as discussed earlier in this chapter.

There is very little experience with encrypted data streams within a digital substations, at the time of writing this book. The interoperability of encrypted data streams needs to be proven through application and testing.

10.11.3 LPITs, Merging Units and IEDs

10.11.3.1 Merging Unit Switchover

Implementation of multi-vendor systems especially in the cases redundancy of critical protection and control functions is usually achieved through use of system A and system B from two different vendors. In some utility application, there might be a requirement for an additional back up and/or hot-standby system. Interoperability of the redundant systems with multi-vendor merging units, switching control units and SAS allows for real-time switchover of devices in case of failure a single device in the function chain. For example, say Vendor Main System A is subscribing to SV stream from MU1 and interacting with the plant for positions, control and trip over SCU1 as shown in Fig. 10.15. In this scenario MU1 and SCU1 could be from the same vendor as the Main System A or from a different vendor. Now supposedly MU1 has a failure and cannot provide a good quality SV stream, ability of Main System A to subscribe to SV stream from MU2 from a different or same vendor either through change of configuration or in real-time allows for continued operation enabled through multi-vendor interoperability. This is a useful feature as it allows for additional level of redundancy, for critical protection functions.

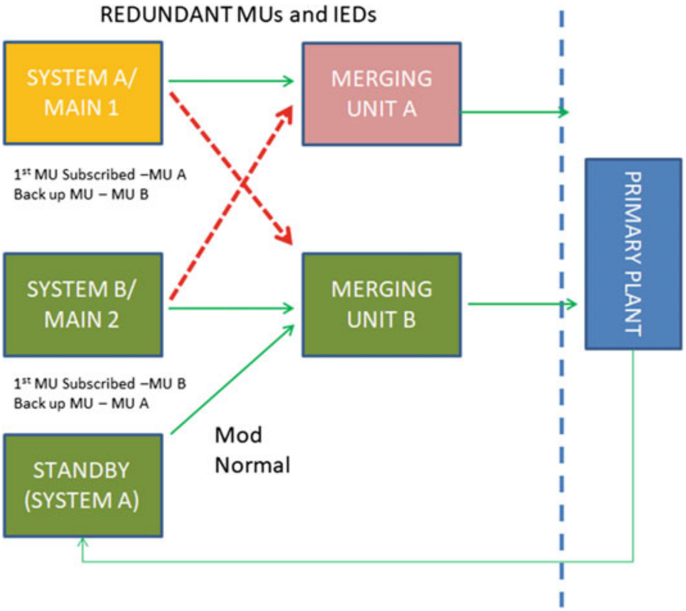


Fig. 10.15 Redundant merging units switchover in real time

10.11.4 Time Synchronisation

Time synchronisation is of paramount importance for maintaining reliability and availability of the process bus and sampled values, and consequently, the availability of critical protection and control functions in a digital substation. Depending on the regulations, utilities may not accept loss of protection functionalities for more than 1–3 secs, and such loss cannot be a frequent occurrence. In digital substations applications time synchronisation is achieved predominantly by application of the IEC 61850-9-3 standard. IEC 61850-9-3 (2016) part of IEC 61850 standard specifies a precision time protocol (PTP) power utility profile which allows compliance with the highest synchronisation classes of IEC 61850-5 and IEC 61869-9.

10.11.4.1 Holdover Times

It should be noted that—as in any protection related matters—it's quite difficult to get the right balance between scheme security and availability under various Sample Value synchronisation conditions. The definition in IEC61850-9-3 for steady state as 30 s after a single master starts to send synchronisation messages and 16 s after a change of master, with no change to the environment temperature, indirectly implies that MUs may not be in a steady state for 16 s during a changeover. This may not be acceptable to utilities for system critical functions. A potential solution could be to increase availability of MUs, for example, vendors could allow MUs to holdover for 30 s for protection applications instead of 10 s as required for

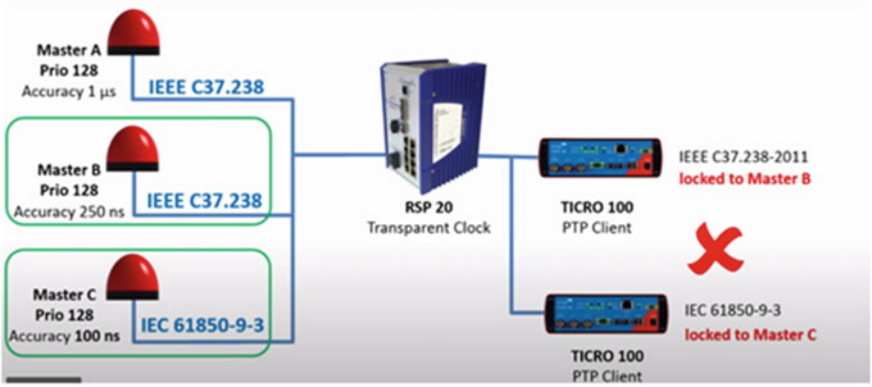


Fig. 10.16 PTP mixing of profiles (*source* OMICRON electronics GmbH)

metering applications. Vendors currently tend to put a strong emphasis on scheme security—although robust enough, under certain re-synchronisation conditions, the MU is blocked, and thus unable to provide Sample Values to the protection and control IEDs. However at the same time, utilities put more emphasis on scheme availability, while expecting to maintain security at an acceptable level.

10.11.4.2 Interoperability of Different PTP Profiles

The use of multi-vendor grand master clocks (GMCs) for time synchronisation should be carefully matched in terms profiles used for PTP as shown in Fig. 10.16. It has been noted in practice that even a slight mismatch in power profiles and configurations in both GMCs increased the negotiation time in the best master clock algorithm. In order to avoid this, both GMCs are best set to power utility profile and associated configurations are exactly matched to significantly performance of the best master clock algorithm. The recommendation is to clearly specify the requirement to match the profiles in the standard.

10.11.4.3 PTP and Redundancy

In general, For PTP messages, the general PRP operation does not apply. IEEE 1588 doesn't specifically mention PRP, but gives some general hints on redundancy. **Annex R—Example inter-domain interactions** shows how a device can receive the time from multiple devices or over multiple paths. Also **Annex S—Security** deals with redundancy as a security measure. Generally the suggestion is using at least three independent paths, this allows for voting algorithms to identify the "wrong" or "bad" time.

With IEC 61850-9-2 ED2.1, the optional field "SyncSrcID" was introduced. It shall carry the GM Clock ID of the master clock the MU is synchronised to.

With this information, a relay can decide if it is itself synchronised to the same clock as the MU or if all MUs from which a relay subscribes SVs are synchronised to the same clock.

But depending on the chosen network/time distribution architecture, there are configurations imaginable (when the redundancy mechanism kicks in) where parts of the devices are synchronised to different clocks. The GM identity (GM clock ID) is only of interest when the sync mode falls back to “locally synchronised”. This information is also carried with the SV stream in the SmpSynch field.

As long as all components in the system are synchronised to a master clock that can claim to be globally synchronised (“traceable” in PTP terms), it does not matter to which clock the devices are synchronised to, the GM identity is irrelevant, with exception of applications of IEC 61850-6-9 standard where this can be enforced.

Only when global synchronisation is lost, then it must be assured that all devices sync to the same master clock. Then the GM identity must match. This feature needs to be independently tested for different IEDs, to ensure interoperability during operation.

10.12 Tools

The requirement for multi-vendor operability of engineering design, testing and commissioning tools is pivotal to successful delivery and maintenance of digital substations. Tools play an important role in transition from conventional to digital substations. The tools required for digital substations are considerably different that for conventional substations based on hardwired designs. The physical parameters of conventional substations are replaced with data in digital substations. The data and information present in digital substations, need to be configured, visualised, tested and monitored using tools that can accurately and reliably interpret the data and create meaningful information for the user. Therein, lies the biggest requirement for digital substation tools to be interoperable with all the vendors and the vendors to provide interfaces and communicate adhering to the standard. Any proprietary communication and data, use of private fields not required by the standard, will result in exclusion, incorrect interpretation and incorrect configuration by the tools. This has been to date one of the most prominent challenges to multi-vendor interoperability in digital substations.

10.12.1 Engineering Design and Configuration Tools

Engineering design is the most crucial part of digital substations project delivery requirements. The challenges described in Sect. 10.4 all apply to engineering design tools as well. The biggest challenge being engineering a multi-vendor substation with one system configuration tool (SCT). The SCT whether from a 3rd party or an IED vendor needs to be able to work efficiently and without ambiguity with other IED data models and configuration files. Currently, there is no clear guideline within the standard regarding the configuration tools. Vendors interpret the standard often differently regarding which parameters are required for configuration as described in detail in Sect. 10.4.

There is currently no SCT on the market that can directly configure a 3rd party IED. All SCTs create a SCD file which is then imported using the IED Configuration Tool (ICT) into the IED. The SCTs and ICTs should be interoperable. A SCD file produced by a SCT tools containing IED configuration, should be imported with the corresponding 3rd party ICT without any interoperability issues. Similarly, a SCD created by SCTs should be correctly read by 3rd party testing and commissioning tools.

In practice, there is still a certain degree of incompatibility between SCTs, ICTs, testing and commissioning tools. Following points highlight some of the main interoperability challenges between the tools:

1. Interpretation of Single Line Diagrams (SLDs): In general SLDs created by one SCT are not accurately imported by other SCTs. In current tools, the X–Y coordinates are not correctly interpreted by 3rd party tools. The SCT will show all substation elements, however the placement of the network elements may be distorted and may need rearrangement to represent the substation SLD.
2. Creation of Virtual IEDs or IED specification definition (ISDs): Virtual IED definitions are only possible in SCDs at the moment, as the standard introduces the concept of ISDs, it will be critical for vendor ICTs to correctly interpret the ISDs and provide ICDs matching the ISD specifications. Currently, with virtual IED definitions the vendors can create custom ICDs based on user specifications (as described earlier in this chapter).
3. Communication Network Specifications: IED port assignments do present some interoperability issues between SCTs and ICTs. The IED port assignments are done in a generic manner for all IEDs in SCTs based on a redundancy protocol which is selectable. If the IEDs have special port naming conventions and/or do not comply by redundancy requirements these configurations pose a challenge during import with the ICTs. Ethernet switch configurations are rarely done using SCTs even though switch ICDs are available from certain manufacturers, at the time this chapter is being written. This remains as a interoperability gap in SCTs and switch configuration tools.
4. System communication engineering: GOOSE, report and SV engineering challenges have been described in detail earlier in this chapter.
5. Flexible naming: Interoperability challenges with flexible naming will be solved when all vendors support flexible naming.
6. Schemas: The compatibility issues between different IEC 61850 schemas have been covered in the backward compatibility section of the chapter.
7. Vendor-specific handling: SCTs currently perform vendor-specific handling to overcome any interoperability challenges specific to vendor ICTs. Vendor-specific handling should not be required in a truly interoperable implementation of digital substations.

The aforementioned issues vary between tools and vendors and are constantly evolving to ensure more interoperability. Wide scale roll-out of digital substations and adoption of top-down engineering approach will help tool developers identify more of these issues and improve interoperability. There is a requirement for guidelines regarding tool interoperability in the IEC 61850 standard. In the meantime, utilities and vendors can participate in IOP process and testing workshops and learn through large scale implementations by utilities.

Vendors could contribute by enhancing their ICT development process, by processing and thoroughly testing interpretation of SCDs created by 3rd party SCTs. In conclusion, adaptation of SCD files with XML editors or workarounds to successfully import a SCD generated with a 3rd party SCT, cannot be acceptable as interoperable and this remains largely a open point in IEC 61850 engineering process.

10.12.2 Testing and Commissioning Tools

Digital substations require novel testing and commissioning tools. As discussed previously in this chapter, these tools need to interoperable with 3rd party IEDs and testing tools.

1. The amount of experience in full-scale digital substations testing is limited at the time this book is written. The testing tools are generally interoperable with all vendor IEDs. Testing tool manufacturers should also participate in IOP testing and workshops, to ensure they can effectively test all manufacturer IEDs.
2. Testing tools based on SCL file for configuration, are similar to 3rd party SCTs. As long as, the SCL is created in line with the standard, this should be interpreted by the testing tools accurately.
3. Testing tools need to keep up to date with new developments in the standards and use logical nodes defined especially for testing and monitoring to provide enhanced visualisation to end-users regarding quality and accuracy of the network.
4. Test tools with Sampled Values (SV) publishing capabilities should be accurately hardware timestamped and should allow user to accurately visualise data on the network.
5. Test tools should also comply to Cyber-security requirements (more in Chap. 6).
6. Test tools should be able to export files in PCAP, comtrade and other cross-platform formats for detailed analysis and/or visualisation with 3rd party software.

10.13 User Case Studies

10.13.1 SP Energy Networks Project FITNESS

The FITNESS (Future Intelligent Transmission Network Substation) project is the first multi-vendor digital substation and automation system in the UK. This venture was funded as part of Britain's electricity regulator, OFGEM (Office for Gas & Electricity Markets), RIIO NIC (Network Innovation Competition) and will be deployed at the Wishaw 275 kV substation in Scotland. The project is an IEC61850-based multi-vendor solution.

In the FITNESS project, the innovation is to be found in the way the overall system was designed in order to prove interoperability with protection and control equipment procured from various Suppliers at; process bus, station bus and SAS. The project proved IEC 61850 multi-vendor interoperability at various system levels. To achieve this, SP Energy Networks (SPEN) worked with two main vendors and also with equipment manufactured by a third vendor. The various levels of interoperability the project aims to prove are:

- Between Vendor A IEDs and Vendor B merging units;
- Between Vendor B and Vendor A merging units;
- Between Vendor A and B PMUs and Vendor C Interrogator;
- Between Vendor A IEDs and Vendor B SAS and vice versa;
- Between Vendor B IEDs and Vendor A SCUs and vice versa;

FITNESS has enabled SP Energy Networks, not only to prove interoperability at multiple levels, but also within a mixture of old and new technologies. In particular, the interoperability of Stand-Alone Merging Units and protection IEDs, IEC61850 and IEC61850-9-2LE was given priority, since aspects such as transient response, accuracy and dynamic behaviour that will come into play and influence the performance of the overall FITNESS scheme, are dependent on multi-vendor IEDs communicating and operating in an interoperable manner.

The FITNESS architecture, as shown in Fig. 10.17, is a single combined architecture based on the proposals of both vendors demonstrating interoperability among multi-vendor Intelligent Electronic Devices (IEDs) and between conventional and digital substation design. The station level architecture is a common architecture agreed by the FITNESS project team, however, each vendor has assumed responsibility for their designated process level architecture with vendor 1 applying HSR network and vendor 2 applying a PRP network. In the FITNESS architecture at station bus level, client/server and GOOSE services are utilised whereas, at process bus level, SV and GOOSE services are utilised. FITNESS proved multi-vendor interoperability of client/server, GOOSE and SV communication.

The key interoperability issues identified in FITNESS have been described in detailed in the sections above in this chapter. FITNESS is a good example, that despite the current interoperability issues successful engineering, configuration,

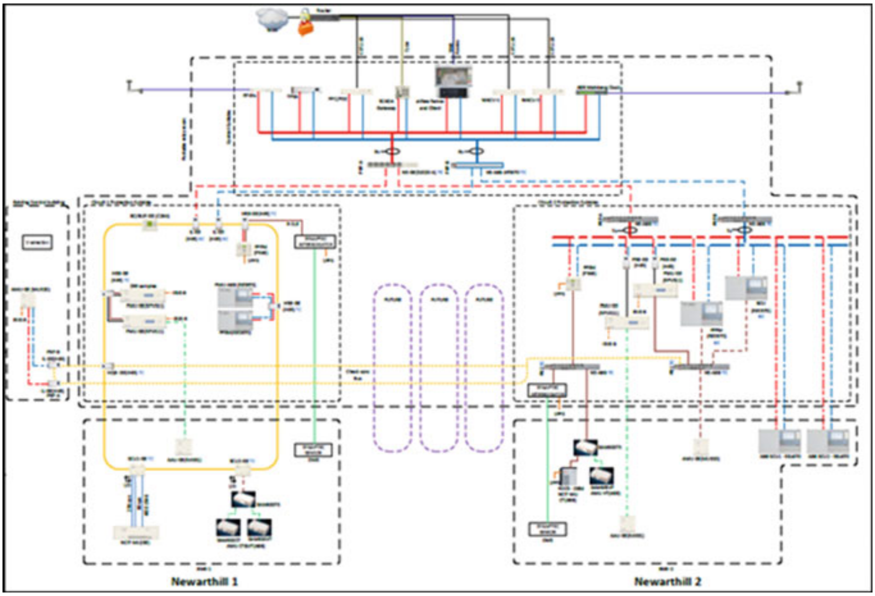


Fig. 10.17 FITNESS architecture (*source* SP Energy Networks)

testing and commissioning of multi-vendor digital substations can be successfully achieved with the devices currently available in the market.

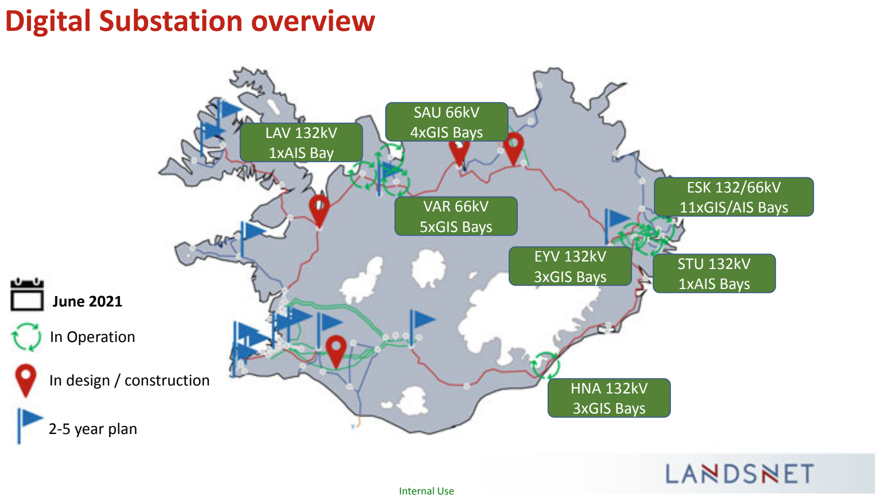
10.13.2 LANDSNET Iceland, Digital Substations

LANDSNET Iceland is currently reinforcing their critical transmission network infrastructure to create extra capacity and allow for better generation and demand management across the country. Digital substations, as shown in Fig. 10.18, are enabling them to build new substations at a faster rate, through efficient offsite testing and less commissioning time on site.

LANDSNET is also deploying multi-vendor digital substations. They have made an additional experience with metering applications, which proves that metering can also be successfully deployed with 3rd party Merging Units and Metering devices. This is shown in Fig. 10.19.

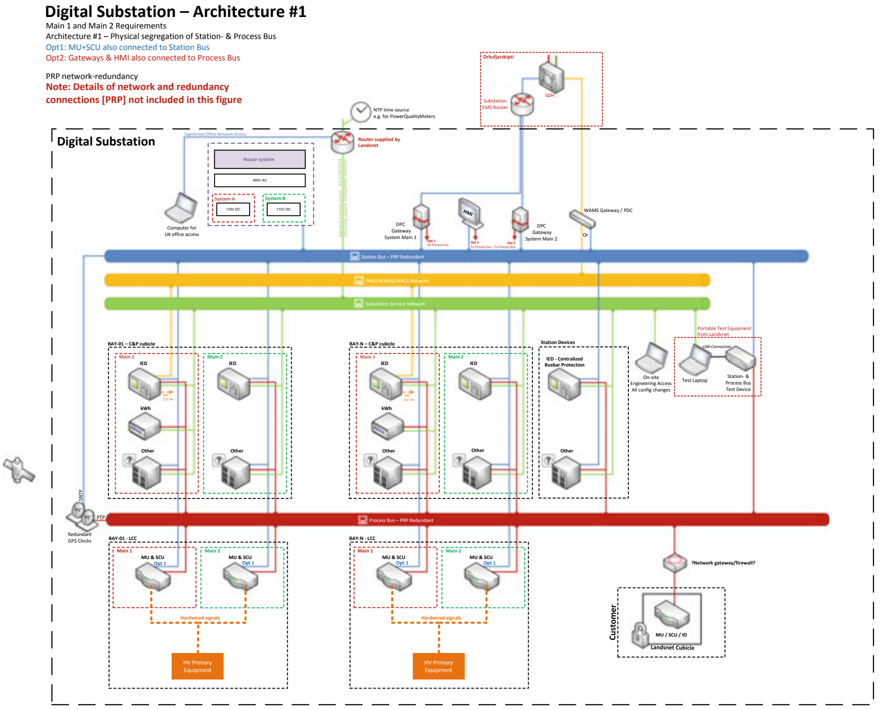
LANDSNET also deployed Sampled Values using IEC 61869-9 flexible datasets and proved multi-vendor interoperability with flexible SVs between multi-vendor IEDs.

The interoperability issues encountered by LANDSNET are mostly with SCTs and ICTs, as described in the chapter. Most challenges were resolved with vendor updates of engineering tools. Remaining interoperability issues are related to schemas, naming conventions and in one case interpretation of local-remote operation by a particular vendor.



Digital Substation overview

Fig. 10.18 LANDSNET digital substations roll-out plan (*source* LANDSNET)



Digital Substation – Architecture #1

Main 1 and Main 2 Requirements

Architecture #1 – Physical segregation of Station- & Process Bus

Opt1: MU+SCU also connected to Station Bus

Opt2: Gateways & HMI also connected to Process Bus

PRP network-redundancy

Note: Details of network and redundancy connections [PRP] not included in this figure

Fig. 10.19 LANDSNET multi-vendor system architecture (*source* LANDSNET)

The PTP-PRP issue described in this chapter was experienced both in FITNESS and LANDSNET projects successfully.

In conclusion, given all the challenges described in this chapter and improvements to be made in the standard, in IEDs and in utility process; multi-vendor interoperability using IEC 61850 standard is possible and examples of successful application exist across the globe.

References

1. CIGRE Brochure "TB 819—IEC 61850 based substation automation systems – Users expectations and stakeholders interactions"
2. ENSTO-E Statement on IEC 61850 2012-04-13. https://www.entsoe.eu/2012/04/13/entso-e-statement-on-the-iec61850-standard/

CT/VT Sampled Value Acquisition Applied to IEC 61850

11

Janez Zakonjšek

Abstract

Reliable and accurate operation of complete digital acquisition chain is very important for performance of PAC devices within modern power systems. Even a perfect algorithm can operate unreliably if quality of Sampled Values (SV) does not secure correct information about measured primary currents and voltages. History of SV development from the beginning of IEC 61850 standard is described within this chapter as well as latest requirements as provided in IEC 61869-9 standard. Different peculiarities of current and voltage instrument transformers (conventional as well as LPITs) are presented as well as some specific needs of different PAC functions for current and future power systems, also considering their decreasing inertia. Some challenges for future development of digital acquisition chain are presented at the end of chapter.

Keywords

Sampled Values • Digital acquisition chain • Transient currents and voltages

11.1 Evolution of Sampled Value CT/VT Definitions and Configurations

Sampled Value is a generic term that applies to a number of different sensors which can be installed for different purposes in electric power installations. In Edition 1 of IEC 61850 Part 7-4 [1], the only two sensors were TCTR for AC current measurements and TVTR for AC voltage measurements.

J. Zakonjšek (✉)
Relarte Ltd., Bohinjska Bistrica, Slovenia
e-mail: janez.zakonjsek@relarte.com

P. Bishop and N.-K. C. Nair (eds.), *IEC 61850 Principles and Applications to Electric Power Systems*, CIGRE Green Books, https://doi.org/10.1007/978-3-031-24567-1_11

Table 11.1 TCTR/TVTR data objects

Data object TCTR/TVTR	Description
Artg/Vrtg	Rated current/rated voltage
HzRtg	Rated frequency
Rat	Winding ratio of an external current/voltage transformer (transducer) if applicable

The TCTR and TVTR Logical Node data model as per IEC 61850-7-4 Edition 2 provides setting parameters as shown in Table 11.1.

According to IEC 61850 TISSUE 1176 [2], this data model will have additional Data Object<<.SmpRte>>without an “a” to be consistent with the other T group LNs of IEC 61850 Part 7-4 edition 2. However, IEC 61869-9 [3] defines a different attribute name for the sampling value used in the SV stream control block as<<.SmpRate>>with an “a”. Hence, the LN may specify a base sampling rate of 14,400 samples/second, but the control block is publishing at 4400 samples/second.

It is to note that TCTR and TVTR are single-phase sensor data models. For three-phase system, it is therefore necessary to provide three instances of each for the individual phase values and a fourth for a neutral sensor where relevant.

The type of physical sensor can be conventional induction (magnetic) current transformers and induction or capacitive voltage transformers. They can also be the increasingly accepted so-called “non-conventional instrument transformers” or “Low-Power Instrument Transformers (NCIT/LPIT) based on optical measurements or Rogowski coils, which are being increasingly used by different vendors.

As the TCTR/TVTR LNs are single-phase instances, it is convenient from a device perspective to have a merging unit (MU) with multiple-phase inputs from the primary sensors and which provides a combined SV stream with the values of multiple phases in one single message.

11.1.1 Interim Guideline IEC 61850-9-2LE

As can be seen in the IEC 61850-7-4 [1] data model, there is no specification of the sampling rate of the sensor, and hence, different applications (e.g. protection at 80 samples/cycle versus power quality 256 samples/cycle) could have different sampling rates and indeed different vendor products could have different sampling rates, noting that the overall sampling frequency of samples/second varies according to the system frequency 16.7, 50 or 60 Hz. Such variety of sampling is not conducive to interoperability where the subscribing IEDs can “know” the meaning of the sample streams they receive. In order to aid in take-up of SV by utilities needing vendor interoperability of the sensors to the protection IEDs, the UCA International Users Group (UCAiug) published a guideline document for the industry with recommended parameters for configuring the merging units. The UCAiug document is known as “IEC 61850-9-2LE_R2-1” [4]; however, it is to note that it is not an official standard, and as such, compliance is outside of IEC 61850-10 requirements and of course is both optional and subjective to what is implemented by the vendor.

The key definitions of the MU under IEC 61850-9-2LE [4] are as follows:

1. Sampling Rate: 80 or 256 samples per nominal cycle
2. MU SV message dataset contents either:
   a. 1 set of samples of 4 × current and 4 × voltage
   b. 2 sets of samples 4 × current and 4 × voltage
3. Time synchronisation as 1 Pulse Per Second via fibre connector

Most vendors have accepted the first two elements but have just used the more common co-axial cable for the 1 Pulse Per Second time synchronisation. At that time of release of the standard in 2002–2004 and “LE”, IEEE 1588 PTP V2 [5] was not in existence, and hence, 1PPS was about the best that could be achieved.

11.1.2 IEC 61869-9 Standard

The IEC TC 38 recognised that CT and VT SV applications needed a more stringent standard to be followed and also cater for wider applications for different sampling frequencies. This work was associated with the revision of IEC 60044 series, in particular IEC 60044-8 as a bespoke type of SV implementation. This work has been released as IEC 61869 series, including IEC 61869-9 [3] in 2016 for current and voltage measurements “Digital interface for instrument transformers” [3].

A key difference between IEC 61869-9 and IEC 61850-9-2LE is a change from the definition of the sampling rate as “samples per cycle” to a direct “sampling frequency” as samples per second. This eliminates any variance due to the system frequency and indeed due to accuracy/sensitivity/responsiveness of the different MUs in the system.

The number of sampling frequencies has also been expanded to cover a broad range as shown in Table 11.2.

As shown in Table 11.2, the IEC 61869-9 [3] has the same frame rate of 2400 frames/second for the preferred sampling frequencies of 4800 Hz and 14,400 Hz. However, the length of the individual messages is longer than the legacy 4000 and 4800 frames per second due to the increase in the number of ASDU (Application Service Data Unit) in each frame.

It is also to note the somewhat odd use, as far as a standard is concerned, of the word “Preferred” for the sampling frequency. It is therefore critical that procurement specifications must be absolutely clear about what sampling frequency is required to be supported by the merging units and the subscribing IEDs.

Table 11.2 IEC 61869-9 sampling frequencies related to [3] Table 902

Sample frequency Hz (samples/second)	No ASDU	Frames/second	Application
4000	1	4000	Legacy 80 samples/cycle 50 Hz
4800	1	4800	Legacy 80 samples/cycle 60 Hz
4800	2	2400	**Preferred** for protection
5760	1	5760	Legacy 96 samples/cycle 60 Hz
12800	8	1600	Legacy 256 samples/cycle 50 Hz
14400	6	2400	**Preferred** for power quality and metering
15360	8	1920	Legacy 256 samples/cycle 60 Hz

Another key change in IEC 61869-9 is the recommendation for the use of optical fibre LAN connections with duplex LC connectors.

Time synchronisation is also now specified as IEC 61850-9-3 (IEEE 1588 PTP v2 profile).

11.2 Additional Important Facts Related to Sampled Values and IEC 61869-9 Standard

At this point, it should be mentioned that IEC 61869-9 [3] standard belongs to the complete family of IEC 61869-1 “General Requirements for Instrument Transformers” and its subgroup IEC 61869-6 “Additional General Requirements for Low-Power Instrument Transformers”. In this respect, it is necessary, when discussing specifics of 61869-9 standard, to consider also certain specifics of all included standards for instrument transformers. It is also necessary to point out that a special standard part, IEC 61869-13 “stand-alone merging unit”, has been published in February 2021.

On the other hand, it is also necessary to look into the importance of SV for the complete performance of digital protection, automation and control (PAC) functionality within modern power systems. It is a fact that reliable transmission of all types of information is important for their reliable operation, but SV have in this respect additional importance, as they influence the operation of different algorithms within PAC equipment. Even perfect algorithm can operate unreliably if SV quality does not secure correct information about measured currents or voltages. It is of course also possible to expect wrong operation when the algorithm does not consider all specifics of conventional as well as modern instrument transformers and their response on different transients in power systems. All such difficulties have been solved during the development of classical IEDs by a single development team, which was responsible for the reliable operation of one complete unit with integrated hardware and software, which is not a general case today. Some of such important elements are presented in further points within this chapter in order to show the most important needs and steps towards the reliable operation of digital secondary equipment, dependent on high quality of Sampled Values as well as analogue current and voltage signals produced by instrument transformers and input elements of corresponding electronic circuits. In this respect has been established also the IEC TC95 W2 group and missioned to cover digitally interfaced protection functions. The group is preparing a TR based on IEC 61869-9 [3] standard as well as other related documents in the view of determining the relevant requirements for IEC 60255 series.

11.2.1 General on Complete Digital Acquisition Chain

Numerical technology together with excellent communication possibilities is a great step forward in relay protection and substation automation practice. Figure 11.1 presents different possibilities for a complete digital acquisition and execution chain, starting at the top with conventional protection and control IED design and ending with MU performing only adjustment of proprietary digital signals from LPITs to IEC 61869-9 standard. It is also possible that LPITs themselves will provide at their output direct digital signal according to IEC 61869-9. All intermediate stages are possible. Stand-alone merging units (SAMU) will make it possible to connect any of the signals specified on Fig. 11.1 below to their inputs.

The upper part of Fig. 11.1 presents a general design common to practically all modern protection and control IEDs, regardless of their origin. Input currents and voltages from conventional instrument transformers (CITs) are adjusted to electronic measurement and galvanically separated in (generally) conventional current and voltage input transformers. This is then followed by certain amount of analogue filtering (anti-aliasing), AD conversion and signal processing. The later one can be executed in separate digital signal processors or within the main processor, which performs also logical functionality, communication and self-supervision and controls the binary input and output elements.

Implementation of Low-Power Instrument Transformers (LPITs) introduces in this respect new functionality: analogue electronic processing of basic information on measured current or voltage (light beam, for example), which provides internally a low-power current (mA) or voltage (V) signal. These signals can be used directly in specially designed protection and control devices (e.g. when Rogowski coils are used for current measurement) or can be further processed to digital form and sent to corresponding IEDs. Here, again two possibilities exist:

- A proprietary digital communication protocol can be used together with specially designed IEDs (but this option is not preferable in current practice)
- A proprietary digital communication protocol is in merging unit adjusted to IEC 61869-9 protocol and transferred to relay execution part (digital signal processing, logic and communication, etc.)

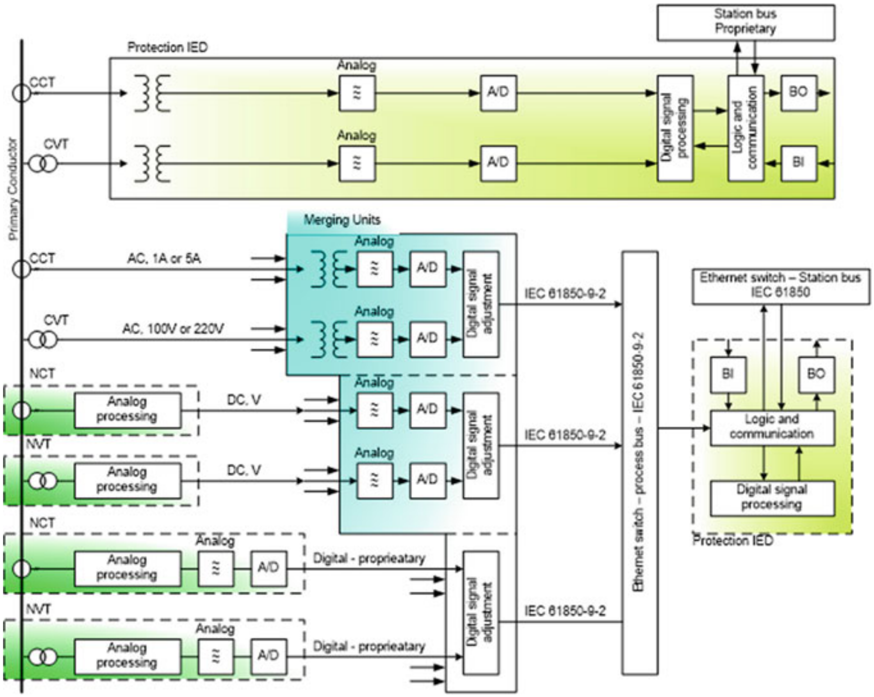


Fig. 11.1 Different possibilities of digital acquisition chain (*Source* [6] Fig. 5.1)

Here, it is possible to observe the main difference in designing protection, control and additional functionality between the conventional one and the modern types. When designing the conventional IED, the developer was responsible for a complete chain, from conventional analogue inputs to complete signal processing, algorithm and logic execution. It was possible to compensate for some deficiencies in one part with special methods introduced in another part. This is even possible with introduction of LPITs and proprietary solutions, but will not be possible with introduction of IEC 61869-9 standard. Here, we have to deal with three completely separated parts: LPIT, MU and Algorithmic Digital Signal Processing within the protection IED. For this reason, it is of outmost importance to provide to the developer of protection, control and other algorithms the reliable information on primary signals as well as on the characteristics of all elements included within the complete chain.

11.2.2 Some Specific Characteristics of Different Instrument Transformers

Each type of current and voltage instrument transformers has its own specifics, which should be considered within the merging units as well as within the PAC algorithms. Many of them are well described in [6]. Here are presented only some characteristics, which are in general not known to greater amount of protection specialists.

11.2.2.1 Saturation of Current Transformers with Very Low Secondary Burden

Figure 11.2 represents a typical example of magnetic (high-remanence type TPX) CT saturation in case when the fault current comprises maximum DC offset in measured primary current. This example is typical for the cases when magnetising impedance is during saturation much smaller than the total resistance of the complete secondary circuit, which is very typical in current practice.

On the other hand, it is possible that the current transformer has extremely low secondary winding and burden resistance and the saturated magnetising impedance will not be able to short circuit completely the secondary circuit. There will be a current distribution between the total secondary resistance and the saturated magnetising impedance. The saturated secondary current can be of considerable magnitude. Input CTs of modern protection IEDs or SAMUs can have extremely low burden and operate in such conditions. Figure 11.3 shows an example of a saturated low remanence CT secondary current in case of an extremely small secondary resistance. The AC component of the fault current is 3 p.u., and the CT saturates after approximately 50 ms.

Secondary current as presented in Fig. 11.3 is in a way very similar to the secondary current of saturated no remanence CT (type TPZ), which has very limited capability to reproduce the DC current component.

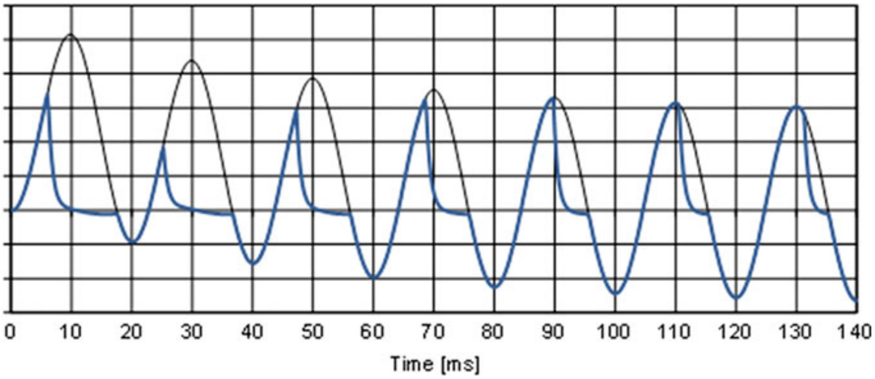


Fig. 11.2 Typical CT saturation with maximum DC offset in measured current (*Source* [6] Fig. 2.7)

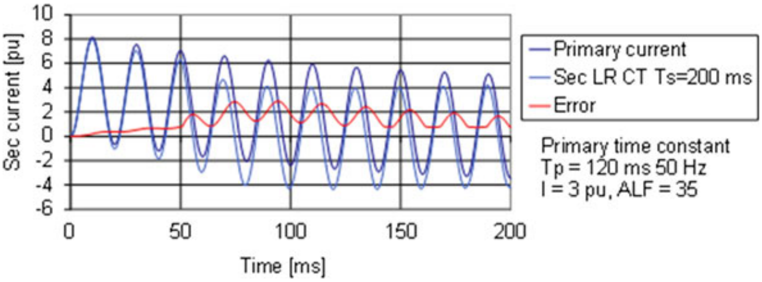


Fig. 11.3 Example of CT saturation in case of an extremely small secondary resistance (*Source* [6] Fig. 2.8)

It is for this reason extremely important that the producers of LPITs as well as SAMUs provide very detailed information about their input current circuits. Here, we consider especially the time constant of secondary circuits and time to saturation.

11.2.2.2 Rogowski Coil Integrated Output Signal

Traditional Rogowski coils consist of a wire wound on a non-magnetic core (relative permeability $\mu_r = 1$) and are quite recognised Low-Power Instrument Transformers (LPIT) for current measurements. They have many advantages compared even to magnetic CTs, which can be also seen in CIGRE Technical Brochure 768 [6]. As the Rogowski coil output signal is a scaled time derivative of the primary current, signal processing is required to extract the power frequency signal for phasor-based protective relays. This may be achieved by integrating the Rogowski coil output signals, or using non-integrated Rogowski coil output signals in other signal processing techniques.

Integration of the signals can be performed in the conventional relay (by analogue circuitry or by digital signal processing techniques) or immediately at the coil, which means also at the corresponding merging units. To use the Rogowski coil non-integrated analogue signal, it is necessary to perform the signal corrections for both the magnitudes and phase angles. For phasor-based protective relaying applications, the Rogowski coil secondary signal must be scaled by magnitude and phase-shifted for each frequency.

One of the Rogowski coil's specifics, which should be considered by algorithm developers, is their response on fault current interruptions, which generally happens in a moment, when the fault current is zero. The derivative signal (di/dt) goes to zero value instantaneously, but this is not a case with integrated signal. Figure 11.4 shows comparison of the fault current recorded by the laboratory current transformer with the Rogowski coil integrated signal. The signal integration was performed off-line using digital signal processing technique. Before the fault current was interrupted, both waveforms (recorded by the laboratory current transformer and with the Rogowski coil) overlap. When the fault current was interrupted at the current zero, the current transformer secondary current was also

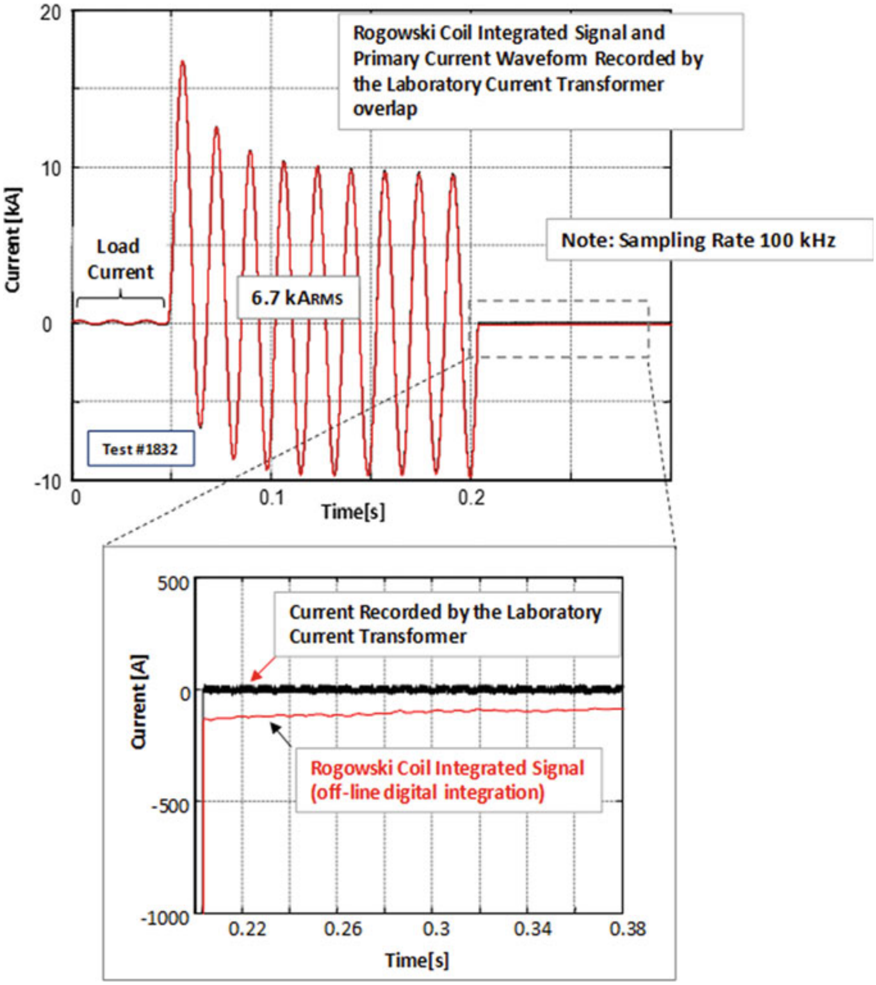


Fig. 11.4 Rogowski coil integrated signal versus traditional current transformer waveform (*Source* [6] Fig. 2.34)

at zero. However, the Rogowski coil secondary signal did not reach zero, but it was approaching zero with a long decaying time constant. Such performance may influence the operation of different protection functions (e.g. breaker failure protection) and should be for this reason considered very seriously by developers of merging units as well as protection algorithms.

11.2.2.3 Capacitive Voltage Transformer (CVT) Transient Response on Close in Faults

CVT-related standard IEC 61869-5 specifies CVT transient response on sudden change in primary voltage as presented in Fig. 11.5 (*source* CIGRE TB 768 [6]).

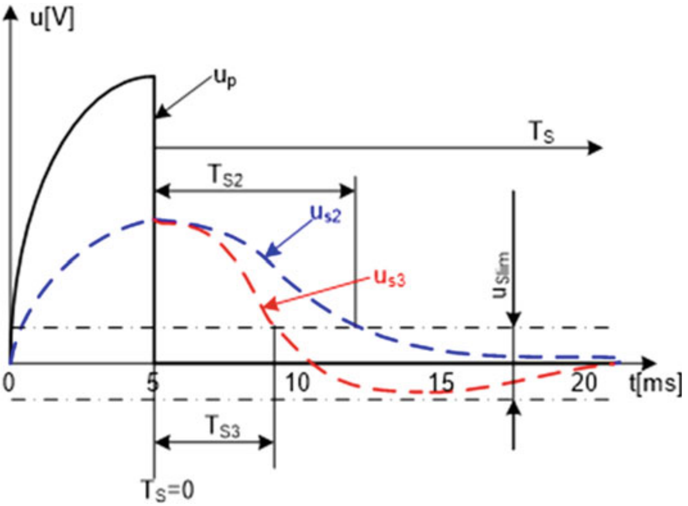


Fig. 11.5 CVT secondary voltages at sudden primary voltage drop to zero according to IEC 61869-5 standard (*Source* [6] Fig. 7 in Chapter 7)

In case that primary voltage u_p drops from its maximum to zero, it is required that secondary voltage drops within certain specified time under specified limit U_{Slim}.

Two transient responses are permitted:

- Aperiodic damping of secondary voltage $U_{s2}(t)$ and
- Periodic damping of $U_{s3}(t)$

Operation of directional measuring elements in especially distance protection may be affected to a great extent by such transients. Periodic damping may result in similar effects as voltage inversion in series compensated networks, which means that distance relays may see the fault in wrong direction. Transient response of modern voltage measuring circuits and associated digital acquisition chains should prevent any possible relay maloperation caused by inappropriate transient response of primary and associated secondary equipment. In general, it is recommended that for all directional elements based on voltage measurement only the aperiodic damping should be used within CVTs.

11.2.3 Frequency Dependence and Bode Diagram

In present standards for current and voltage instrument transformers, the main parameters are only given for the rated frequency. Examples are magnitude and phase angle error. Other parameters like DC-offset behaviour must be derived from design of current transformers or must be inquired by the manufacturer. The same

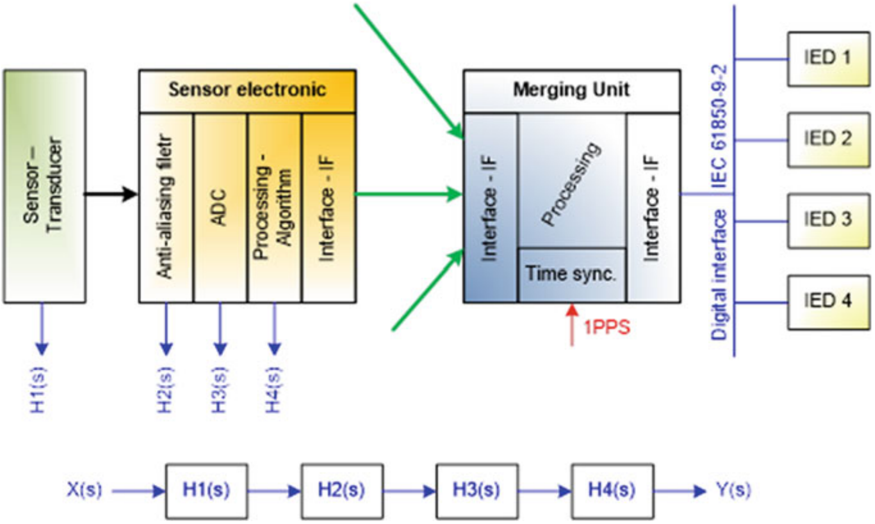


Fig. 11.6 Example of a possible structure of NCIT with SAMU (*Source* [6] Fig. 4.7)

holds for transmission of harmonics, which are getting important role in modern systems with renewable generation, and power electronic converters.

One main benefit of the new sensor technology and data acquisition (see also typical configuration on Fig. 11.6) is the wide range of application. The data can be used for measurement, control and protection, monitoring and power quality analysis. Therefore, the knowledge of frequency response is important and useful for system evaluation.

The Bode plot is a widespread tool to describe the transfer function (magnitude and phase angle) versus frequency. It is valid for linear (for example: no saturation), time-invariant system, what can be assumed for observed application. The Bode plot is usually a combination of a Bode magnitude plot (expressed as dB of gain) and a Bode phase plot (the phase is the imaginary part of the complex logarithm of the complex transfer function).

Figure 11.6 describes a typical "non-conventional data acquisition system" for a process bus application (for more details see also [6]. In the data acquisition system (sensor, sensor electronic) operate different sub-transfer functions, which can be described generally by $H1(s)$ to $Hn(s)$. The total transfer function $H(s) = H1(s).H2(s)...Hn(s)$ is important for the application. The input signal in the Laplace domain $X(s)$ goes through all transfer functions and results in output signal $Y(s)$. The output signal is determined by the transfer functions. For different sinusoidal signals (constant magnitude and variable frequency), the output signal can be damped or amplified as well as shifted in the phase.

Table 11.3 Presents more detailed values of Bode plot of specifically selected values versus frequency

fin[Hz]	16.7	50	60	100	150	250	350	550	750
$H(f)$[pu]	1	1	1	0.999	0.997	0.992	0.985	0.964	0.934
$Ph(f)[o]$	–1.113	–3.624	–4.362	–7.303	–10.97	–18.29	–25.62	–40.26	–54.90

Example of detailed calculation of the complete chain is presented in [6]. Here, we present for this example only the resulting Bode diagram and corresponding conclusions as follows.

- Magnitude error is zero over a wide frequency band (0.5–300 Hz), see additional information on Table 11.3.
- At higher frequencies, the input signal will be damped. This must be considered at calculation of harmonics (correction by a factor). The determination of up to 25th harmonic (1250 Hz for $f_N = 50$ Hz) shall be possible. Higher harmonics need a higher sampling rate, and the down sampling filter must be modified.
- The phase angle shift must be considered in the system. Due to the used decimation filters, the final phase shift at 50 Hz is –3.62°. If the same filters are used in all data acquisition systems, there are no problems for a further signal processing. Otherwise, phase angle correction is necessary within the IED.

11.2.3.1 Conclusions Related to Frequency Dependence and Bode Diagram

The example shows impressively the benefits of the Bode plot, as shown in Fig. 11.7. A lot of helpful information can be derived from such a plot for further signal processing. It helps at evaluation of different data acquisition systems. Interoperability or interchangeability decisions and, further, necessary countermeasure in the IED (algorithm development/improvement) can be derived. This is also the reason why it is recommended that the final Bode diagram (magnitude and phase) should become a part of documentation for the complete secondary data acquisition chain. The best solution for such presentation is the mathematical description of the transfer function in the Laplace or z-domain. The Bode plot should be drawn and presented for the rated values of measured current and voltages. As suggested within the presented example, the frequency range should be at least between 0.01 and 10 kHz.

11.2.4 Dynamic Ranges for Measured Currents and Voltages

Available dynamic ranges for measured currents and voltages are very important for all types of MUs because they directly influence reliable operation of all PAC functions installed within the related IEDs. Annex 9A to IEC 61869-9 standard [3]

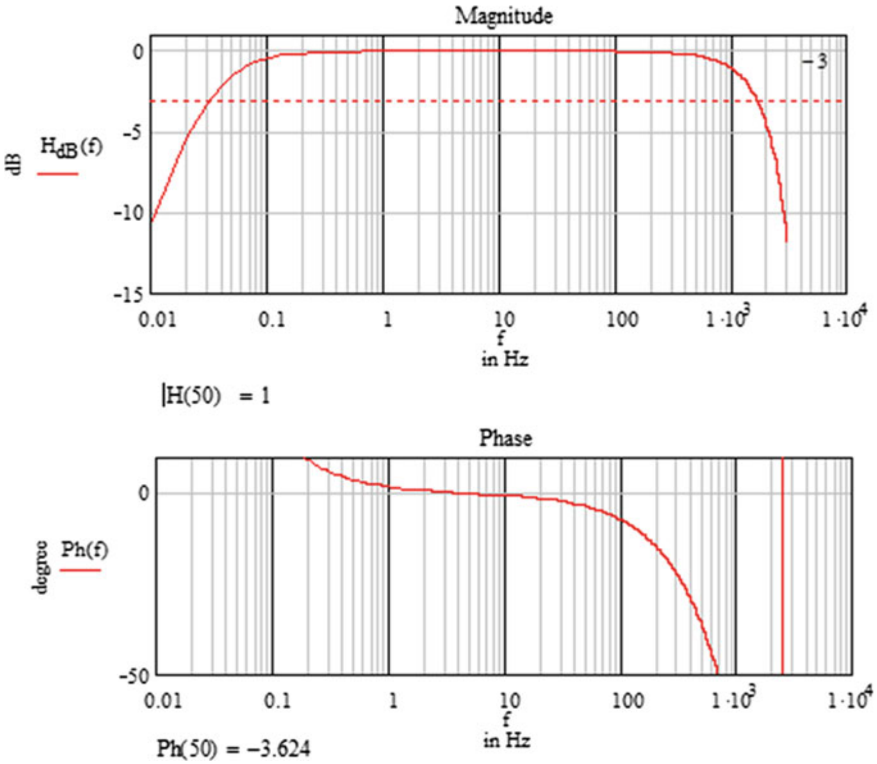


Fig. 11.7 Bode diagram of a complete system (*Source* [6] Fig. 7.1)

provides excellent fixed scaling, which can be used to satisfy the complete dynamic ranges required by the majority of power system applications. Two nomograms within Appendix 9 present in graphical forms the required dynamic ranges for different classes of instrument transformers as well as for the complete range of protection functions. The nomograms are presented also in Figs. 11.8 and 11.9.

Some of the most important values are pointed out as follows (related also to accuracy limit factor):

- minimum value of measured current should be less than 5% of rated input current
- maximum value of measured current should be at least 65 times of rated input current, but when considering also the DC short circuit current component, the maximum value should not be less than 130 times of rated input current
- minimum value of measured voltage should be less than approximately 2% of rated input voltage
- Maximum value of measured voltage should be up to 2.5 times of rated input voltage

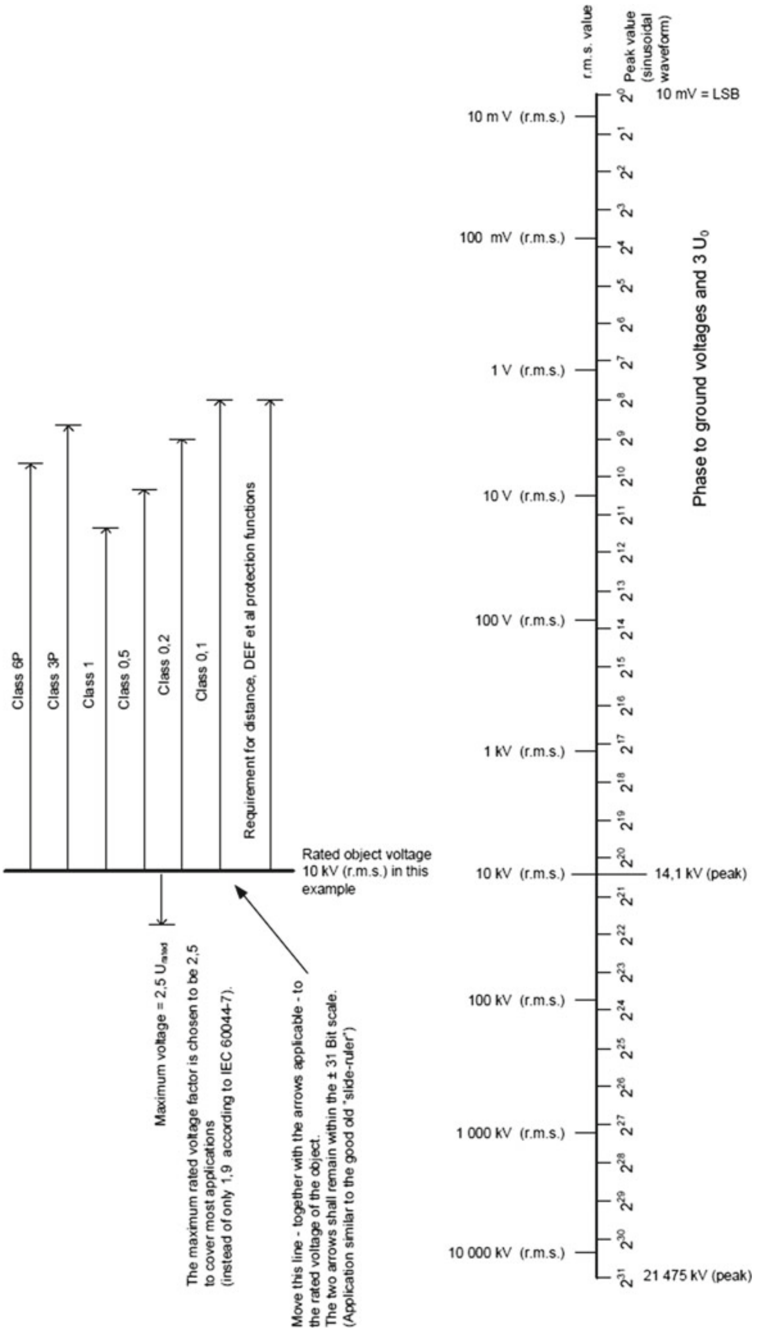

r.m.s. value
Peak value (sinusoidal waveform)
2^{0} 10 mV = LSB
10 m V (r.m.s.)
2^{1}
2^{2}
2^{3}
100 mV (r.m.s.)
2^{4}
2^{5}
2^{6}
1 V (r.m.s.)
2^{7}
2^{8}
2^{9}
2^{10}
10 V (r.m.s.)
2^{11}
2^{12}
2^{13}
100 V (r.m.s.)
2^{14}
2^{15}
2^{16}
1 kV (r.m.s.)
2^{17}
2^{18}
2^{19}
2^{20}
10 kV (r.m.s.)
14,1 kV (peak)
2^{21}
2^{22}
2^{23}
100 kV (r.m.s.)
2^{24}
2^{25}
2^{26}
1 000 kV (r.m.s.)
2^{27}
2^{28}
2^{29}
10 000 kV (r.m.s.)
2^{30}
2^{31} 21 475 kV (peak)
Phase to ground voltages and 3 U_0
Class 6P
Class 3P
Class 1
Class 0,5
Class 0,2
Class 0,1
Requirement for distance, DEF et al protection functions
Rated object voltage 10 kV (r.m.s.) in this example
Maximum voltage = 2,5 U_{rated}
The maximum rated voltage factor is chosen to be 2,5 to cover most applications (instead of only 1,9 according to IEC 60044-7).
Move this line - together with the arrows applicable - to the rated voltage of the object. The two arrows shall remain within the ± 31 Bit scale. (Application similar to the good old "slide-ruler")

Fig. 11.8 Nomogram for voltage (IEC 61869-9 Appendix 9A.1)

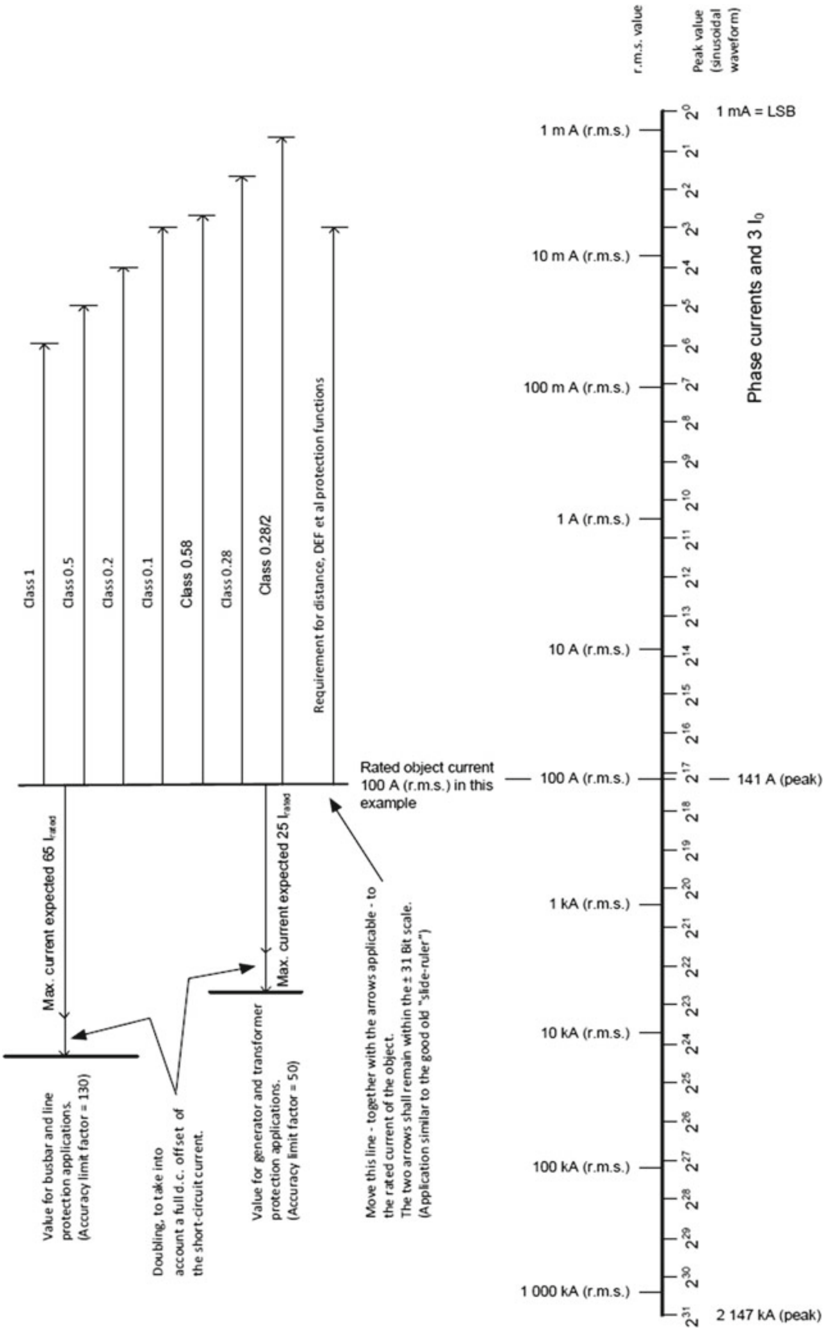

r.m.s. value
Peak value (sinusoidal waveform)
1 mA = LSB
Phase currents and 3 I_0
1 m A (r.m.s.)
10 m A (r.m.s.)
100 m A (r.m.s.)
1 A (r.m.s.)
10 A (r.m.s.)
100 A (r.m.s.)
1 kA (r.m.s.)
10 kA (r.m.s.)
100 kA (r.m.s.)
1 000 kA (r.m.s.)
2^{0}
2^{1}
2^{2}
2^{3}
2^{4}
2^{5}
2^{6}
2^{7}
2^{8}
2^{9}
2^{10}
2^{11}
2^{12}
2^{13}
2^{14}
2^{15}
2^{16}
2^{17}
2^{18}
2^{19}
2^{20}
2^{21}
2^{22}
2^{23}
2^{24}
2^{25}
2^{26}
2^{27}
2^{28}
2^{29}
2^{30}
2^{31}
141 A (peak)
2 147 kA (peak)
Class 1
Class 0.5
Class 0.2
Class 0.1
Class 0.58
Class 0.28
Class 0.28/2
Requirement for distance, DEF et al protection functions
Rated object current 100 A (r.m.s.) in this example
Max. current expected 65 I_{rated}
Max. current expected 25 I_{rated}
Value for busbar and line protection applications. (Accuracy limit factor = 130)
Doubling, to take into account a full d.c. offset of the short-circuit current.
Value for generator and transformer protection applications. (Accuracy limit factor = 50)
Move this line - together with the arrows applicable - to the rated current of the object. The two arrows shall remain within the ± 31 Bit scale. (Application similar to the good old "slide-ruler")

Fig. 11.9 Nomogram for current (IEC 61869-9 Appendix 9A.2)

Specified dynamic ranges can appear rather high or very low for certain electronic equipment and applied algorithms, especially when it comes to conventional input transformers as well as A/D converters. It is for this reason required that all producers of MUs specify their complete dynamic ranges and not only accuracy at rated input currents and/or voltages. This should include also their initial clipping points because clipped signals of voltages and currents definitely influence also the reliable operation of APC algorithms.

11.3 Future Challenges

Modern power systems are currently facing extremely big and important changes, which will definitely significantly influence their needs for reliable operation of secondary equipment as well as communication systems. It is clear that digital communication technology is still a subject to on-going changes, which will continue also in the future and will be especially important for their reliable operation in electric power systems.

Introduction of renewable energy sources and related power electronics is the second very important influencing factor, which requires today important changes also in functionality of applied relay protection and automation systems. Decreasing mechanical inertia or even zero inertia systems require new or significantly improved protection algorithms.

11.3.1 Needs of High Frequency-Based Directional Earth Fault Protection

On the other hand, it is necessary as well to consider some needs of existing power systems and their protection, which is not completely covered by characteristics of current standards. One such example is high frequency directional earth fault protection of resonantly earthed systems (for details, see [6]). Especially in specific European countries, networks up to and including 110 kV are operated to a quite large extent with resonant-earthed neutral points. This practice provides the advantages of the possibility of fault self-extinction (in case of overhead lines) and the option to keep the network in service in case of a single phase to earth fault. However, selective fault detection becomes more challenging due to the low fault current level.

Directional comparison of residual currents ($3.I_0$) and voltages ($3.U_0$) is based on signals with high frequency, which can be expected reasonably up to 5 kHz. Even some higher frequencies are theoretically possible, but they will generally not appear in practice. According to the Nyquist theorem, the sampling frequency must be at least two times of the signal frequency to be detected. Therefore, the minimum sampling frequency to measure the charging oscillation with reasonable precision should be 10 kHz or even 16 kHz (preferred). This means on the other hand that standardised sampling frequencies, as presented in Table 11.2, are not sufficient for such protection application unless we accept for protection purposes also the signals for power quality.

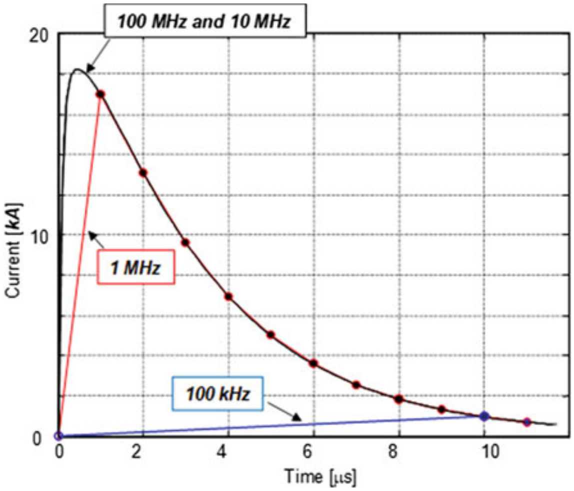
11.3.2 Travelling Wave Protection

One of the possible solutions for reliable protection of power lines (but probably also for some other elements) within low inertia power systems is travelling wave-based protection (TWP).

Travelling wave theory is well known for more than hundred years but has been applied for protection functionality just a few years ago, as the previous technologies used for protection did not allow detection of so extremely fast transients. This technology has been used for some decades before also for fault location purposes on power lines, but not for protection purposes. When discussing at conventional protection functions about time constraints in milliseconds (ms), it is necessary to turn at travelling waves to microseconds (μs). Quite a lot of additional information is available in [6]. Here is presented just a need to required sampling rate of measured currents (generally applied for TWP), which should be far higher than the values proposed so far in different IEC standards, including IEC 61869-9.

Figure 11.10 shows computer simulation of the first incoming travelling wave for a fault on 130 km long transmission line, using different sampling rates. Since travelling waves have speed close to the speed of light, a travelling wave will pass through 300 m in 1 μs. For the travelling wave detection, sampling rate of 1 MHz may be adequate. However, for fault location it may introduce an error of 300 m. For more accurate fault location, higher sampling rate is required.

Fig. 11.10 Impact of sampling rate on travelling wave detection (from [6] Figs. 4–16 from TB768)



Here, we are discussing protection functionality with fault detection time around 150 μs and protection operating time of more than 3 ms, because it depends also on communication between two line ends.

Quite different requirements on fault clearing time appear (and will appear) in DC power systems, which are in fact much closer to their implementation as many of us imagine today. In this respect, we need to discuss fault detection time of less than 150–200 μs and fault clearing time under 500 μs. The required sampling rate for such digital protection is of course related to travelling wave theory and also a sampling rate, as already presented above in Fig. 11.10.

Transmitting one million Sampled Values (but need to consider also three-phase currents and maybe even three-phase voltages, which means six million Sampled Values) per second from a merging units to control houses with protection IEDs is a big challenge even for modern digital communication networks.

This challenge will have to be solved within next five to ten years. Will modern communication tool development allow such approach or, maybe we need to make such protection again close to the basic source of information, which are analogue outputs of CTs and VTs (different technology) close to their basic source? This means that all protection equipment (also a today so-called modern relays) should be installed in the fields close to primary equipment. But this will definitely initiate many additional questions.

11.3.3 Required Protection Operating Time

Fast and reliable operation is one of the highest requirements on modern protection systems, regardless whether they are based on conventional or the latest digital technologies. Different historical disturbance reports show that even electromechanical relays designed for HV and EHV systems have operated faster than 12 ms (in 50 Hz systems). Static (electronic) line protection, based on delta (Δ) quantities, has operated many times faster than 8 ms, while static busbar protection operated many times faster than 5 ms. Requirements on fast operating time are today even more demanding due to significantly decreasing system inertia and increasing amount of power electronic.

Comparing in this respect classical and modern protection systems, we need to consider that digital systems, based on MUs and separated protection devices, need more time to provide final trip signal because they have to cover (compared to classical design) two additional signal transmission times:

- transmission of SV from MU to protection IED (up to 4 ms, see item 4.4.2.)
- transmission of GOOSE tripping command from protection IED to MUs (up to 3 ms, see item 4.4.2.)

This way the final tripping time can be prolonged up to 7 ms. A question appears whether this is acceptable for modern protection systems and especially for travelling wave protection systems, which could provide final tripping signal (including modern communication systems and static output electronic) in less than 5 ms.

References

1. IEC 61850-7-4 Basic Communication Structure—Compatible Logical Node Classes and Data Object Classes, Eddition 2.0, 2010-03. Copyright © 2016 IEC Geneva, Switzerland. www.iec.ch
2. IEC 61850 TISSUE 1176 dated 27.10.2019; https://iec61850.tissue-db.com/tissue/1176
3. IEC 61869-9 (2016) Instrument transformers - Part 9: Digital interface for instrument transformers, https://webstore.iec.ch/publication/24663. Copyright © 2016 IEC Geneva, Switzerland. www.iec.ch
4. IEC 61850-9-2LE: UCA IUG "Implementation Guideline for Digital Interface to Instrument Transformers using IEC 61850–9–2" http://iec61850.ucaiug.org/Implementation%20Guidelines/DigIF_spec_9-2LE_R2-1_040707-CB.pdf
5. IEEE 1588 Standard for a Precision Clock Synchronization Protocol for Network Measurement and Control Systems ("V2" 2008, "V3" 2019) https://standards.ieee.org/standard/1588-2019.html
6. CIGRE TB-768 (2019) Protection requirements on transient response of digital acquisition chain https://e-cigre.org/publication/768-protection-requirements-on-transient-response-of-digital-acquisition-chain

Process bus Applications in IEC 61850 12

Rannveig S. J. Løken

Abstract

There are several generations of architecture of Protection, Automation and Control System based on IEC 61850. In this chapter, the main focus is reference to papers using IEC 61850 Process bus Application with PRP architecture and HSR architecture.

Keywords

IEC 61850 Process bus Application • IEC 61850 PRP Architecture • IEC 61850 Architecture

12.1 Introduction

In Chapter 4, the architecture of a Protection, Automation and Control System (PACS) based on IEC 61850 [1] was introduced.

There are several generations of architecture of Protection, Automation and Control System based on IEC 61850. In many cases, the first step will be to introduce the Station bus with communication between the different IED on the station level and towards the dispatch centre. The measurement and commands to/from the switch yard are in this first step normally implemented using hardwired copper cabling.

The next step of the architecture of the PACS based on IEC 61850 is to include digitalisation towards the primary equipment by using IEC 61850-9-2 [2]. The hardwired copper cabling will then be replaced by an optical fibre-based network.

R. S. J. Løken (✉)
Statnett, Oslo, Norway
e-mail: Rannveig.loken@statnett.no

P. Bishop and N.-K. C. Nair (eds.), *IEC 61850 Principles and Applications to Electric Power Systems*, CIGRE Green Books, https://doi.org/10.1007/978-3-031-24567-1_12

12.2 Protection, Automation and Control System with Station bus and Process bus

IEC 61850-5 [3] uses the terms “Station bus” and “Process bus” with no precise definition. In reality, these two buses are not specific physical entities, i.e. any particular segment of LAN cabling or LAN switches could be carrying both Station bus- and Process bus-related signals. Therefore, in order to understand what is meant by “Process bus Implementation” it is necessary to define exactly what is meant by “Process bus”. Please also see Chapter 4 for further description.

IEC 61850-2 [4] defines 3 “levels” of devices in an automation system:

1. Station Level: station HMI, gateway interface to SCADA and station loggers
2. Bay Level: protection relays, meters and controllers
3. Process level: switchgear, transformers, sensors and I/O interfaces

There can be communication between the station level devices and the bay level devices, as well as bay level to bay level or station level to station level—this type of communication has been termed “Station bus” and is typically based on IEC 61850-8-1 [5] MMS and GOOSE messages. However, it is also possible that a conventional CT/VT input protection relay is publishing IEC 61850-9-2 [2] Sampled Values which are used by other SV subscribing relays on the system. Hence, Station bus can carry all three protocols.

There can be communication connection between the bay level devices and the process level devices—this has been termed “Process bus”, as it refers to messages only related to the process interface equipment, i.e. to the primary plant. These messages include critical status of the process equipment (GOOSE) and instantaneous analogue values of the primary system (Sampled Values) as used by the bay level devices. The Process bus is also carrying messages from/to the station level HMI or gateway as commands to the primary plant (open/close, on/off, raise/lower …) and receiving reporting from the primary equipment. Hence, the Process bus can also carry all three protocols

It is therefore possible to consider the substation LAN as the (proverbial) “communication cloud” linking all three levels as shown in Fig. 12.1.

In the physical implementation of any system, based on the asset owner network policy and device capabilities, further decisions must be made about the physical implementation of the substation LAN based on the individual IED capabilities—e.g. the bay level devices may inherently have different ports for the SV messages to the GOOSE and MMS messages—even so, they could be connected to different switches associated with independent physical LANs, or both of those ports could be connected to the same LAN switch.

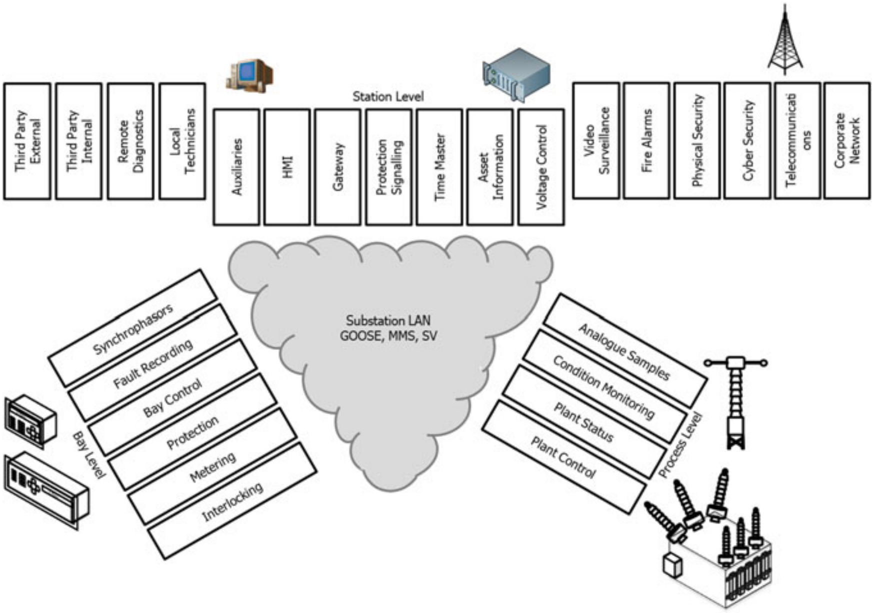


Fig. 12.1 PACS cloud linking three substation levels (*source* [6])

12.3 Process bus Structures [7]

The structure of the architecture of Process bus is not defined in the IEC 61850 standard [1]. The technical report IEC 61850-9 [8] shows different suggestion to architecture that is possible to use in a Protection, Automation and Control System (PACS). It is possible to combine the Station bus and the Process bus in the same physical network, or it is possible to have them in physically separate network. The digitalisation will be performed in the switch yard close to the primary equipment by use of Merging Unit (MU), Stand-Alone Merging Unit (SAMU) and Switchgear Control Units (SCU). The MU is used in case of Low-Power Instrument Transformer (LPIT) components, and the output for the MU is on the IEC 61850-9-2 format [2]. The SAMU is used to convert analogue voltage and currents from conventional instrument transformers to digital values based on the IEC 61850-9-2 format [2]. The SCU will convert the commands from IEC 61850-9-2 [2] format to binary contact signals that can be used to trip the coils in the primary equipment like circuit breaker, disconnector and earthing switch. If the primary equipment has an IEC 61850 [1] interface, there will be less need for SCU and SAMU as they can be connected directly to the network. The IEC TC 38 [9] address the performance of the MU and SAMU, to make sure that the MU/SAMU and IED will function well together in the functional chain, part 13 is published, and part 7 is for review at this stage, please also refer to Chapter 11. In recent years, an increasing number of publications have reported the design or commissioning of demonstrations, pilot projects, pre-series or series of fully digital PACS using IEC 61850 Process bus. This constitutes a major development, as up to now PACS were mainly using only IEC 61850 Station bus. The availability on the market of Intelligent Electronic Device (IED), Stand-Alone Merging Units (SAMU), Merging Units (MU), Switchgear Control Unit (SCU) and Low-Power Instrument Transformers (LPIT) sustains this trend.

The scope, goals and design of these projects vary widely. This includes the number of feeders, the number of different manufacturers involved, the use of LPIT and/or SAMU, with or without trip signal to the circuit breakers (real trip—closed loop/monitoring only—open loop). Also, the estimated or reported economic benefits show a considerable variation depending on the considered use case and context.

12.3.1 Process bus Using HSR and PRP Architecture

In the following subchapters, examples from projects in published papers, that use High-availability Seamless Redundancy (HSR) in combination with Parallel Redundancy Protocol (PRP) architectures for Process bus, are shown.

12.3.1.1 FITNESS SP Energy Networks (UK): Multivendor Open Loop

FITNESS is a pilot project [10] in a 275 kV substation in Scotland on two line bays, please refer to Chapter 10 in Sect. 10.12.1 for further details. The equipment provided by several vendors includes LPIT and SAMU connected via a redundant Process bus and is deployed in open loop, without trip contact connected to the circuit breaker, in parallel with the conventional system. Refer to Fig. 12.2.

The FITNESS PACS includes protection IED and Bay Control Unit (BCU) from the same vendors. The LPIT and MU from one vendor are connected to protection IED and BCU of another vendor to investigate multi-vendor issues in an IEC 61850-9-2 [2] Process bus system.

Manufacturer Message Specification (MMS) and Generic Object-Oriented Substation Events (GOOSE) services are utilised at Station bus level, whereas Sampled Values (SV) and GOOSE services are utilised at Process bus level in this project. In addition, the project investigates different network architecture on the Process bus using one bay with High-Availability Seamless Redundancy (HSR) system and the other with Parallel Redundancy Protocol (PRP) system.

The main purpose of the project was to investigate interoperability between different vendors, reduce the outage duration and master risks during substation asset replacement by replacing hardwired signalling with digital communication. In addition, faster deployment, greater availability, improved safety and greater controllability with a reduced footprint and lower cost than conventional design were another purpose of the project. The execution of the project provided valuable insight about IEC 61850-based testing and engineering and prepared the requirements of the next-generation substations of SPEN.

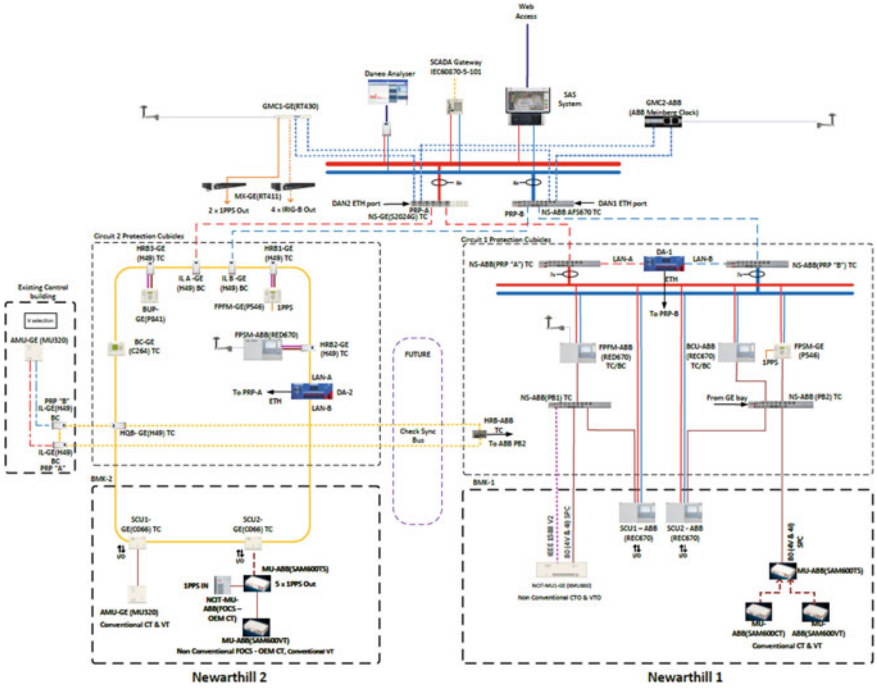
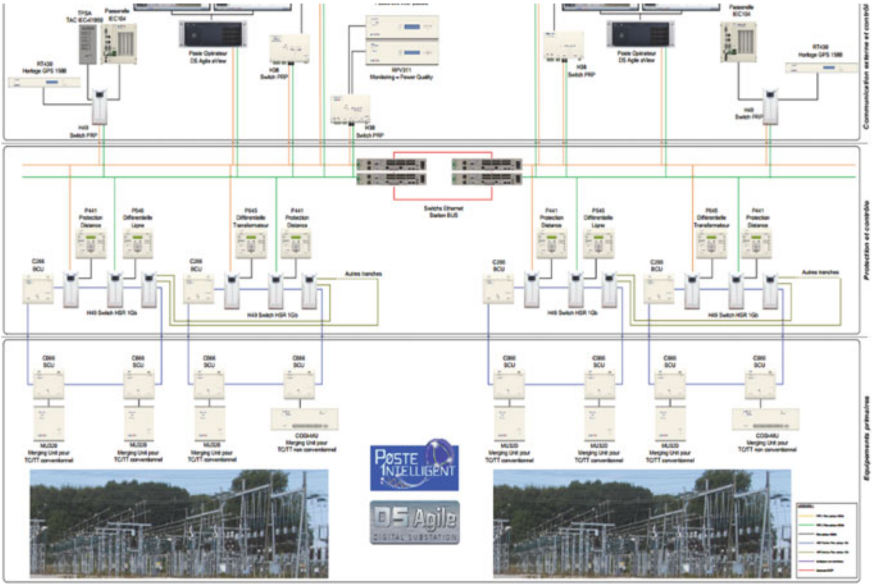


Fig. 12.2 FITNESS project architecture

12.3.1.2 RTE "Postes Intelligents" Project (FR): Active Demonstrator

RTE's "Postes Intelligents" project (Smart substation in French) consists in the installation of completely digital PACS in two substations (Blocaux 225 kV/90 kV and Alleux 90 kV) situated in northern France [11]. The project was designed as demonstrator for several innovative technologies including Process bus, LPIT and digitally interfaced primary equipment. For some feeders, LPIT interfaced directly via IEC 61850 Process bus are employed. One important characteristic of the "Postes Intelligents" PACS is the implementation of process-near acquisition and marshalling equipment in external cabinets installed in the switchyard including all hardwiring connections of switchyard equipment, which are in turn connected to the cubicles hosting protection and control IED by optical fibre. Refer to Fig. 12.3.

For the "Postes Intelligents" project, Parallel Redundancy Protocol (PRP) was selected for the Station bus and High-Availability Seamless Redundancy (HSR) system was selected for the Process bus. Two bays were combined in one HSR ring in addition to an inter-bay HSR ring. The Process bus is used both for the data acquisition of the protection functions and for tripping. No conventional hardwired "back-up" system is implemented, neither for data acquisition nor for tripping. The project design also included an online spare IED that can replace any faulted IED in the system upon request.



TPSA TAC IEC61850
Passerelle IEC104
RT430 Horloge GPS 1588
Poste Opérateur DS Agile aView
H38 Switch PRP
RPV311 Monitoring + Power Quality
H49 Switch PRP
Switchs Ethernet Station BUS
P441 Protection Distance
P546 Différentielle Ligne
P645 Différentielle Transformateur
C266 BCU
H49 Switch HSR 1Gb
Autres tranches
C066 SCU
MU320 Merging Unit pour TC/TT conventionnel
COSI4MU Merging Unit pour TC/TT non conventionnel
POSTE INTELLIGENT
DS Agile DIGITAL SUBSTATION
Communication externe et contrôle
Protection et contrôle
Equipements primaires

Fig. 12.3 Blocaux substation architecture

One of the major aims of the project was to design, test and commission a PACS based on IEC 61850 Station bus and Process bus. The gained experience is used to specify and design the next generation of fully digital PACS.

12.3.1.3 National Grid VSATT Project (UK): Multivendor Test Platform

The approach of National Grid from UK was to first design a complete test platform for the future generation of PACS—the Virtual Site Acceptance Testing and Training facility (VSATT) [12]. This platform allows to test the interoperability of IEDs of different vendors when used in the chosen Process bus architecture. The VSATT facility includes an in-house developed data monitoring tool, which can visualise data flows in IEC 61850 networks to validate the information exchanged. Each bay has two physically isolated Process buses for redundancy purposes. Process bus 1 and Process bus 2 are used to exchange local SV/GOOSE messages for Main Protection 1 and 2 systems, respectively.

The measurement bus (or inter-bay Process bus) provides high accuracy metering across bays, such as SV with 256 samples per cycle. Each bay which requires high accuracy metering should install a separate Merging Unit (MU) connected to the measurement bus. The bay solutions can be provided by different suppliers. Each supplier configures IEC 61850 [1] devices, e.g. MUs and Intelligent Electronic Devices (IEDs), for its own bay. This bay solution-based approach reduces the possibility of having interoperability issues within a bay and simplifies the system integration process. The concept is based on a standardised design and configuration that can be rolled out repeatedly at various sites. The Station bus provides a digital interface for the local HMI as well as to the remote control centre to access and control any bay IEDs via IEC 61850-8-1 MMS messages. Also, inter-bay signals (e.g. station-wide automation schemes, CB failure trip, etc.) could be transmitted via GOOSE over the Station bus. The Station bus (or measurement bus) can be implemented either as a ring network with the High-availability Seamless Redundancy (HSR) protocol or two parallel networks with the Parallel Redundancy Protocol (PRP).

12.3.2 Process bus Using PRP Architecture

In the following subchapters, examples from projects in published papers, that use Parallel Redundancy Protocol (PRP) architectures for Process bus, are shown.

12.3.2.1 TransGrid Project Avon (AU): Multivendor Series Deployment

The Avon substation project realised by TransGrid Australia [13] is an operational PACS with Process bus. The transition to PACS with Process bus involved both technological change in addition to culture and operational practices, and therefore, it was very important to ensure full support by management and clear identification of benefits roadmap. Refer to Fig. 12.4.

The Avon Digital PACS includes protection, control, metering and condition monitoring interfaced via the Stand-Alone Merging Units (SAMU). This required digitalisation in the yard of binary contact signals, current transformers, voltage transformers and analogue sensors. Digitisation close to the source allows each piece of data to be digitised once and used multiple times. It also minimises the number of connections and reduces cable sizes and lengths.

Two redundant secondary systems are provided at Avon, each from a different manufacturer. This was implemented to limit interoperability as earlier testing had revealed interoperability issues.

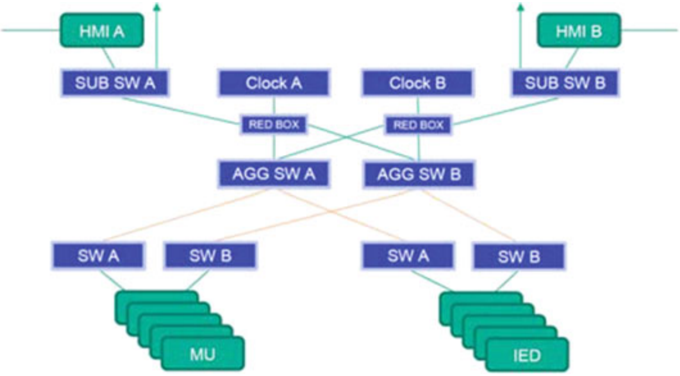


Fig. 12.4 Network topology for one system of TransGrid Avon system

In order to increase reliability of the overall system, Parallel Redundancy Protocol (PRP) was implemented on both No. 1 and No. 2 systems. To minimise connections to the yard and allow compensated time correction to end devices, PTP was implemented over the same Ethernet connection. To handle the large volume of Sampled Values, VLANs were assigned to each SV stream based on IEC 61850-9-2LE [2]. This created a virtual point-to-point connection for instrument transformer Sampled Values and ensured that each IED received on its Ethernet port only the data it required and no additional information. The system is deployed as a full-scale project without a conventional back-up system in parallel.

The Avon project was designed to use Process bus in an overall optimised way and to act as a pilot PACS for subsequent rollouts. The approach is based on process-near digitalisation in order to save substantial costs by replacing copper cable by optical fibres and enable faster testing and commissioning.

12.3.2.2 Statnett R&D Project Digital Substation (NO): Multivendor Open Loop

The R&D digital substation PACS pilot project is installed in the Furuset substation from Statnett [14]. The main objective was to investigate benefits from the use of IEC 61850 Process bus and, on that way, investigate new ideas challenging some traditional PACS design principles. The approach was to combine many functions in a restricted number of IEDs to investigate into the interoperability between protection and control equipment from different vendors. The equipment provided by several vendors includes LPIT and SAMU connected via a redundant Process bus based on Parallel Redundancy Protocol (PRP) network and is deployed in open loop in parallel with the conventional system. The control functionality and distance protection 1 for two separate 300 kV line bays were included in one Protection and Control Unit (PCU1), whereas PCU2 contained back-up control and distance protection 2 for the same two bays. Additionally, PCU3 was used for distance protection 3 for the two lines and PCU4 for the distance protection 4 for Line 1. The use of Process bus instead of hardwired connection to the primary bay introduces the possibility for new design of the control and protection in a substation. The system was time synchronised on the Process bus from two time sources, GPS1 and GPS2, using the Precision Time Protocol (PTP) v2 to ensure 1 μs accuracy. Refer to Fig. 12.5.

The main purpose of the project was to gain experiences with Process bus installations, LPIT, reduce the size of the PACS and investigate interoperability between several vendors. The execution of the project provided important experience about testing. Interoperability issues due to heterogeneous implementation of options of the standard by the vendors have been identified.

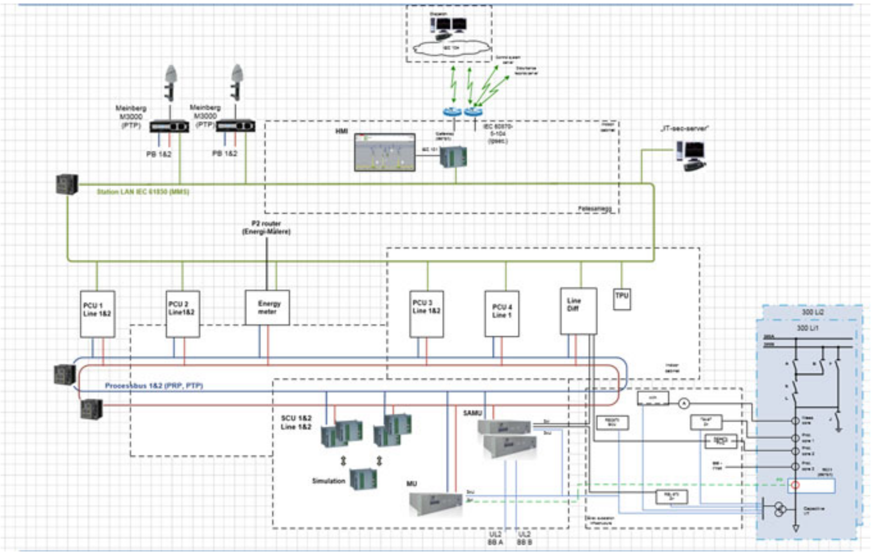


Fig. 12.5 Architecture of Statnett R&D digital substation

12.3.3 Choice Between PRP and HSR [7]

In an IEC 61850 LAN which carries Sampled Values, a disruption of this duration is not acceptable due to requirements for availability and reliability of protection and automation functions on bay level or for the whole substation.

Only two network redundancy protocols providing a “zero recovery time” are recommended by IEC 62439-3 [15]: HSR and PRP. They both rely on the following principle: Frames are sent and received on both ports simultaneously for every IED. More precisely, two identical frames are sent on both ports and only the first received frame is processed whilst the second is discarded.

HSR, for High-availability Seamless Redundancy (Fig. 12.6 Left): The IEDs are connected together as a ring. This architecture is favoured when the number of IED is limited. The network is resilient to one node failure. Every frame transits through every IED.

PRP, for Parallel Redundancy Protocol (Fig. 12.6 Right): The IEDs are connected to two independent LANs. The network is resilient to one LAN failure. A PRP interface on an IED has two physical ports but a unique MAC and IP address.

In Table 12.1, advantages and drawbacks between HSR and PRP are summarised.

Given the constraints of the system in maintainability, scalability and continuous availability, PRP is recognised to be more appropriate for R#SPACE’s LAN.

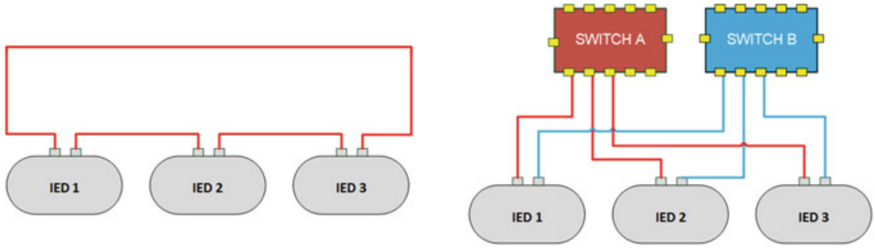


Fig. 12.6 Seamless network redundancy protocols HSR (Left) and PRP (Right)

Table 12.1 Comparative assessment between HSR and PRP

	HSR	PRP
Advantages	• No of few switches required • No switch configuration required for ring topology	• No switch configuration required for redundancy • More flexibility for topology, evolution, and maintenance • Traffic optimisation possible
Drawbacks	• Same traffic for every IED in the ring → more bandwidth required • Less scalable: Bandwidth compatibility of every IED of the ring required • Interruption of ring in case of addition, removal, update, or maintenance on an IED in the ring	• 2 physical LANs implemented and maintain (cost impact) • System collapse in case of interconnection between the 2 LANs (human mistake) • Switches required

12.3.4 Process bus Using Direct Link Architecture

There are examples where the hardwired copper cables are replaced by fibres connecting the primary components to the IEC directly without use of switches or network.

There will normally be two separate protection system with its own IED/MU/SAMU/SCU chain. This solution is similar to the hardwired solution of today.

In a paper from Canada [16], an IEC 61850-9-2 Process bus architecture where the copper wiring is replaced by placing electronic modules throughout the switchyard and using fibre communications for fast exchange of data between the switchgear and the control room is presented. The primary goal is to deliver switchyard data to the protection and control devices and to return commands from the latter to the switchyard devices. The Merging Units are designed to interface with all signals typically used for SAS as close to their respective origins as practical. The outdoor fibre cables contain a pair of DC supply wires to provide control power to the Merging Units including the internal wetting voltage for field contact sensing within the switchgear associated with each Merging Unit, independent

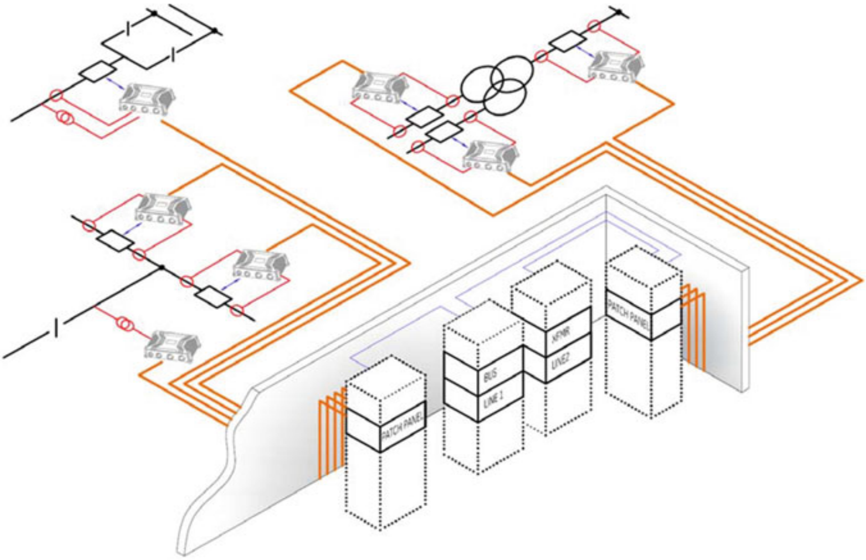


Fig. 12.7 Process bus architecture for a distribution system

from the control power in the field. Patch panels are used to land and organise the outdoor cables and to distribute and individually fuse the DC power to the Merging Units. Standard patch cords are used to accomplish "hard-fibering", making all the necessary IEC 61850 [1] connections between the relays and the Merging Units as dictated by the station configuration on a one-to-one basis, without the use of switched network communications as detailed below in Fig. 12.7.

12.3.5 Software Defines Process bus Networks [17]

Software-defined networking (SDN) is an emerging technology that offers significant benefits to simplify the management of network switches that form an IEC 61850 Process bus Furthermore, it provides a platform to enhance the cybersecurity protection of access to the SDN switches by providing timely reports of misconfiguration of the Process bus switches. A model-based systems engineering (MBSE) description of the Process bus operating configuration is described. This view is generated as a black-box and white-box description of the SDN switch management process that uses the SDN controller and communication flow control to assign the switch ports.

SDN virtualises or abstracts the functionality of dedicated network devices into a software function to facilitate network management by dynamically configuring the network resources. SDN facilitates this scheme by separating the network's control and forwarding planes, thus enabling the network control to become directly programmable. In Fig. 12.8 a high-level view of Open Network Foundation (ONF) SDN network architecture is shown.

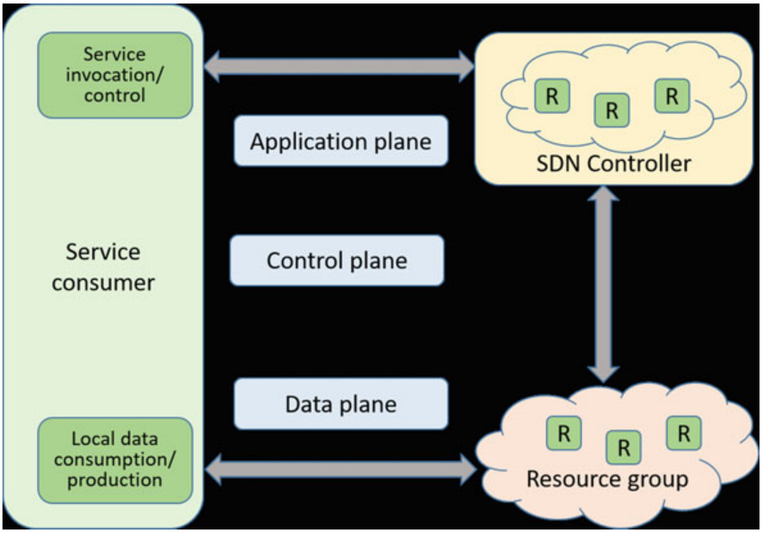


Fig. 12.8 ONF defined SDN network architecture

These models can be expanded to define the user requirements for any SDN solution.

12.4 Advantages and Drawbacks

The projects that have been described in paragraph 3.3.1 and 3.3.2 are of various types and scopes, but all of them have given experience to the utilities that have investigated the project.

The projects from France and Australia are full-scale deployment of Protection, Automation and Control Systems with Process bus. These projects provide experience in design, engineering, commissioning and operation for real fully digital PACS.

TransGrid indicates that they will use the same design as the demonstrator for several substations in the years to come, whereas the experience feedback from the two full-scale substations in France will be used to specify the design of future fully digital PACSs with Process bus. The two projects from United Kingdom and the one from Norway are open loop demonstrations without the trip to the circuit breaker. The advantage of this type of project is that it is possible to try, without the risk of maloperations, new designs that might be a good approach for a future PACS with Process bus. The drawback is that there is a need to prove that a design for one or two bays or a lab model is relevant for the full-scale deployment.

The bus structure for the projects had different architectures. In the FITNESS project, two different bus architectures for Process bus were implemented, both

HSR and PRP. This allowed a comparison of the two architectures during the different phases in the project and to obtain real experience from the combined design. In the Statnett project, PRP was chosen for both of the bays of the Process bus. There was a physical separation between Station bus and Process bus, in addition to use of VLAN for data segregation on the Process bus for both of these projects. In the TransGrid project, two different physical PRP networks were implemented, one PRP network for each vendor. The advantage of this design was two physical segregated networks covering measurement, protection and trip for each vendor systems. The Station bus and Process bus were segregated using VLAN and not separate physical networks. The "Postes Intelligents" project had two duplicated parallel networks consisting of PRP network on the Station bus and Process bus based on HSR. Each HSR ring on the Process bus combined two bays; in addition, there was an inter-bay HSR ring. One of the advantages of this architecture was that it was possible to upgrade one of the systems with Station bus and Process bus and have the other system in full operation. The VSATT project was focussed on a bay design and had developed an architecture with two redundant Process buses for each bay related to main 1 and main 2 protection systems. In addition, there was an inter-bay Process bus used across the substation for busbar protection and other functions needing measurement from several bays. The Station bus is physically separated from the Process bus and can be on HSR or PRP design.

All analysed digital substations projects demonstrate that the IEC 61850-based Process bus technology is mature and ready for massive deployment. The availability of LPITs and SAMUs with IEC 61850-9-2 LE and/or IEC 61869-9 interfaces from multiple suppliers from Europe, North and South America and Asia provides a wide range of options to be used for the most efficient design of digital substations.

Whilst today all projects are based on the IEC 61850-9-2 LE implementation guideline, future design should be based on the IEC 61869-9 standard, which provides backward compatibility with the LE guideline.

Further improvements in the efficiency of fully digital PACS are possible using integrated primary equipment—digitally interfaced switchgear—with optical sensors.

The operational interoperability between devices from different manufacturers is significantly improved as demonstrated during the 2019 UCA International Users Group hosted interoperability testing in Charlotte, NC, USA, during the week of September 23–27, 2019. Most of the challenges are related to the engineering of digital substations due to some lack of support of all sections of the system configuration language (SCL) files.

12.5 Process bus Sampled Values Other Than CT and VT

The digitisation of the primary current and voltage waveforms has been an extremely topical discussion since the release of the source sampling Logical Nodes TCTR and TVTR in IEC 61850-7-4 (2003) along with IEC 61860-9-1 (2003) and IEC 61860-9-2 (2004) and the UCAIUG industry guideline referred to as “IEC 61850-9-2LE”. It is important to note that the “LE” document is not an official standard, but just a guide for the various vendors considering implementing Sampled Values on how to configure the various parameters reasonably consistently in their respective Merging Units, largely based on the old IEC 60044-8. The differences between the “LE” document parametrisation and those of IEC 61869-9 are discussed in Chapter 11.

Edition 1 of IEC 61850-7-4 only had two T group Logical Nodes: TCTR and TVTR, representing the CT and VT waveform samples.

The CT/VT samples need an extremely high level of guaranteed transmission and reception where the subscribing protection functions cannot afford to have messages lost due to a LAN failure. The Merging Units publishing the TCTR/TVTR SV therefore generally need the PRP or HSR, as well as the subscribing ports of the bay level IED architecture to ensure maximum reliability of message reception.

IEC 61850-7-4 Edition 2 in 2010 added a further 20 T group Logical Nodes dealing with a wide range of analogue sensors as shown in Table 12.2.

These T group Sensor Logical Nodes are all sources of Sampled Values as the time-based direct analogue value. Of course, these samples can be at widely varied sampling rates from “thousands of samples per second” to “thousands of seconds per sample”, e.g. the temperature of the transformer (using TTMP) may only need to be sampled once every minute or the level of the water in the dam (using TLEV) only need to be taken once every hour. Equally, the definition of the SV dataset elements will not be constrained as is the case with the four currents and four voltage samples in an IEC 61869-9 dataset.

In terms of overall architecture, and as discussed in [18], the non-CT/VT Sampled Values generally do not represent real-time critical information to the same extent as the CT/VT samples. Obviously, aspects such as a particular level in a reservoir of some sort may have certain critical implications, but a message failing to be delivered for a few seconds whilst the LAN “recovers” after a failure is perhaps not so critical, but should be assessed on a case-by-case basis.

However, even though the Process bus is implemented with HSR and/or PRP “bumpless” redundancy and dual LAN port sensors, these other T group LNs would generally only warrant IEDs with a single port. This is not inconsistent with PRP networks as the sensor only needs to communicate on one of the LANs, provided the subscribing IEDs are connected to the same LAN. However, HSR inherently requires messages to travel in both direction, and hence, single port sensors and subscribers would need to be connected via a HSR Redundancy Box (a.k.a RedBox).

Table 12.2 IEC 61850-7-4 Ed2 (2010) T Group Logical Nodes [18]

	Logical Node	Analogue value
1	TANG	Angle
2	TAXD	Axial displacement
3	TCTR	Current transformer
4	TDST	Distance
5	TECW	Measurement of electrical conductivity in water
6	TFLW	Liquid flow
7	TFRQ	Frequency
8	TGSN	Generic sensor
9	THUM	Humidity
10	TLEV	Level sensor
11	TLVL	Media level
12	TMGF	Magnetic field
13	TMVM	Movement sensor
14	TPOS	Position indicator
15	TPRS	Pressure sensor
16	TRTN	Rotation transmitter
17	TSND	Sound pressure sensor
18	TTMP	Temperature sensor
19	TTNS	Mechanical tension/stress
20	TVBR	Vibration sensor
21	TVTR	Voltage transformer
22	TWPH	Water acidity

12.6 Recommendations

There are also numerous other projects featuring Process bus pilot or demonstration PACS in all parts of the world. Many utilities have adopted a conservative approach trying to gain some experience before committing to a large-scaled roll-out of fully digital substations. The scope, goals and design of these projects vary widely.

The published experience feedback does not report major problems with the use of Process bus. This includes HSR and PRP architectures and Process bus conveying both Sampled Values and trip GOOSE.

The interest in digital PACS is driven by the significant benefits that they offer in comparison with conventional, hardwired substations. However, the estimated or reported economic benefits show a considerable variation depending on the considered use case and context.

IEC TC95 WG2 [19] is commissioned to investigate and develop guidelines and standards for functional interoperability for digitally interfaced protection and control functions.

An industrial deployment of process-based PACS will only happen if they can be competitive with respect to the conventional PACS. This includes the economic evaluation, but also other criteria like safety and sustainability.

Regarding LPIT, their industrial deployment is in practice conditioned by the availability of Process bus-based PACS. This illustrates that it is not always possible to compare only conventional and process-based PACS, since advantages of use of LPIT might largely compensate higher costs for the control system.

An emerging trend is digital substations designed as centralised substation PACS with a digital process interface and the different protection, measurement, monitoring and control applications running on redundant substation level servers. Hybrid PACS systems with the distribution of various functions between process interface IEDs and central computers are also an alternative architecture being tried in existing projects.

There is a need for all manufacturers to fully implement the features of the IEC 61850 standard that will improve the interoperability not only between the devices, but also between the engineering and testing tools.

References

1. IEC 61850 Communication networks and systems for power utility automation, full standard, https://webstore.iec.ch/publication
2. IEC 61850-9-2 2011 Communication networks and systems for power utility automation- Part 9-2: Specific communication sercie mapping (SCSM)—Sampled values over ISO/IEC 8802-3, IEC 61850–9–2:2011+AMD1:2020 CSV, "Copyright © 2011 IEC Geneva, Switzerland.www.iec.ch" | IEC Webstore | cyber security, smart city, LVDC
3. IEC 61850-5: 2013 Communication networks and systems for power utility automation- Part 5: Communication requirements for functions and device models, IEC 61850-5:2013, "Copyright © 2013 IEC Geneva, Switzerland.www.iec.ch" | IEC Webstore | LVDC
4. IEC 61850-2:2019 Communication networks and systems for power utility automation-Part 2: Glossary, IEC TS 61850-2:2019, "Copyright © 2019 IEC Geneva, Switzerland.www.iec.ch" | IEC Webstore
5. IEC 61850-8-1: 2011 Communication networks and systems for power utility automation, Part 8-1: Specific communication service mapping (SCSM)—Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3, IEC 61850-8-1:2011+AMD1:2020 CSV, "Copyright © 2011 IEC Geneva, Switzerland.www.iec.ch" | IEC Webstore | LVDC
6. Rod Hughes Consulting Pty Ltd. https://rodhughesconsulting.com/: IEC 61850 Training Courses
7. CIGRE session 2020, paper B5-216, e-cigre > Publication > Design constraints and choices for the LAN in RTE's R#SPACE system
8. IEC 61850-9: 2011 Communication networks and systems for power utility automation-IEC 61850:2022 SER, "Copyright © 2011 IEC Geneva, Switzerland.www.iec.ch" | IEC Webstore | LVDC
9. IEC TC 38, IEC-TC 38 Dashboard > Structure: Subcommittee(s) and/or Working Group(s), Membership, Officers, Liaisons

10. CIGRE session 2018, paper B5-207, e-cigre > Publication > FITNESS Multi-Vendor Interoperability in Digital Substations
11. CIGRE session 2018, paper B5-215, e-cigre > Publication > Experience Feedback of Testing and Commissioning of a fully Digital IEC 61850 based PACS
12. CIGRE session 2018, paper B5-206, e-cigre > Publication > Design of multi-vendor bay solutions and their interoperability performance assessments in a fully digital substation
13. DPSP 2018. https://doi.org/10.1049/joe.2018.0171
14. CIGRE session 2018, paper B5-203, e-cigre > Publication > Experience with Process bus in Statnett R&D project Digital substation
15. IEC 62439-3: 2021 Industrial communication network- High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR), IEC 62439-3:2021, "Copyright © 2021 IEC Geneva, Switzerland.www.iec.ch" | IEC Webstore
16. CIGRE session 2008, paper B5-105, e-cigre > Publication > A practical IEC61850-9-2 Process bus architecture driven by topology of the primary equipment
17. CIGRE session 2020, paper B5-201, e-cigre > Publication > Implementation of Digital Substation Automation Systems in Brazil - Challenges and Findings
18. Rod Hughes Consulting Pty Ltd. https://ideology.atlassian.net/l/c/s7KiH65C: IEC 61850 T Group Logical Nodes
19. EC TC 95 WG 2, IEC - TC 95 Dashboard > Documents: Working Documents, Other Documents, Supporting Documents

13 Wide Area Implementations of IEC 61850 Substation Systems

Mark Adamiak and Herbert Falk

Abstract

As the complexion of the grid becomes more diverse with the integration of significant levels of Distributed Energy Resources (DER), the need for advanced control and measurement tools becomes more acute. Moreover, as we look to the future, the concept of dynamic contingency analysis, that is the ability to detect and remediate incipient failure modes on the grid, is in the offing. This technology requires knowledge of the “state” of the grid as viewed through the value of the Synchronised Positive Sequence voltage (known as a Synchrophasor) at all substations in the grid at the same instant in time (distribution state estimation is forthcoming). Such visibility is referred to as the Situational Awareness of the power grid. This chapter will review the concept of the synchrophasor, the secure transmission of such via the IEC 61850 Routable Sample Values (R-SV), an overview of and an array of Smart Grid applications based on the availability of secure event-based communications (Routable GOOSE).

Keywords

Synchrophasor • PMU • Routable GOOSE • Routable Sampled Values

M. Adamiak (✉)
Adamiak Consulting LLC, Paoli, USA
e-mail: adamiakconsulting@aol.com

H. Falk
OTB Consulting Services LLC, Troy, USA
e-mail: herb.falk@otb-consultingservices.com

P. Bishop and N.-K. C. Nair (eds.), *IEC 61850 Principles and Applications to Electric Power Systems*, CIGRE Green Books, https://doi.org/10.1007/978-3-031-24567-1_13

13.1 Synchrophasors

The concept of the phasor dates back to an 1893 AIEE paper by Charles Proteus Steinmetz where he first proposed using complex numbers to describe AC waveforms. In this paper, he described the plots of the complex numbers on a real and imaginary axis as phasors. Phasors have been used ever since to describe the relationship between voltages, currents and impedance on the power system. This technique works well in offline simulation tools where all values are computed on the same time base. However, when applied in real time, phasors measured at different locations typically do not have an accurate common time base.

In the late 1970s, American Electric Power (AEP) was performing research on the use of digital computers to protect power lines. In the course of this research, it was identified that the Fourier transform being used in the protection algorithms would rotate angle in proportion to the off-nominal power system frequency. Analysis of this phenomenon brought to light the fact that if the calculation of the Fourier phasor was synchronised to absolute time, then phasors calculated throughout the power system would all be related. Thus was born the Synchrophasor.

The definition of the Synchrophasor is most simply given by the equation:

$$x(t) = X_{mt} * \mathrm{Cos}(\omega t + f_t) \tag{13.1}$$

where the Synchrophasor magnitude is: $(X_{mt}/\sqrt{2})$ where the magnitude and angle are measured at a specific instant in time "t" and as referenced to a Cosine reference signal by a precision time source such as a Global Positioning System (GPS) clock. This is illustrated in Fig. 13.1 which shows the a waveform with the peak of the Cosine and a Time Pulse—labelled with Universal Time Coordinated (UTC) time highlighted. The magnitude of the reported Synchrophasor is the "peak" of the fundamental value—scaled to RMS by dividing the magnitude of the fundamental signal peak magnitude by $\sqrt{2}$.

As the concept of the Synchrophasor gained traction in the power industry, standards on how to measure and report the Synchrophasor were developed. The active standard is now a dual logo standard: IEEE/IEC 60255-118-1-2018 [1]. Of note in this standard are the definitions of criteria that the Synchrophasor calculation must meet as well as standard reporting rates for Synchrophasors computed on both 50 and 60 Hz power systems.

It is worth emphasising that the magnitude and angle of only the fundamental frequency component are to be reported. The measurement technique must filter out the effects of Harmonics and Interfering Signals (noise) around the fundamental frequency.

Additionally, the standard defines criteria for the response of a measurement to harmonics, and to magnitude and frequency step and ramp input signals.

At the time the Synchrophasor was identified, there was not a viable time source to provide the accurate time synchronisation needed around the grid. It is to be observed that a one millisecond time error on a 50 Hz power system results in

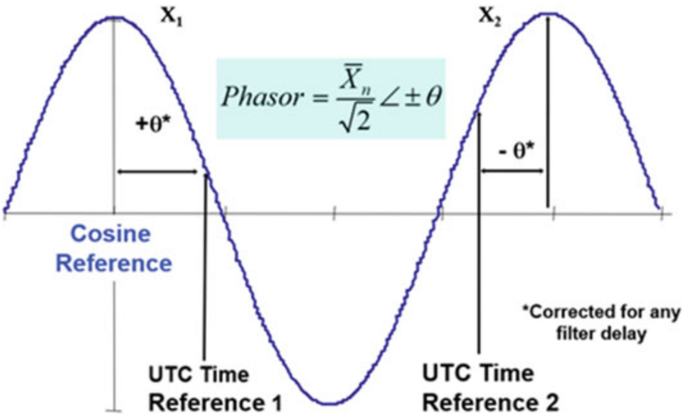

X1
X2
$Phasor = \frac{\overline{X}_n}{\sqrt{2}}\angle \pm\theta$
+θ*
- θ*
Cosine Reference
UTC Time Reference 1
UTC Time Reference 2
*Corrected for any filter delay

Fig. 13.1 Synchrophasor measurement definition (*Source* [7])

an 18° phase angle error in the calculation of the phasor (a function of the power system frequency). Around the late 1970s, the US government was developing a satellite-based time synchronisation system known as Navstar Global Positioning System or GPS. This system of satellites was designed to provide sub-microsecond time synchronisation to terrestrial-based receivers. The GPS system has a compliment 24 active satellites in six orbital planes as well as 6 spare satellites, one in each plane, that can be moved into position as needed. This design provides high availability for GPS timing signals. Similar satellite-based time systems have subsequently been developed by Russia (GLONASS), China (BeiDou or North Star) and the European Union (Galileo). In general, various clocks or time sources are referred to as a Global Navigation Satellite System (GNSS) clocks.

Although a time accuracy is not specified in the standard, a maximum error for the Synchrophasor measurement, known as the Total Vector Error (TVE), which includes measurement error, is specified to be less than 1%. TVE is defined as:

$$\mathrm{TVE} = \frac{|X_{\mathrm{ideal}} - X_{\mathrm{actual}}|}{|X_{\mathrm{ideal}}|} \quad (13.2)$$

This equation can be visualised in Fig. 13.2 which shows vectors from the Ideal Synchrophasor (typically created from an equation), the vector emitted from the PMU and the difference vector between them. TVE is the ratio of the magnitude of the difference vector ($V_{\mathrm{ideal}} - V_{\mathrm{Measured}}$) and the magnitude of the Ideal Synchrophasor.

The device that produces Synchrophasors has been termed a Phasor Measurement Unit or PMU. There are no design restrictions on a PMU as it may compute Synchrophasors for a single line or an entire substation.

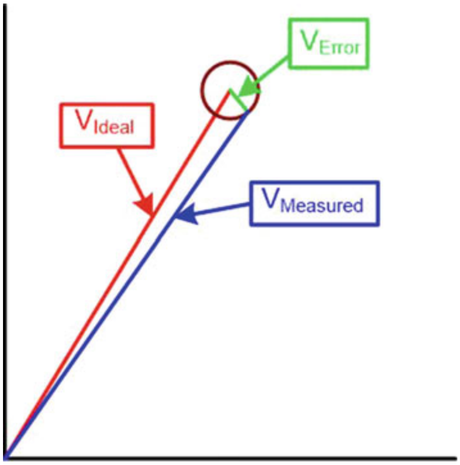


Fig. 13.2 TVE concept (*Source* [7])

13.2 Synchrophasor Calculation Window

Computation of a Synchrophasor involves integrating multiple samples of data to compute the value. By varying the size of the window of integration and associated filters, the resultant Synchrophasor changes characteristics. There are two primary integration classes identified in the standard (others are not precluded), namely P or Protection Class Synchrophasors and M or Measurement class Synchrophasor. The integration window for a P-Class Synchrophasor is always 2 cycles long and is typically filtered with a triangular filter. As such, the latency in emitting a P-Class Synchrophasor is only slightly greater than the period of one cycle of the fundamental frequency for any reporting rate. Based on its low-latency emission rate, it was given the name of protection or P-Class Synchrophasors. Note that the Synchrophasor measurement is time stamped in the middle of the integration window.

The second defined Synchrophasor class is labelled a measurement or M-Class Synchrophasor. This class requires the elimination of “interfering frequencies” around the fundamental frequency. Implementation of this function requires a Band Pass filter centered around the fundamental frequency be applied to the input signal. The Integration Window of the Band Pass filter is a function of the reporting rate of the M-Class Synchrophasor. For example, for a reporting rate of 50/60 measurements per second, the required integration window size is about 9 cycles. For slower reporting rates (e.g. 10 measurements per second), the integration window is on the order of 55–65 cycles (on 50/60 Hz systems, respectively). In as much as the emission rate is a function of the integration window, an M-Class Synchrophasor will have about a 4.5 cycle delay in emission at a 50/60 Hz output rate and up to a 33 cycle delay at a 10 Hz reporting rate on a 60 Hz system.

The reporting rate has an effect on the information provided by the Synchrophasor. A P-Class Synchrophasor will measure fault voltage and current when breaker clearing times are 3 cycles or greater. An M-Class Synchrophasor will "average" voltages and currents over the window resulting from the setting of its reporting rate. The larger window size will not show fault voltages and currents (unless the fault/system condition remains stable for a period of time relating to the reporting rate).

The emission rate can typically be set at 12, 15, 20, 30, 60 and 120 measurements per second on a 60 Hz system and 10, 25, 50 and 100 emissions per second on a 50 Hz power systems. It should be noted that the specified rates are integer dividers of the primary frequency as well as integer multiples of the fundamental frequency for rates greater than the fundamental frequency (e.g. 100). The PMU is to specify its supported emission rates.

The IEEE/IEC Synchrophasor Standard ([1]) defines the ability to transmit Synchrophasors in either Integer16 or Float32 format. In the IEC 61850 R-SV profile, the Common Data Class (CDC) or data format for Complex Measured Values (CMV) only supports Float32. Additionally, the Complex Measured Value Common Data Class only reports data in magnitude and angle (in degrees) format. A unique facet of R-SV is the ability to send multiple datasets in a single message. As such, it is an option to send the present Synchrophasor dataset as well as 1 or 2 or 3 "older" datasets to make up for missing samples.

Another aspect of Synchrophasor performance is its response to off-nominal frequency. Given a "perfect" fundamental frequency input to a Synchrophasor calculation algorithm, the output will be a fixed magnitude and phase angle. As the power system seldom operates at the same frequency, the Synchrophasor responds to off-nominal frequency by changing the phase angle of the output phasor. This can be seen in Fig. 13.3 where an off-nominal frequency signal less than the fundamental frequency is shown. The calculation windows—which are fixed by a GNSS clock—shows different views of the input signal and correspondingly different phase angles (Fig. 13.3).

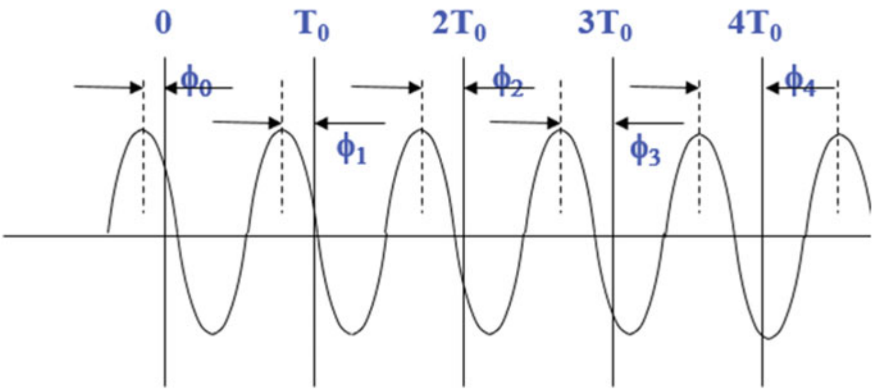


Fig. 13.3 Off-nominal frequency synchrophasor computation window (*Source* [7])

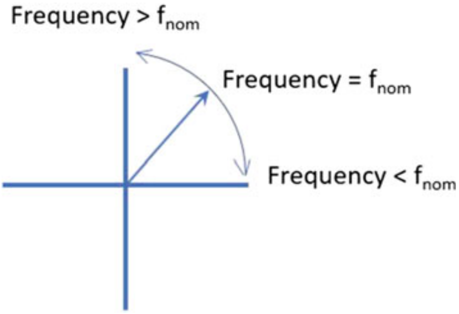

Frequency > f_{nom}
Frequency = f_{nom}
Frequency < f_{nom}

Fig. 13.4 Synchrophasor rotation for off-nominal frequency (*Source* [7])

The sample points (0, T_0, $2T_0$, $3T_0$, $5T_0$) are based on absolute time where T_0 is the period of the fundamental frequency of the monitored system. The frequency of the example waveform in Fig. 13.3 is less than nominal frequency. What is to be noted is that the phase angles (φ_0, φ_1, φ_2, φ_3, φ_4) are increasing with each sampling period, T_x. Plotting the phase angles on a complex plane, it can be seen in Fig. 13.4 that the phase angles are increasing in angle. When potted on a polar plane, frequencies less than the fundamental can be seen to be rotating in a clockwise direction. For frequencies greater than the nominal frequency, the Synchrophasor will rotate in the counterclockwise direction.

13.3 Synchrophasor Communication

When Synchrophasors were first brought to field trials, the primary communication technology in the utility industry was serial data via a RS-232 interface. Most specifically, the first communication link was a 4800 bit/sec analogue modem. To optimise the data that could be sent serially, a communication profile was developed that contained only binary data. A set of communication frames were developed to:

- Define the configuration of the data being sent
- Send Synchrophasor data
- Define a header frame format
- Define a control frame format

The data frame contained the following information:

- Sync Word—containing a Sync byte (AA hex), version #, Frame Type (config, data, Hdr, Cmd)
- Number of bytes in the frame (Max of 65,535)
- Device Identification Code (IDCode—Max of 65,535 devices in the original definition)
- Second of century—time stamp in seconds of the Synchrophasor

- Fraction of second with 59.6 ns resolution
- Status flag
- Phasors
- Frequency
- Rate of change of frequency
- Additional analogue values
- Digital status values.

As Ethernet became more main stream, this packet format was mapped onto either a TCP/IP or UDP/IP stack (setting option) which is codified in IEEE C37.118-2 [2]. Most implementations are configured to use the Ethernet/IP/TCP implementation.

13.4 IEC 61850 Routable Sample Values and Routable GOOSE

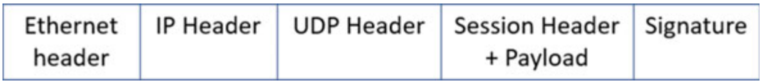
In the 2008–2010 time frame, use cases were identified by an IEC/IEEE Task force for the Network Multicast of both GOOSE and Sampled Values messages. Multicast is the concept of sending a message from one device to many other devices. In the development of this profile, the goal was to send the data over a wide area network. The sender and associated listeners are part of a Multicast Group. By design, there is no limit as to the number of devices that can be part of a Multicast Group. Other drivers for this development were that the communication format of the IEEE C37.118 standard was not compatible with IEC 61850 and that the C37.118 standard did not address Multicast Interoperability nor security. To address these needs, a report (TR 90-5—now deprecated and the content part of IEC 61850 Ed. 2.1—February 2020) was created which defined routable profiles for SV and GOOSE and was entitled:

Communication networks and systems for power utility automation Part 90-5: Use of IEC 61850 to transmit Synchrophasor information according to IEEE C37.118

The two primary use cases that drove the development were:

- Secure Synchrophasor Transmission
- Secure Wide area Remedial Action and Control

In the use-case development, it was observed that Synchrophasors are emitted on a periodic basis. The periodic emission was similar to that of Sampled Values. As such, the Routable Sampled Values profile is based on the IEC 61850 Sampled Values model of periodic data transmission. It was also noted that multicast routing capability could be added to the GOOSE message with the obvious difference being that the Routable GOOSE or R-GOOSE is launched on Data Change or periodically as a keep-alive. The routable piece is created by adding a UDP Multicast IP header to the message as shown in Fig. 13.5. Additional data fields have



Ethernet header	IP Header	UDP Header	Session Header + Payload	Signature

Fig. 13.5 UDP/IP header for R-SV and R-GOOSE (*Source* [7])

been added to the message to address security through authentication and optional encryption. Security details are presented in chapter 6.

Creating the path for R-GOOSE or R-SV from the publisher to the subscribers is performed using two different protocols.

A device wishing to join a Multicast Group issues a "JOIN" request via the Source-Specific Multicast (SSM) profile of the Internet Gateway Management Protocol (IGMP—specifically version 3). A subscriber for information from a Publisher sends out an IGMPv3 SSM <<JOIN>> request that contains the multicast destination address of the publisher and its source address. This request is designed to route ONE Hop to the router connected to the requesting host device. The router receiving this <<JOIN>> request proceeds to search for the requested destination and source address using a special Routing Protocol known as Protocol-Independent Multicast or PIM (see Fig. 13.6). PIM is "routing protocol independent" as it does not create its own routing tables but rather uses the existing routing tables from whatever routing protocol is in use to find the requested Publisher. Note that with SSM, the path between the source and the receivers is established from the receiver end of the path. In ver3, the user may require SSM in the group establishment. When PIM finds the requested source (group) and destination addresses, the path is remembered by the routers in the route which is then used to forward any multicast messages issued by the publisher to the requesting host(s).

It is to be noted that not all routing network equipment support IGMPv3 and PIM. In this case, the use of IGMPv2 and Unicast Addressing may be needed so an implementation should be able to support non-source-specific multicast. Unicast support is not specified in the standard but could be implemented by a vendor.

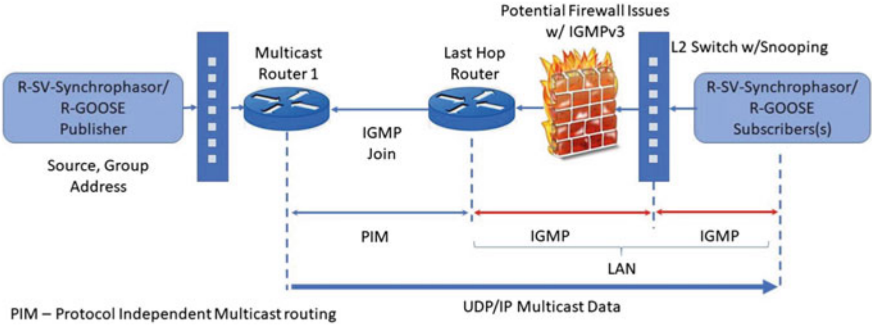


Fig. 13.6 Establishment of a multicast path (*Source* [7])

Another feature of IGMP is the Keep-Alive messaging. Periodically, the router closest to the requesting device will send a message to the host which asks the question to the host: “Are you still there?” If a response is not received, the Multicast path is removed. In IPv4, the overall Destination Multicast IP address range is from 224.0.0.0 to 239.255.255.255. When using IGMPv3 requiring a Source-Specific Multicast address, the address range of 232.0.0.0 to 232.255.255.255 has been allocated.

13.4.1 Session Header

Information about the message is found in the Session Header. The same Session Header is used for both R-GOOSE and R-SV. Specifically, the Session Header identifies:

- Session Identifier which includes Message type (R-GOOSE, R-SV, Management)
- Session Header Information which includes
  - # of bytes in the Session Header
  - Header Length
  - Session Number
  - Version Number
- Security Information
  - Time of current key
  - Time until next key
  - Key Identifier
  - Initialisation Vector
- Payload Information
- Signature

More details on the packet structure can be found in chapter 6.

13.4.2 Synchro Logical Nodes

In IEC 61850, Synchrophasors are special measurements that are contained in Logical Nodes (LNs). The Logical Nodes that would typically be involved in a Synchrophasor report are MMXU (Phase Voltage and Current Measurements) and MMSQ (Sequence Components). To identify that a LN is a Synchro LN, there are additional data attributed in the Common Logical Node for that LN that must be configured to aid in the identification and operation process. Of note, the Class of the Synchrophasor (protection (P) or measurement (M)) and the emission rate must be set. This information is located in an extension to the ClcMth data attribute (DA) which now allows the values of:

- P-CLASS—for Protection Class Synchrophasor emission
- M-CLASS—for Measurement Class Synchrophasor emission

The DA Calculation Mode (ClcMod) is to be set to PERIOD indication that the calculation is to be performed in a periodical time cycle.

The DA Calculation Interval Type (ClcIntvTyp) for Synchrophasors would be set to either CYCLE or PER-CYCLE.

The DA Calculation Interval Period (ClcIntvPer) is related to a multiple of the ClcIntvTyp. For example, for a report rate of 30 Synchrophasors per second, the ClcIntvTyp would be set to CYCLE and the ClcIntvPer would be set to 2. For a rate of 120 Synchrophasors per second, the ClcIntvTyp would be set to PER-CYCLE and the ClcIntvPer would also be 2.

It is recommended that the last letter of the LN prefix be set to either P or M to indicate the Synchrophasor class being emitted from that LN.

13.4.3 Synchrophasor Time Stamp

All Synchrophasors messages are Time Stamped using a Universal Time Coordinated (UTC)-based value. The Time Stamp is composed of 64 bits of information. For both Synchrophasors and IEC 61850 events, the first 32 bits are decoded as an Unsigned Integer and contain the number of seconds since 1 January 1970. This Start time is referred to as an Epoch (the start of time) for this time scale. Leap Seconds are not included in this count so the number of seconds in a year are clearly defined. Note: Leap DAY (February 29) is included in the count for a Leap Year and is included in the 4-byte Seconds count. Since a 4-byte Unsigned Integer can count up to 4,294,967,295 s and as there are 44,676,000 seconds in a year, a simple calculation shows that this count can identify a second of time for up to 136 years or until the year 2106.

The next 24 bits identify the Fraction of Second of the reported value. The Fraction of Second divides a Second into 16,777,216 counts or 59.60 ns per count.

The last 8 bits of the Time Stamp identifies the Quality of the Time Stamp. For example, if the Satellite Clock has lost visibility to any satellites due to positioning of the antenna or an antenna failure, the local oscillator may begin to drift. A worst-case drift can be estimated based on the Stability of the oscillator in the clock. For example, a simple Crystal oscillator is typically accurate to 1μsec over 4 hours after loss of satellite sync. This information is reported with the Synchrophasor as the estimated drift error and can be used to identify the "accuracy" of the computed Synchrophasor. A Clock Drift error results in a Phase Angle shift in the Synchrophasor. For example, a 1μsec error on a 50 Hz system results in a 0.018° error in the measured angle, whereas a 1 ms error in timing results in an 18° angle error. It is to be noted that the definition of the Time Quality byte differs between the Synchrophasor Time Stamp and the IED 61850 Time Stamp.

13.5 Applications: R-GOOSE

13.5.1 Remedial Action

All equipment on a power system is protected from short circuits through protection systems; however, there is increasingly a second level of protection that is based on the performance of the entire power system. This secondary protection is known as System Integrity Protection Schemes (SIPS) and is often referred to as a Remedial Action Scheme or RAS. SIPS looks at complex system situations where planning studies have shown that certain combinations of events and circumstances may result in a larger system collapse. SIPS can cover the entire grid or be focussed in a region. SIPS may have stringent performance requirements for execution in the 20–50 ms time frame, and all SIPS today have security requirements. A SIPS can be a stand-alone system for one particular system contingency though many SIPS today are “centralised” where system operating conditions and resulting controls may be shared by multiple schemes. This “sharing” of system information and control leads to the “centralised” architecture shown in Fig. 13.7. In this architecture, the elements can be classified as:

- Measurement and Monitoring
- Logic Processing
- Mitigation/Control.

These elements then need to be connected via a high-speed/redundant communication system. Communication profiles such as the Synchronous Optical NETwork (SONET)/Synchronous Digital Hierarchy (SDH), Redundant Ethernet, and Multi-Protocol Label Switching (MPLS) have been used for this purpose. What has been

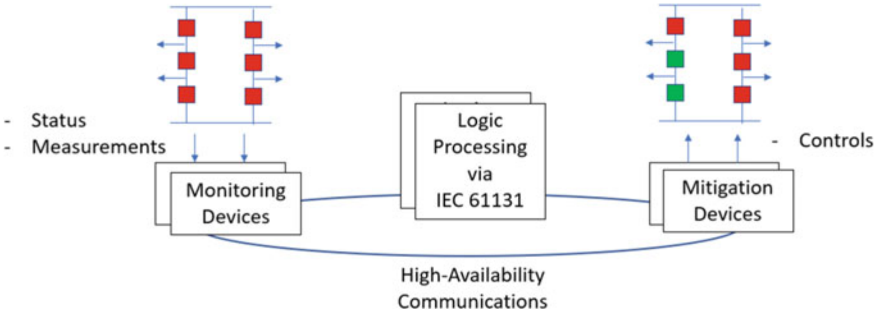


Fig. 13.7 Centralised remedial action architecture (*Source* [7])

found to be an efficient and high-performance transport mechanism for this functionality is the IEC 61850 Routable GOOSE. As a Multicast profile, one message can be sent from one location to multiple receivers. Transmission on Change of a Substation Event (Digital or Analogue value) results in low-latency communication, and the ability to Authenticate and Encrypt the message meets security requirements. Another unique feature of R-GOOSE is the ability to perform configuration of the system through the use of device IEC 61850 Configured IED Description - CID files.

13.5.2 Multi-Terminal Transfer Trip

The function of Transfer Tripping is one of communicating a Trip message from one terminal on the power system to one or more other terminals. Typically, this function is invoked when one terminal identifies a fault or situation where one or more other terminals surrounding the event also need to be taken out of service. One example of this is when, on a distribution feeder, a fault at a certain location cannot be "seen" at the head end of the distribution feeder. A present solution is to install a Ground Switch at the sub-distribution terminals that places a fault on the high side of the transformer—which can then be seen by primary protection at the head end. An example of this is shown in Fig. 13.8 where a fault in and around the distribution transformer cannot be detected by the protection at the 69 kV breaker.

The Routable GOOSE now provides a solution to this problem. Upon detection of a fault in or after the distribution transformer, a "secure" Transfer Trip message can be sent via a multicast message to all other participating terminals to effect

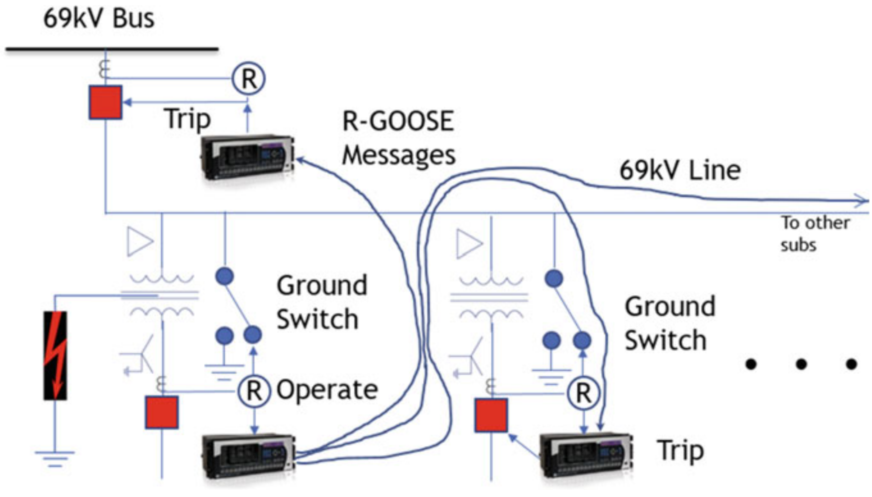


Fig. 13.8 Multicast transfer trip (*Source* [7])

a remote trip. This solution is significantly faster than a ground switch and less stressful to the grid.

13.5.3 Demand Side Management

Demand Side Management (DSM) is the concept of managing load on the grid by dynamically adjusting the price of electricity. It has been shown that electricity has a price elasticity [3] meaning that as the price of electricity increases, in an automated system with an override option, people will generally use less electricity. There are many loads whose disconnection will have no short-term effect on daily living (e.g. electric heat/air conditioning, hot water, dryer, dishwasher). Additionally, there is a need today to balance load in conjunction with changing generation from intermittent renewable resources. The challenge with implementation of this function is being able to securely reach millions of metres over a wide area in a short period of time with new pricing information. Radio is being used for load shed, but this is a one-way methodology. Packet-based systems have also been deployed, but these systems have significant time delays. Time delay is an issue when the same infrastructure is used for Direct Load Control (see Sect. 13.5.4). Additional controls would be required at the home with the ability to communicate with house load and effect the Demand Response. The IEC 61850 R-GOOSE profile provides an ideal solution for these requirements. The multicast capability of R-GOOSE can securely and quickly reach millions of homes. Devices in the home could be adapted to acknowledge acceptance of the new pricing as well as activation time (or denial) of the pricing request. Use of an International Standard facilitates Interoperability. R-GOOSE can be multicast over unlicensed or licensed radio and achieve secure wide area coverage with low latency (20–30 ms).

13.5.4 Direct Load Control/Surgical Load Shed

When an abnormal condition occurs on the grid (e.g. loss of large generation, loss of transmission), a “remedial action” may be needed to maintain grid stability. In Sect. 13.6.1, remedial action typically requires the rapid detection of conditions and mitigation (50 ms) of large blocks of load or generation to maintain stability. The shedding of large blocks of load is disruptive and can present societal dangers such as loss of traffic signal control and medical emergencies such as loss of home ventilator power. As noted in Sect. 13.5.3, there are many household loads that can be disconnected without disruption to home life and still effect significant load shed. The ability of R-GOOSE to multicast to millions of homes in 10s of milliseconds enables it to rapidly execute Direct Load Control (or better identified as Surgical Load Shed) as part of a Remedial Action Scheme. Existing radio technology can cover a 45 km radius (terrain dependent) with a multicast message. Since the message is authenticated and optionally encrypted, existing home Internet connections can also be advantaged. This link can be bi-directional, and each meter can report the result of the requested action. The same link could also be used to re-instate load or to rotate shed load in a region. It is anticipated that price incentives would be offered by the utility for homeowner participation.

13.5.5 Transactional Energy

Energy supply on the grid is in the process of evolving from a "numbered" set of large/larger generating plants to millions of Distributed Energy Resources (DER). Today, energy prices are set in a commodity setting where electricity is bought and sold between the relatively few large generators and energy consumers in a bidding market. Transactional Energy envisions millions of DER generators looking to sell energy to energy consumers. This process will require that the DER producers reach out to many potential energy consumers with their ask price for electricity. This is clearly a Multicast situation and, once again, R-GOOSE, when connected to appropriate management software, can provide a solution.

13.6 Applications: R-SV

13.6.1 State Estimation through Multicast Synchrophasor Delivery

The state of the power system is defined as the Positive Sequence Voltage and Phase Angle at an instant in time at substations throughout a system. Since SCADA cannot make precision time-synchronised measurements, the state of the system was "estimated" through a software tool known as a State Estimator or SE. Traditional SE tools were designed to solve for the system state (Positive Sequence voltage and angle at each bus) using non time-aligned Watt and Var measurements from substations throughout the system.

Today, there are two variants of the State Estimation process that incorporate Synchrophasors in the calculation. The first variant is the Phasor Assisted State Estimator which uses several Synchrophasor measurements from around the grid as "anchor points" in the SE solution. These measurements improve the accuracy of the overall SE output. A second technology being used is known as a Linear State Estimator where the state of the system is directly computed from PMU measurements around the grid. Although the Synchrophasors provide the direct measurement of the state, a PMU may provide bad data. A mathematical formulation has been developed to detect and adjust the calculation for bad measurements. The resultant computation is a direct matrix multiplication and does not require any iteration. Implemented systems update the calculation at up to 30 times per second.

All utilities have redundant control centres and, as such, control centres using Synchrophasor-enhanced SE tools requires Synchrophasor data. With the IEC 61850 R-SV Multicast profile, a single PMU can send Synchrophasor data to two or more locations simultaneously. More specifically, since the R-SV message can be authenticated and encrypted, transmission of Synchrophasor data from one control centre to multiple other control centres can safely be accomplished. As noted above, the Payload of the R-SV message is about 65,000 bytes of data. Given this larger message size, entire system states can be shared among control centres and system operators.

13.6.2 Frequency Network—FNet

The electric power grid with its rotating machines and stored energy elements such as inductors, capacitors and long lines has an electro-mechanical response to power system events. One way that this response is manifest is in how the frequency around the grid changes in response to a disturbance. Frequency does not change instantaneously but, as shown in the water ripple example, takes time to propagate through the power grid. This response can be visualised through the analogy of throwing a rock into a pond. The rock makes a big indentation at the entry location but also emits ripples or travelling waves of water—emanating from the point of the disturbance (see Fig. 13.9). The frequency and speed of the ripple wave are a function of the viscosity of the liquid through which the waves are travelling.

The same phenomenon occurs on the power system when a disturbance results in either a change in power level or system configuration. By monitoring the "instantaneous frequency" at points throughout the grid, an image of the frequency ripple resulting from a disturbance can be visualised (See FNET Server page—[4]). Frequency information can be included in the R-SV Multicast Synchrophasor package (inclusion of frequency is mandatory in the IEEE C37.118.2 standard) and can provide the necessary frequency values. Additionally, IEC 61850 defines models for latitude, longitude and altitude which would be included in the CID file and could also be mapped into the message. Periodic multicast messages could reliably

Fig. 13.9 Frequency wave visualisation (*Source* [7])

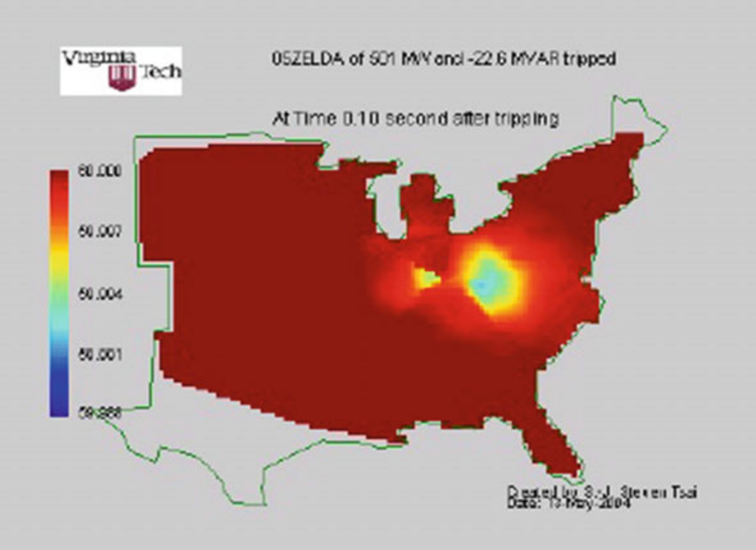

Virginia Tech
05ZELDA of 501 MW and -22.6 MVAR tripped
At Time 0.10 second after tripping
60.000
60.007
60.004
60.001
59.998
Created by S.-J. Steven Tsai
Date: 13-May-2004

Fig. 13.10 Change in frequency at time t0 (*Source* UTK [4])

be sent to multiple operator stations and system operators. Figures 13.10 and 13.11 show, through changing colours, an actual frequency event and how the frequency changes over time.

Analysis of frequency change over a power system has identified two significant characteristics of this phenomenon:

1. The speed of the frequency ripple: Measurements on the East Coast of the US carriage return have shown that the frequency wave travels at 560 km/sec on the East Coast of the US and 1760 km/sec on the West Coast of the US carriage return.
2. <CR> A relationship between the change in frequency and the amount of generation lost was identified:
3. <cr> The Rate of Change of Frequency often abbreviated as ROCOF, this value is the first derivative of frequency and, as such, is an early indicator of a system disturbance. As a derivative, the output can be noisy so some filtering is often advised.

13.6.3 Synchrophasor-Based Fault Location

In the beginning of the introduction of Digital Relays, most relays performed Fault Location based on measurements from one end of a line. These Fault Location measurements contained location errors due to fault impedance and differences in

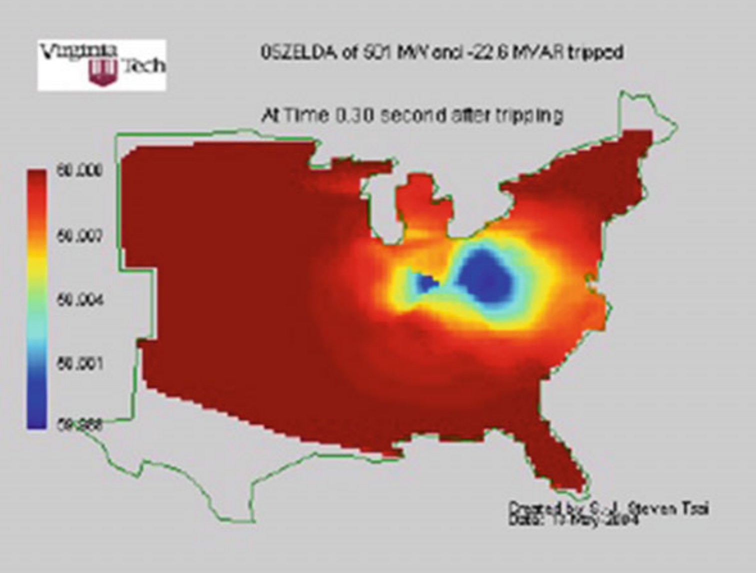

Virginia Tech
05ZELDA of 501 MW and -22.6 MVAR tripped
At Time 0.30 second after tripping
60.010
60.007
60.004
60.001
59.998
Created by S.-J. Steven Tsai
Date: 19 May 2004

Fig. 13.11 Change in frequency at time t1 (*Source* UTK [4])

the Voltage Phase angle between the ends of a line. The use of Synchrophasors in Fault Location eliminates these errors as the Voltage Source angles are now precisely known which enables the elimination of errors from Fault Resistance. A Line Fault can be modelled via a Positive Sequence/Clarke Component model [5] as shown in Fig. 13.12 where all measured values are Synchrophasors. Note that the Synchrophasor Report Rate needs to be sufficiently high (60 or 120 measurements/sec) on a 60 Hz system - similar on a 50 Hz system and/or the clearing time of the fault must be long enough to capture stable fault data.

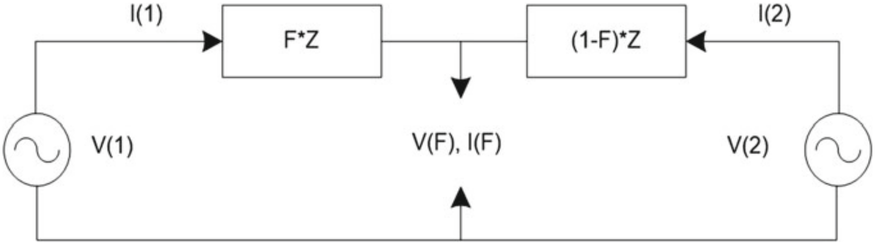


Fig. 13.12 Double-ended fault location model (*Source* [7])

Given Synchrophasor data (either Sequence or Modified Clark Components), the location to the fault can be found from the equation:

$$F = \mathrm{Real}\left[\frac{\frac{V(1)-V(2)}{Z}+I(2)}{I(1)+I(2)}\right] \tag{13.3}$$

13.6.4 Broken Wire Detection

When a phase wire breaks, the voltage will show a step change of the voltage phasor on either side of the break. One such application is on distribution feeders with multiple branches (Patented—[6]). The PMUs are installed at the source end of distribution line and tap points which would be implemented on the feeder. Data from the mounting locations can be streamed via R-SV to a central computation location (typically the substation) or, if the PMU contains computational capability—analysis at each PMU is possible. Figures 13.13 and 13.14 show relative change in phase angle and/or magnitude of the Voltage Synchrophasor before and after the line break. For intermediate line locations, Line Post Insulators can be used to input low-voltage signals into a PMU.

Broken wires on transmission (typically not an issue) and sub-transmission lines can also be detected in this manner but using impedance instead of voltage.

Fig. 13.13 Phase angles before line break (*Source* [6])

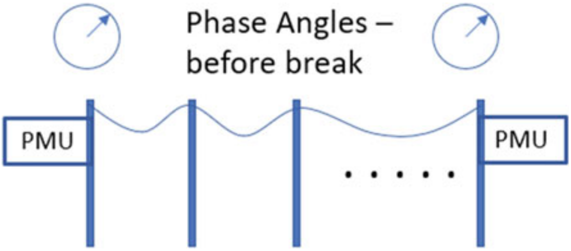
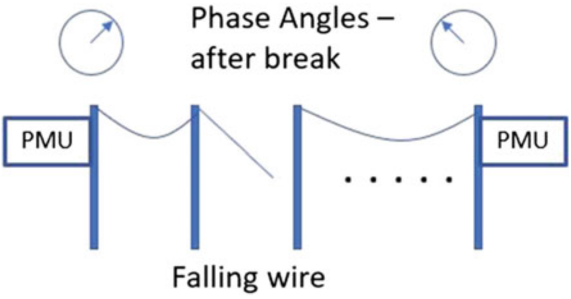


Fig. 13.14 Phase angles after line break (*Source* [6])



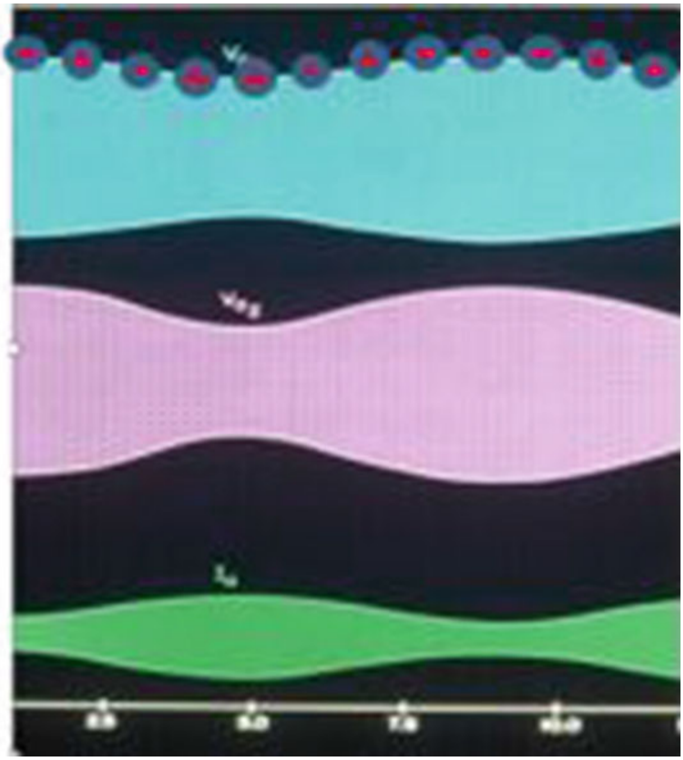


Fig. 13.15 Synchrophasor-based oscillation monitoring (*Source* [7])

13.6.5 Oscillation Monitoring

The evolving power system has not only a strong electro electro-mechanical make-up but is now developing a significant electronic controls component—both of which can result in voltage, current and, subsequently, power oscillations. In addition, events such as Coronal Mass Ejections (solar flares) can result in Geo-Magnetic Disturbances (GMD) and the ensuing low-frequency oscillations. These oscillations manifest themselves as modulations of the fundamental frequency, Fig. 13.15, which are outlined by magnitudes of the associated Synchrophasors.

A harmonic analysis of the Synchrophasor magnitudes can extract the oscillation magnitude and frequency. Note that there is a Nyquist component in this process as the highest frequency oscillation extractable is a function of the Synchrophasor emission rate. For example, a Synchrophasor frame rate of 60 measurements per second, per the Nyquist sampling theorem, can extract at most a 29 Hz oscillation. Monitoring of higher-order oscillations, such as those resulting from Sub-Synchronous Resonance (SSR), require much higher sample frequencies (e.g. 64 samples per cycle) to analyse.

References

1. IEEE/IEC 60255-118 Synchrophasor for power systems Measurements. https://webstore.iec.ch/publication/28722
2. IEEE C37.118-2 IEEE Standard for Synchrophasor Data Transfer for Power Systems. https://ieeexplore.ieee.org/document/6111222
3. Results of USA's Largest VSP (Variable Spot Pricing) Program at American Electric Power; P. Spaduzzi, M. Coleman; DA/DSM '92; Fort Lauderdale, FL; January 13–15, 1992
4. FNet Server Web Display: fnetpublic.utk.edu
5. Double-Ended Distance-to-Fault Location System Using Synchronized Positive or Negative Sequence Quantities; Steven Turner; US Patent 6,879,917; April 12, 2005
6. System for Detecting a Falling Electric Power Conductor and Related Methods; Patent US 9,413,56; Aug 9, 2016
7. Adamiak Consulting LLC, AdamiakConsulting@aol.com, Various training and marketing materials prepared since (2009)

IEC 61850 for SCADA Applications 14

Pablo Humeres Flores

Abstract

In a digital substation, the local SCADA system takes a fundamental role as a human–machine interface to guarantee the controllability of the installation. This chapter presents the aspects to be attended by the SCADA system when the protection, automation and control system is based on IEC 61850, involving the requirements and strategies for its implementation and maintenance. Aspects related to the SCADA system's function of providing information to remote operation and maintenance systems are also presented.

Keywords

SCADA system • IEC 61850 • HMI • Information

14.1 General Considerations

The control and supervision in an older type electric power substation were traditionally done through panels where there was a mimic of the single line with position lights, keys to operate commands and annunciators to show alarms. Mechanical flags signalled protective actuations.

The digitisation of the protection, automation and control systems had a profound impact on this interface, since it migrated to a computational environment with Screen Displays, Alarms, and Sequence of Events, in a graphic human–machine interface (HMI).

Supervisory systems, SCADA—Supervisory Control and Data Acquisition, are designed to perform control of the power system from control centers. Their role

P. Humeres Flores (✉)
CGT Eletrosul, Florianopolis, Brazil
e-mail: hpablo@cgteletrosul.gov.br

P. Bishop and N.-K. C. Nair (eds.), *IEC 61850 Principles and Applications to Electric Power Systems*, CIGRE Green Books, https://doi.org/10.1007/978-3-031-24567-1_14

was to supervise the system conditions (measurements and equipment status) and to control the primary equipment. SCADA is part of a set of software needed to control the power system in real time called Energy Management System—EMS that includes other functionalities.

The impact of adopting SCADA on substations was enormous. Operators accustomed to command by panels, keys and positional announcers had to get used to using a mouse, screens and an alarm list. Maintenance had to change its knowledge profile to understand computing, Ethernet networks and communication protocols.

With the consolidation of the IEC 61850 standard and the advancement of new technologies, the supervisory systems will be fully integrated with the protection and control system and these in turn integrated with the primary equipment or Stand-Alone Merging Units. The wired connections for commands, measurements and protection will be replaced by communication protocols on an Ethernet network.

An important impact of the digitalisation process of the substation is that we now have several services as a result of the information available. The main ones would be as follows:

- Greater visibility of the power system information, positively impacting the control, protection and supervision of the system.
- New functionalities such as application of PMU—Phasor Measurement Unit, allowing real-time visibility of the system phasors and thus creating possibilities for real-time analysis and improvement in the safety and stability assessment of the power system.
- TWFL application—Travelling Wave Fault Locator, for fault location and the possibility of new protection features.
- Monitoring of primary equipment, especially transformers, improving operational safety, maintenance management and evaluation of incidents.
- Monitoring and management of the entire infrastructure of the protection, automation and control system, allowing for improved availability and management of its maintenance.
- Asset management, as a consequence of the amount of information available, both of the primary and secondary equipment of the system.
- Availability of information for real-time analysis, such as event collection, DFR information—Digital Fault Recorder (COMTRADE files).

The strategy of managing this entire system data set can vary according to the vision of each company, its infrastructure and its systems. In this direction, we can have several concentrators in each installation collecting specific systems, or a single concentrator delivering the information for each system.

Figure 14.1 shows a typical application with several concentrators for each system.

In this case, each concentrator acquires its specific data and delivers it to the application system.

Figure 14.2 shows a solution with a single concentrator.

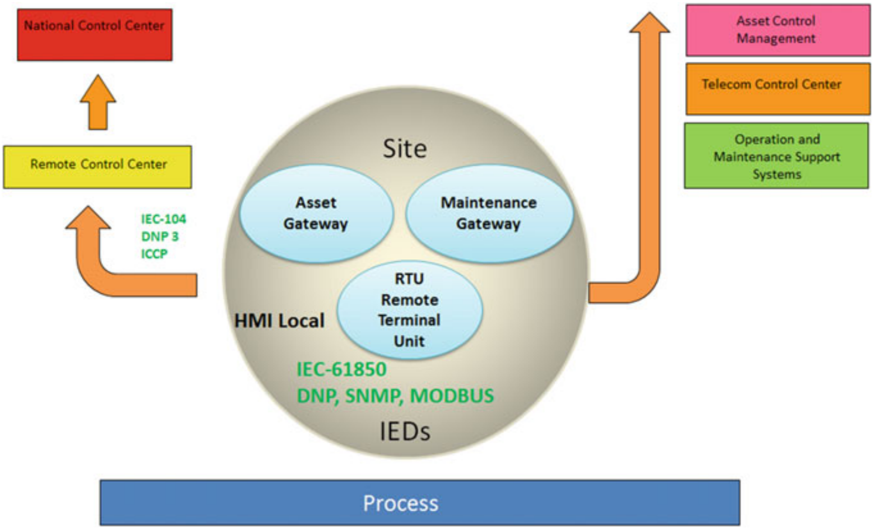


Fig. 14.1 Several concentrators for each system [1]

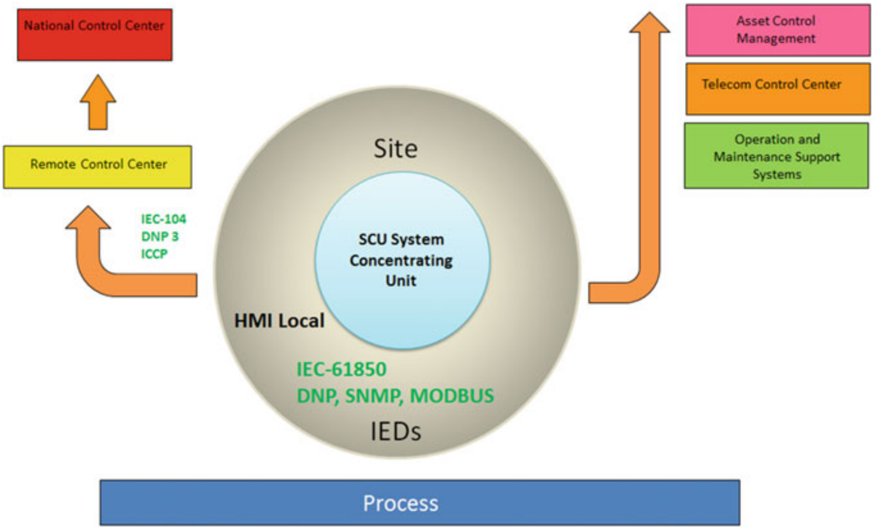


Fig. 14.2 Substation concentrating unit—SCU [1]

In this case, local SCADA collects all the data assuming the function of System Concentrating Unit—SCU, presenting only the operation data in the local HMI interface, and delivering the data to the remote systems with all the necessary information according to its specialty.

14.2 Local SCADA Implementation

In a substation, the first step is to define how data acquisition will happen and how to convert it into information. In a digital solution, the substations have a set of IEDs (protection relays, acquisition and control unit, multi-meters, equipment monitoring units, remote terminal unit), using an Ethernet infrastructure for local communication (switches, converters, terminal servers, routers) and a computational infrastructure (Substation Concentration Unit, HMI, monitoring and engineering computers).

The planning of the supervision system requires the use of a data structure (Data and Information Structure—DIS). It must meet all protection and automation, monitoring, diagnostics and support functions. Considering the use of IEC 61850 and the CIM (Common Information Model), DIS should reinforce the systematic approach that allows applications to interact and should facilitate functional implementation throughout all levels of the operational hierarchy. Figure 14.3 shows the hierarchy and relative requirements for data and information at each level. It also shows how data must be converted into information as it moves up the information hierarchy. It also shows that it involves generation, transmission and distribution centres (GCC, TCC, DCC) related to this (G, T and D). The ISO level (RCC, NCC) depends on the structure of each country.

DIS must meet the following requirements:

- Best cost–benefit ratio: transforming data into information only once at the lowest possible hierarchical level and at minimal cost,
- Consistency: using data or information only after validation and meeting the level of quality required for the specific application,
- Consistency: apply the same data or information for all functions, for exposure to the operator and for corporate dissemination,
- Redundancy: using an abundance of data for validation, according to a quality level ranking,

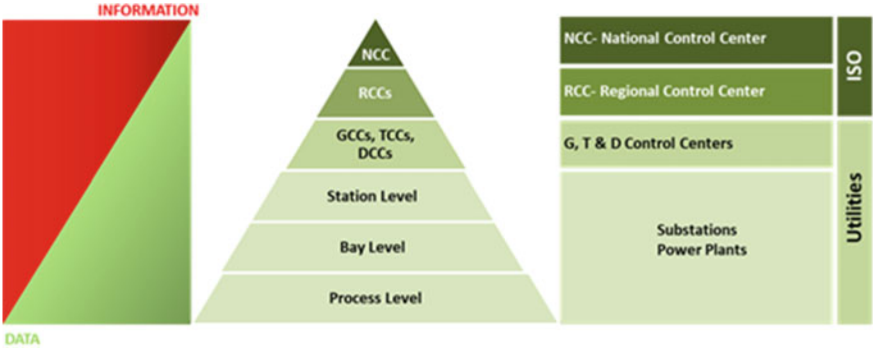


Fig. 14.3 Data and information requirements [1]

- Reliability: extension of the concepts of protection of reliability and security for all functions,
- Cybersecurity: meet the basic requirements specified for the Global Energy Management System of regional and national control centres,
- Sharing: use the same data or information for the owner of a single function (for example, component protection,) and for multi-owner functions (for example, system integrity protection schemes—SIPS),
- Scale: for each function and at each hierarchical level, use only the data necessary for the assignments of that system within each hierarchical level.

In the substation environment, we will always have a variety of communication protocols. The Substation Concentrating Unit—SCU must have the ability to interoperate with several protocols. It must also have the processing and intelligence capacity to convert the acquired data into information. Investing here means optimising data traffic and improving information quality. It is also possible with some resources to capture disturbance files and log files on DER and relays. From the SCU, it is also possible to popularise a database in some corporate standard, storing information to make available the management systems: support to the operation, maintenance and monitoring.

The configuration of SCADA is based on specific software. The steps to be able to carry out this implementation are as follows:

- Definition of the communication architecture,
- Definition of redundancy requirements,
- Definition of communication connections (IEDs) and protocols,
- Definition of the list of signs to be acquired,
- Treatment of signals within SCADA,
- Preparation of unifilar screens,
- Making of complementary screens,
- Definition of data history,
- Definition of database configuration,
- Definition of users and profiles,
- Definition of information to be passed on to other levels.

The resources to carry out these activities depend on each product, company, auxiliary tools and established standards.

14.3 SCADA and IEC 61850 Standard

In the implementation of the supervisory system, the objective is to optimise the process avoiding data that needs to be translated into real information and manual settings that depend on the designer's ability.

The best way to do this is to apply a data model, in order to have structured information. The IEC 61850 standard is exactly that, a model-based descriptive

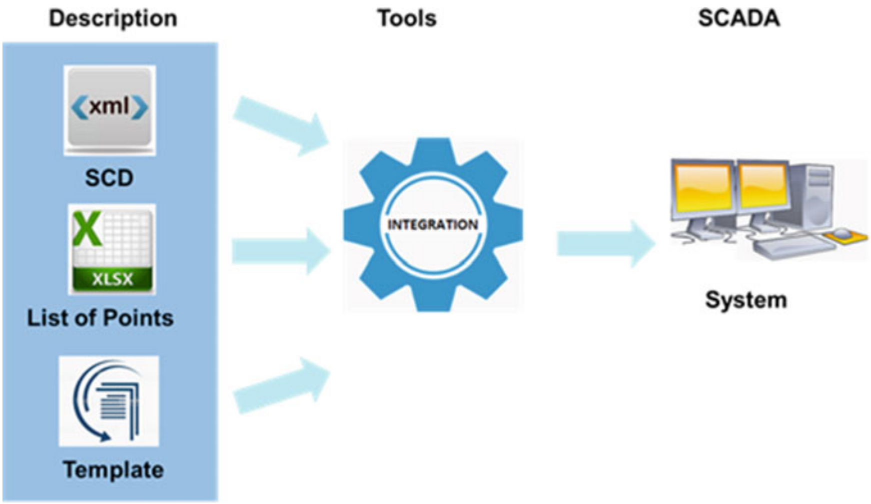


Fig. 14.4 Configuration process [2]

configuration, logical nodes, with definition of attributes and description of the communication and its infrastructure.

Therefore, the substation descriptive SCD file can be used as the base file to configure our SCADA system as illustrated in Fig. 14.4. It has all the necessary information from the IEDs to supervise the states, conditions and equipment measurements, in addition to their functional health.

In applying the SCD file, some aspects must be observed:

- The SCD file has much more information than is needed by the supervisory system,
- There are generic GGIO and GAPC objects originating from data that are not defined in the standard or were necessary to customise functionalities,
- The SCD nomenclature and description are not the one desired by SCADA users,
- The SCD does not define the level of severity of an information: critical, alarm, signalling and only historical record,
- The SCD does not define the treatment within the supervisory system: with what colour, source should it show or not in an alarm list and what level of sound should be associated with,
- The SCD does not define what information should or should not go to the Screen Display and how it should be presented (objects, texts, permanent or only when requested),
- SCD nomenclatures usually follow a project description, which does not correspond to the operational description, which may even change over time,

- The SCD file may not contain other connections from SCADA, with legacy systems, other non-IEC 61850 devices and exchange of local data with other systems/companies in other protocols.

So although the central role of the SCD file (Substation Configuration Description), it is not sufficient to configure and define the SCADA configuration.

Therefore, other sources of information must be considered. It can especially consider two other sources of information about the project.

List of Points: It uses a dictionary for the treatment and nomenclature of all signals, measures and commands that will define the SCADA database. It usually basically contains the following:

- Physical and logical information of the source of the signals,
- Protocol and address of each signal,
- Operational nomenclature,
- Identifier and description based on a standard company dictionary,
- Treatment definition: alarm level, displays where to display the information.

Template: In order to be able to generate SCADA screens, it needs the colour definitions, fonts, details of the substation line and other screens used (protection flags, communication, etc.). The way to be able to automatically generate these screens obviously depends on the SCADA software applied, but it is usually possible to generate the files automatically if the definition of typical bays exists:

- Function: Transmission Line, Transformer, Auxiliary Service, Busbar, etc.,
- Voltage level,
- Substation arrangement,
- Complementary information (detail boxes on the screen).

There are different resources to carry out this process. Newer generation SCADA systems are able to integrate these sources of description and generate the database and single-line drawings.

Currently, it is more common to use Virtual Basic for Applications—VBA tools, programming in the Excel spreadsheet, where we import the SCD file, we have the dictionary definition, and we interpret the project information to the operational and treatment descriptions. Depending on the SCADA, it is even possible to directly export the screens using templates typical of the company's application.

The form, however, is not the most important aspect, but taking advantage of being able to automate the configuration process. The main ones are as follows:

- Less implementation time to configure the entire SCADA system,
- Greater quality assurance and adherence to defined standards,
- Ease to make secure changes to the system,
- Documentation of all applied information,

- Pattern change management with reliability and the possibility to do it on a large scale without prejudice to the systems in operation.

14.4 SCADA Communication

The local communication SCADA is based on Manufacturing Message Specification—MMS and applies the project SCD to configure and apply communication connections. But considering current deployments, the local SCADA will sometimes have legacy communications, so it will have to be prepared to accord with IEC 61850 solutions and older systems.

Communication protocols have evolved over time, moving from protocols based on memory area scans, such as Modbus, to master slave with DNP 3.0 or IEC 101 in serial communication. The next step was protocols in Ethernet network over TCP/IP such as IEC 104 and DNP 3.0 itself. But the most significant change is in the application of MMS, because it is a protocol based on client server and request instructions.

The description of the Manufacturing Message Specification—MMS is detailed in chapter 4 in item 4.6.3 and the mechanisms involved in client–server communication.

The advantage in this case is especially that the IED makes its information available and the client, in this case SCADA, decides the information that is important to him. Then, if the information later changes, it will be enough to change the configuration of the client.

In addition, the MMS allows the acquisition of COMTRADE files, which means making the protection performance records available in real time. Strategies can be adopted so that these collections are made available immediately to protection operation teams to analyse events and to generate a historical database.

SCADA can also read health attributes in the logical node, which can be very important in the operation of real time to know the conditions and limitations of a protection, control or measurement function.

14.5 Management of SCADA System

In a digital substation, control options are becoming increasingly dependent on the local SCADA system. When SCADA is unavailable, options for control are usually very restricted and avoided as much as possible. In addition, they may require local control, which in most cases makes operation very difficult since the current practice is that most installations are remote controlled.

When applying an IEC 61850 solution based on MMS communication, the possibility of availability is greatly increased. This is because the devices support the connection of multiple clients, which means that if maintenance intervention is required, it is possible to maintain an active service, update one of the SCADA's redundancies, check its consistency and return in parallel with the service with a minimum of unavailability, or even without interrupting the service.

SCADA is naturally a system that undergoes many updates. They can be corrections, changes in the supervision of states or measurements, implantation of new bays and new functionalities. In addition, the computational infrastructure itself where it runs undergoes changes, corrections and substitutions throughout its life cycle.

Because of this characteristic of applying continuous updates, it is important to have an efficient backup management of the database and what should include all files involved in the functioning of the system.

Another important aspect is the possibility of maintaining a large volume of records, not only of the signals of the power system but of health of all functions, services and devices. In this sense, it is important to have management over these data so that they are in fact available to each team and at the right time. The information must be treated to assist in the analysis of system performance and preventive maintenance actions. The possibility of monitoring the protection, automation and control system in real time is a fundamental factor to guarantee the reliability of the power system.

14.6 Remote Systems

Remote systems can be focussed in three directions: operation centers, asset management centers and support centers.

The digitalisation process of the facilities allowed remote control in a safe way, as the solutions of the devices incorporated microprocessor technology and the Wide Area Network—WAN improved bandwidth and safer alternative routes.

Operation centres can perform diverse tasks depending on how a company's operating strategies are. They can carry out full control of a remote substation or power plant, either partially or only by coordinating the operation. The important issue is that the decision on how to carry out the operation is not limited by technology but only follows decisions on the efficiency of the operating processes.

The way of communicating the local SCADA with operation centers varies according to the practices of each company.

Communication using the DNP3 and IEC 60870-5-104 protocol is still very common and quite consolidated. But it implies converting information back into data defined by an address with no functional meaning. Therefore, it seems more adherent to an IEC 61850 solution to apply a data model communication.

The communication protocol that has this focus is the Inter-Control Centre Communications Protocol—ICCP, standard of IEC 60870-6/TASE.2 (Telecontrol Application Service Element 2). It makes use of MMS, in the same way as IEC 61850.

In this direction, we benefit from a data model protocol client server and work with sending information, not just data to higher levels.

Some SCADA systems allow configuring the ICCP server as a generic server. This means that it makes its entire database available to the client that connects to it. The advantage of this approach is that it is not necessary to configure which points will be made available for a particular client system, but it is he who decides which points are of interest to him. This reduces the possibility of errors in the configuration of the distribution and facilitates changes in the information desired by the operation center and the inclusion of new connections with little effort.

As already mentioned, the facilities have a high volume of condition data from the devices, services and Ethernet network. They pass this information on to asset management centers, which may or may not be integrated with the local SCADA itself or even the remote operation centre. They in turn will forward the data to the operation and maintenance teams, so as to be available at the appropriate time for the necessary team, the specific information for analysis and decision-making of operation, maintenance and life cycle of the systems. The final management systems are usually in the corporate environment of companies in order to make information access easier and safer, without access to real time where performance and cybersecurity aspects may be compromised. Chapter 15 presents the issue of maintenance and asset management for IEC 61850 systems, showing other aspects of the subject.

A very important change with all the technological advances was the support in real time. For this, the utilities of electric power have built specific WAN networks for these accesses, which allows a specialist in protection, automation, control and telecom to access any system and device and make checks and corrections especially in complex situations of system unavailability in real time.

When the solution in the installation is IEC 61850, this intervention gains special efficiency, because it allows remote accesses and tests without making services unavailable. Thus, the diagnosis can be much more efficient and the intervention for alterations much safer.

In the future, more intelligent support systems will be able to handle data and make decisions and guide actions much more efficiently. For this, it will be important to invest in Artificial Intelligence—AI, where the analysis time will be dramatically reduced and decision errors will be reduced.

14.7 Cybersecurity Aspects

In chapter 6, cybersecurity aspects were addressed in an IEC 61850 solution. What will stand out in this chapter is the importance of a global vision of cybersecurity, considering that the supervisory system integrates different local, remote and corporate systems.

Threats can be considered with respect to two sources: internal and external risks.

Internal threats are very worrying, as it means having someone who knows in detail, not only how the protection and automation system works, but also the most vulnerable access points that allow attack vectors. Therefore, cybersecurity must start internally, looking for incidents that may be caused, for example, by dissatisfied employees (or ex-employees), called insiders, who have access to the company network, or by human failures and errors in configuration and operation, caused mainly by excessive privileges and/or inadequate access (quite frequent). Cyber incidents are not always caused by targeted attacks, and internal incident situations can be avoided by applying good practices, appropriate security policies and appropriate technical actions.

Consideration should be given not only to utility employees, but to companies that provide IEC 61850 devices and systems, system integrators and consultants that support all aspects of the protection and automation design, testing and commissioning that normally need access from anywhere of the system.

External risks mean a higher level of security, when the intention is to protect against imminent threats and targeted attacks, requiring more stringent protection measures, the use of appropriate equipment and technologies and the application of restricted access controls. In addition, the training of the technical staff that operates and maintains the system is extremely important, as in most cases people are the weakest link in the chain and can be used as the first attack vector for manipulation and infiltration in companies, through a mechanism known as social engineering.

One of the important concepts in these strategies and presented in the IEC 62443 standard is that of Defence-in-Depth (DiD) as shown in Fig. 14.5.

The basic principle is not to rely on a single security measure to prevent intrusions. In this way, several layers of protection must be built, each one supporting the other layers. In this way, we increase the security of the system, and if the invasion occurs in a layer, we hinder the progress and gain time to detect the threat and take protective actions to react in time.

In addition to the direct care with the protection, automation and control system—PAC, it will be necessary to apply specific products and cybersecurity systems. The main ones are as follows:

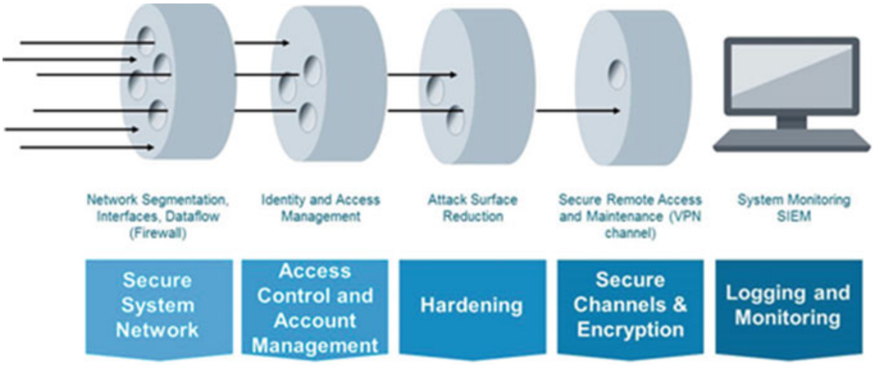

Network Segmentation, Interfaces, Dataflow (Firewall)
Identity and Access Management
Attack Surface Reduction
Secure Remote Access and Maintenance (VPN channel)
System Monitoring SIEM
Secure System Network
Access Control and Account Management
Hardening
Secure Channels & Encryption
Logging and Monitoring

Fig. 14.5 Defence-in-Depth (DiD) [2]

- **Remote Access (VPN)**: Remote access is a fundamental resource in the management of the systems of a digital substation. But it is important to apply a virtual private network (VPN) that guarantees secure and encrypted access, especially if the access comes from a public network infrastructure. For external remote accesses, it is important to consider mechanisms with multiple factor of authentication (two-factor authentication);
- **Firewalls**: It is a security solution based on hardware or software (most common) that, based on a set of rules or instructions, analyses network traffic to determine which data transmission or reception operations can be performed, blocking unauthorised ones;
- **Access Control and Account Management**: It means a centralised management system, to authenticate user accounts, to map user roles and to have management and rules at the time of execution;
- **Registration and Monitoring**: Perform the collection of equipment log and information monitoring. It means having a SysLog Server, a SysLog Agent and centralised management of security events with a SIEM—Security Information and Event Management, usually located in the SOC (Security Operation Centre);
- **Protection against malware**: Protection against malware requires software that acts in a way that can be categorised into two strategies:
  - Blacklisting (classic antivirus),
  - Whitelisting (application whitelist).
- **Hardening**: The hardening guarantees safe products and solutions, through safe configuration, reducing its attack surface. For example, this is achieved by removing unnecessary software, unnecessary usernames or logins, disabling unused ports and protocols or strengthening HW/OS;
- **Backup and restore**: The backup and restore process ensures that the entire system can be restored after accidental data deletion or corruption, hardware failures and damage to facilities due to natural disasters, fire or flood. It means the ability to recover from security incidents, denial of service and malware actions. Backup and restore are the foundation of a Disaster Recovery Plan (DRP) that includes:
  - Application: for example, firmware and operating system,
  - Configuration: HMI screens, logic and control and protection settings and switch/router settings,
  - Real time: for example, event list, measurement and fault logs.
- **Detection Systems:** There are basically two types of systems for detecting intrusions, monitoring in real time all traffic on the Ethernet network:
  - Intrusion Detection System (IDS),
  - Intrusion Prevention Systems (IPS).

For substation automation systems, a network-based IDS is recommended to provide additional protection, for example, against malware, for the substation automation zone. This is because in the case of a “false positive”, there is no risk of interruption of services.

References

1. Flores, P.H.: Information management in the supervision, control and protection system: a critical evaluation of the generation of data and information, PAC World Latin America (2012)
2. Flores, P.H. et al.: Aplicações da Norma IEC 61850—Sistemas de Automação Operando com Redes de Comunicação (Applications of IEC 61850 standard—Automation Systems operation with Communication Networks), in Portuguese," Cigré Brasil, Rio de Janeiro (2020)

Maintenance and Asset Management for IEC 61850 Systems

15

Anders Johnsson, Rannveig S. J. Løken,
and Pablo Humeres Flores

Abstract

This chapter presents aspects related to asset management of PACS, including useful life, performance management, risk management, maintenance processes and asset information collection. Specific effects of using IEC 61850-based PACS are presented from the perspectives of strategy, life cycle management, performance management, decision-making/risk management, information and human resources and organisation.

Keywords

Asset management • Operation • Maintenance

15.1 General Introduction and Scope

The scope of PACS asset management inside utilities and industries owning electrical assets involves the establishment of strategies for the entire life cycle of the asset, from procurement, commissioning, operation, maintenance or modification, to decommissioning as shown in Fig. 15.1. The main aspects related to asset management include useful life, performance management, risk management,

A. Johnsson (✉)
Vattenfall Eldistribution, Solna, Sweden
e-mail: anders.johnsson@vattenfall.com

R. S. J. Løken
Statnett, Oslo, Norway
e-mail: Rannveig.loken@statnett.no

P. Humeres Flores
CGT Eletrosul, Florianopolis, Brazil
e-mail: hpablo@cgteletrosul.gov.br

P. Bishop and N.-K. C. Nair (eds.), *IEC 61850 Principles and Applications to Electric Power Systems*, CIGRE Green Books, https://doi.org/10.1007/978-3-031-24567-1_15

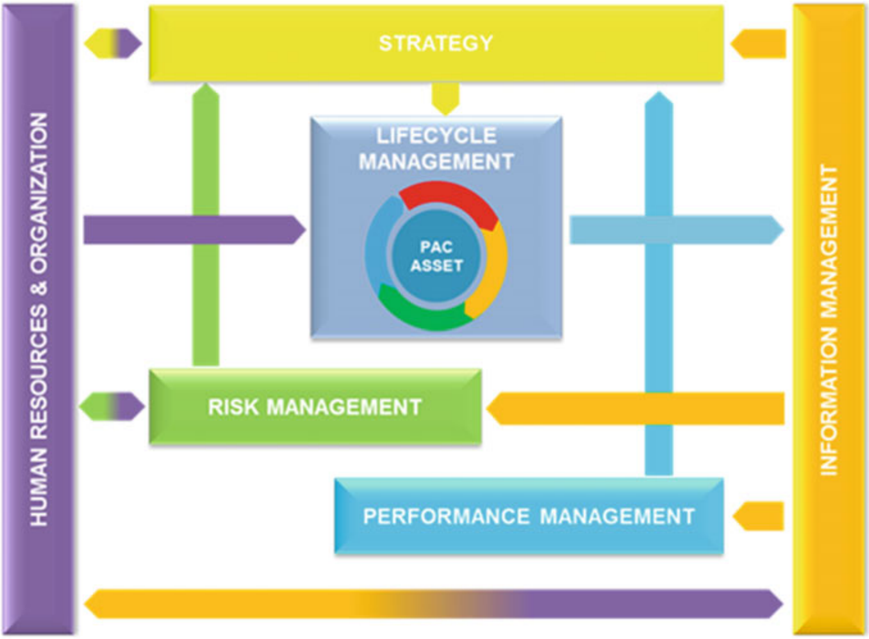


Fig. 15.1 Interrelations between asset management strategy, asset life cycle and enablers

maintenance processes and asset information collection. Accordingly, PACS asset management can be dealt with from the following perspectives:

- The strategy perspective, where key decisions are traced, for instance what is done internally versus what is externalised, how the regulatory constraints are being addressed, etc.
- The life cycle management perspective, describing the PACS life cycle, from tendering to end of life. Time is here the base element.
- The performance management perspective, viewed as a value chain composed of condition monitoring and assessment of the systems risks.
- The decision-making/risk management perspective, including the processes and methods developed by an organisation to evaluate and to analyse different scenarios in order to take decisions on capital investments and maintenance activities.
- The information perspective, that ranges from asset registration to the coordination of protection setting, model management and digital twins.
- The human resources and organisation perspective, which are usually considered as the most precious assets of a company. Training is for instance part of this perspective.

Asset management of PACS should be part of the enterprise-level asset management system that manages all types of assets. But it is in many cases still considered to be an isolated activity. The focus is here on the maintenance and asset management of practical IEC 61850 PAC systems. An important difference with IEC 61850 PACS asset management compared to asset management in general is that the built-in functionality and data model of the PACS can be used to provide status information on the assets in operation. Asset owners can monitor performance, history and availability in real-time and apply preventive maintenance policies with greater security. Asset management has become increasingly important, both in business to guarantee the return on investments and technically to ensure the availability of the PACs, which is essential for the safety and reliability of the power system. The integration of real-time process information and corporate information positively impacts the entire management of the company's business.

The most important aspects for successful and efficient performance of PACS maintenance and modification tasks belong to the quality and usability of documentation, tools and testing procedures. Therefore, the way the IEC 61850 standard is implemented into the products and tools will have significant impact on the work at this stage, e.g. due to the level of interoperability. The basis for efficient and effective management is already set out in the design and planning of the IEC 61850 substation system, as presented in chapter 7. Thus, application planning for an IEC 61850 PACS installation should consider not only an implementation plan but also its management throughout the installation's life cycle. This means defining a predictive and corrective maintenance policy for the installation.

The following requirements to be included in the technical specifications are considered key points for PACS asset management optimisation:

- Definition of a standardised PACS project documentation, including common file types, location of the repository, etc.
- Use of IEC 61850 self-diagnostic capability, with watchdog and communication link supervision, to get early and immediate notice of deviations.
- Remote access for monitoring, allowing immediate analysis of status.
- Definition and implementation of the data models to be used for asset management.

These aspects are further described in the sections following.

15.2 Asset Management and Maintenance Strategies

15.2.1 Roles and Responsibilities

Stakeholder interactions in the operation, maintenance and services processes depend on the network owner's operation and maintenance (O&M) organisation and its policies. This is true for all assets but the focus is here on what impact the implementation of IEC 61850 PACS solutions has on operations and especially maintenance. The main user groups affected by operation and maintenance are as follows:

- operation personnel;
- owner/utility personnel, asset managers (of TSOs, DSOs, IPPs); and
- maintenance engineers (in-house staff or outsourced from service suppliers like consultants, system integrators, entrepreneurs, contractors or vendors).

The different tasks can be either in-house or outsourced to service suppliers. IEC 61850 and other types of standardisation give the owner more options regarding insourcing/outsourcing of maintenance. For outsourced maintenance, the contracts and service level agreements will have significant impact on the contents of maintenance tasks and also on the reaction times to faults/alarms.

The processes can be divided into following parts:

- Continuous collection of operational data from PACS assets. Used by the operators to give performance and operational feedback to asset management, technical specialists and protection engineers
- PACS asset condition monitoring and operational data analysis. Asset management, technical specialists and protection engineers collect feedback from operations, maintenance and projects in order to evaluate the condition of its assets and remaining technical-economical lifetime of the assets and determine maintenance, repair, upgrade or renewal requirements and needs. They often also exchange PACS experience with other external users via bilateral communication, user groups, conferences and work arranged by specialist organisations/bodies like CIGRE, IEEE, IET, IEC, etc.;
- Protection configuration and settings by protection engineers. These are calculated, evaluated and re-calculated in projects, modifications and after grid disturbances, based on the experiences and planned (network, substation) changes;
- Configuration and settings documentation, handled by the PACS System Administrator, who is responsible for the platform(s), where all necessary files are located;
- Regular (preventive) or event-based (corrective) maintenance and testing of the PACS assets, fault tracing and repair or minor equipment replacement work at site, performed by PACS maintenance and testing staff;
- Modification work on the PACS equipment regarding equipment replacements, upgrades, configurations, settings and parameters that include system integration work, performed by PACS system design engineers; and
- Major or demanding PACS repairs, spare part deliveries as well as PACS equipment upgrades, replacements and modifications: sometimes, the Original Equipment Manufacturers (OEM) are needed and part of this kind work.

Good interaction between relevant parties is needed for efficient condition monitoring, performance data collection and analysis and feedback (also from operations) to asset management specialists as well as to protection setting/configuration engineers (for decision-making and change management). Good stakeholder interaction is also a prerequisite for exchanging experiences between users as well as between users and vendors, repairs, modification management and implementation, training, testing, etc. The maintenance engineering teams also have to maintain technological dominance, in order to have the necessary support for executive field teams.

Knowledge management is a challenge when introducing digital solutions with IEC 61850. The shift from hardwired solutions affects not only the PACS owners but also system integrators, maintenance companies and also suppliers, which are often contracted to carry out maintenance activities on PACS.

In addition to the asset management processes, staff training also has to follow the “Plan, Do, Check, Act” (PDCA) method. Required stakeholder skills are influenced by the installed PACS typologies and on the insourcing/outsourcing strategy of maintenance activities. With IEC 61850, there is a trend that many network owners establish an internal technical group of people capable of performing maintenance intervention and providing support in specific areas. Internal routines are then established for reporting and classifying malfunctions, errors or failures. The owner has to maintain continuous qualification policies according to the activities and responsibilities of each team.

Management strategies for new technologies associated with digital IEC 61850-based PACS need attention. Some examples are sensors for HV equipment, low power instrument transformers and merging units, while for protection relays, it is normally clear where it is managed within the organisation. Shift to IEC 61850 PACS may require change/adaptation of the utility organisation. The responsibility for the substation communication network may be assigned to the IEC 61850 protection devices or separately.

15.2.2 Knowledge in System and Component Assets of IEC 61850 PACS

As mentioned, PACS maintenance, testing and repair can be performed in-house or outsourced to service suppliers. In any case, the staff performing PACS equipment maintenance, testing and repair need to have a very good knowledge level regarding IEC 61850. If the work is outsourced, then the utility itself needs PACS asset management specialists with at least basic understanding of IEC 61850 technology, in order to be able to supervise and evaluate the quality of work. Maintenance staff also need to configure spare parts and, thus, need knowledge also to use the configuration tools, especially the IED tool. If maintenance staff do not know how to use the system configuration tool, there must also be a System Design Engineer involved. This is occurring at least in modification work.

IEC 61850 PACS call for some new skills and include knowledge of not only automation and protection functions, wiring schemes and interlockings but also knowledge in programming languages, LAN architectures, communication protocols, use of configuration tools and cybersecurity. Both the owner's asset management plans and the maintenance service provider business plans need to consider these topics and develop a structured approach towards knowledge management. Each type of component has to be considered in the maintenance plan. Cybersecurity is a new domain to integrate into asset management. Existing and well-known technologies and subsystems are typically managed in a coherent way. New technologies such as IEC 61850 need attention, especially for process bus with merging units, sensors for HV equipment and non-conventional instrument transformers.

15.2.3 Operation and Maintenance Tasks

Some of the tasks in operation of PACS that could have an effect on the reliability and safety of the system as well as financial implications include protection setting, switching of circuit breakers and disconnectors from local HMI and operation during local or remote interventions on equipment. Key is then to have well-adapted ergonomics of PACS standard design (hardware and software), to simplify maintenance by taking all possible benefits from self-supervision and to set up clear O&M procedures. Regarding more specifically the maintenance of the system, it will be important to apply philosophies focussed on reliability, to optimise actions and ensure availability. Chapter 7 describes impacts on the company: team organisation, routines and procedures, infrastructure, application tools and training. This can be developed further for the O&M tasks specifically.

The maintenance tasks for digital solutions are different from those applied to electromechanical solutions. Digital devices, IEC 61850 devices included, have the advantage of providing real-time diagnosis of all component and functional conditions. This makes it easier to manage the maintenance of devices and systems during the complete life cycle.

The fact that the process bus does not bring signals as current and secondary voltage to the control room also makes the isolations and tests safer, for the maintenance team and for the system, since it prevents electrical accidents. Since the devices do not depend on electrical signal connections, IED replacements in the control room can be performed much faster, and in the same way merging units in the yard. This physical decoupling between the Station Level and the Process Level also facilitates the management of the different life cycles of the equipment and devices, the utility being able to carry out exchanges at different times, just keeping the signals sent and received via communication protocol (Sampled Values and GOOSE signals).

15.2.4 Remote Operation Capability

A large number of equipment will need to be monitored, patched, updated and reconfigured. Some maintenance and asset management could even be done from remote, which reduces the amount of time personnel spent in a substation environment. Centralised remote access systems can be implemented, which make it possible to quickly put specialists into action when necessary. This possibility is however not unique to IEC 61850 but to most digital PACS. Many utilities today apply remote access to carry out maintenance on protection, automation and control systems. In an IEC 61850 substation, this type of intervention can be carried out more safely. All configuration is performed by software, including logic and communication signals, without the need for physical changes. In addition, it allows the application of tests that are understood by the devices as a test condition, avoiding improper trips. This impacts positively on cost and risk.

15.3 Information Management

15.3.1 Information Assets

Associated with the physical asset is also an information asset. This set of data is required to operate and maintain the physical asset and forms an integral part of PACS. For IEC 61850 PACS, the additional information asset consists of software and firmware versions running on the different physical devices. These information components also have to be stored and maintained. For this, management systems for software and system backup are to be applied.

15.3.2 Documentation

Access to documentation and tools with PACS information is key for correct maintenance. The total set of useful documentation may include as-built and as-configured documentation, inventory of all the PACS components and actual firmware/hardware version, IED/SCADA configurations, used configuration tools and documented changes. The recommendation is to use professional asset registers, IED databases and documentation systems. Access to IEC 61850 documentation and tools can also be secured by support contracts with manufacturers, including software manufacturers (if possible).

Beyond the use of the IEC 61850 standard itself, the usage of templates is recommended for a given user context. A template could include the definition of default setting of an IED, the association of a series of logical nodes in a bay, etc.

When maintenance is outsourced, clear rules should be specified in the contracts to get documentation over the realised interventions (maintenance reports with dates, found problems, undertaken actions, etc.) in order to follow up on the assets and to be able to move to another subcontractor if needed, while preserving the information about the asset during its life cycle.

15.4 Risk Management

Ensuring that in-service assets deliver the intended function over their expected life cycle is a core function of PACS asset management. The focus is here on the in-service strategy. Typical strategical topics that must be considered in the definition of plans for in-service PAC systems are related to asset maintenance, management of spare parts, outsourcing activities management, upgrades management and change management as shown in Fig. 15.2. The figure has been developed by CIGRE working group B5.63.

15.4.1 Maintenance Management

Asset management is about risk evaluation and management, but also regular and remote upgrade of configurations, software and firmware of the devices, that require new maintenance principles, avoiding outage as much as possible. Users can also invest in management systems that supervise protection, automation and control systems in real time, facilitating predictive maintenance and history of system performance.

Self-supervision allows the maintenance policies to shift from periodic to condition-based maintenance. Still, according to the results of an WG B5.63 survey [1], preventive maintenance based on periodic tests is still the most common practice in the PACS field especially for protection relays (regardless of their technology) and static batteries. This outcome indicates a certain scepticism among utilities about digital relays whose manuals usually suggest that a regular maintenance is not necessary considering that the self-monitoring functions automatically detect hardware errors and also many software errors.

The IEC 61850 standard provides different Data Objects to model information related to self-supervision and to the health condition of each device and of the whole system. Examples are as follows:

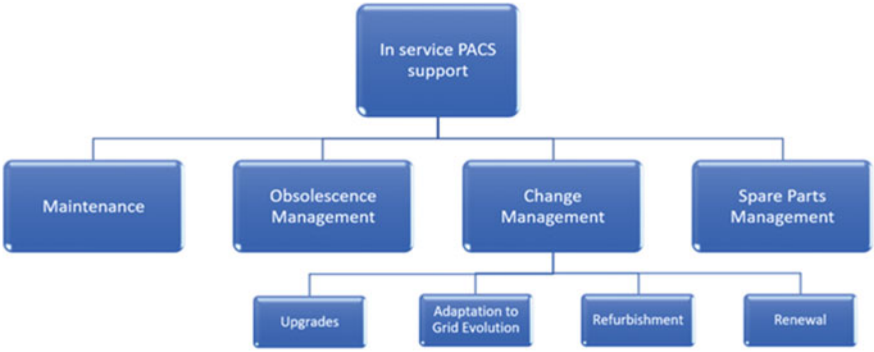


Fig. 15.2 In-service PACS support activities

- Data Object Health defined in the Common Logical Node and inherited by the <<LLN0>> and all other Logical Nodes;
- Data Object <<PhyHealth>> in the Logical Node LPHD (Physical Device Information);
- Logical Node LCCH (physical communication channel supervision)
- Quality attributes for both data objects and timestamps.

Furthermore, it is possible to define private Data Objects related to specific supervision functions that are not provided by the standard model.

15.4.2 Obsolescence Management

In general, any in-service PACS support strategy includes also obsolescence management. The PACS can for example support the obsolescence management by exposing the hardware and software versions installed. But this is not specific to IEC 61850.

15.4.3 Change Management, Fault Tracing and Time to Repair of Faulty Equipment

A standardised solution, for example based on the IEC 61850, facilitates the change management, ensuring that the owner can more easily replace parts of the system, extend the installation to include new devices, define monitoring requirements and optimise technical and economical solutions. Advantages through remote access to PACS and other devices at the substation also support improved change management, faster fault tracing and shortened Mean Time To Repair (MTTR) of faulty equipment. Improved change management by easier replacement requires backward compatibility of the PACS products and tools, including GOOSE messaging, in order to replace a faulty IED with a newer one without having to reconfigure a whole lot of IEDs and equipment.

Modifications can be minor or major. Minor modifications may be setting/parameter changes, firmware update or exchange of a single PACS device. Major modifications may be adding of a new bay to the substation or upgrading of a significant part of the secondary systems of the substation. There is no specific limit stating which kind of modification work is considered to be a minor one and which kind is a major one. However, the way the modification work will be performed is affected by the extent of work needed. Major modifications are often managed as their own projects that are purchased from contractors/service suppliers using public bidding procedures (unless also such work is done in-house). Modification work often requires changes both in the system configuration and in IEDs, so System Design Engineers probably need to be involved.

15.4.4 Spare Parts Management

Spare parts are needed for all PACS equipment supplied and installed. The availability of spare parts should be guaranteed for a minimum period of time, typically around 10 years. Standardisation on IEC 61850 and further specification of implementation of software make it possible to limit the number of different software and hardware components in the substation, and so also the different spare parts. Furthermore, a high level of interoperability between products and tools creates a flexibility to use a spare part as replacement for several similar products, because the effort to adapt to the implemented solution is low.

15.5 Performance Management

A digital substation allows the monitoring of a large number of variables, with which the asset management team can evaluate failures and performance. The definition of the maintenance indicators, Key Performance Indicators (KPI), will help to optimise the availability of the system and the repair time. With automatic fault monitoring in place, more focus can be put on performance monitoring. Thus, IEC 61850 capabilities that affect system operations and maintenance of PACS could improve asset and maintenance management due to improved condition monitoring and available asset information. The capabilities include remote access to PACS and substation primary devices, all the configuration files, logs and other documentation. Further to this, the capabilities include improved version management, including patch management and firewall updating, possibly also by remote access, product updates and end of life. And finally better easy-to-use tools to manage the PACS assets and their configurations and parameters as some today's tools are quite complicated and non-intuitive in their users' interface. Information is used to support maintenance, for statistics and planning and for failure analysis.

15.6 Maintenance Testing

15.6.1 Reasons for Testing IEC 61850 PACS in Operation

The purpose of the maintenance test is to ensure that all system components are functioning as intended. Maintenance tests are traditionally focussed on component tests and for a hardwired system also the wiring between the components. With IEC 61850, functionality and wiring are replaced by communication and software-based logic. The PACS logic will remain the same for the whole life cycle of the system, unless it is modified by an engineer. Therefore, for a system in operation no maintenance testing is required unless new components are added to it, or undetected errors in the logic occur later during the life cycle. The IEDs and their associated communications are self-monitored and will issue an alarm if they fail. Thus, there is no need for time-based maintenance tests to verify that the IEDs work correctly. Tests after configuration and setting changes, system upgrades or modification work during the lifetime of the PACS can also be considered as maintenance tests. Tests are also conducted as part of the work to identify the reason for a fault in the system during operation, i.e. as part of fault corrective maintenance. Fault finding methods differ depending on the type of the fault (erroneous operation of protection function, IED blackout or communication fault).

When testing an IED within an in-service substation, proper isolation (either physical or digital) is required. In a traditional substation, the IED contact outputs are isolated with physical test switches that provide a physical and visual isolation of the tripping and inter-tripping signal, giving confidence to the test technician that the tests will not cause an accidental tripping of other bays in the substation. However, when using IEC 61850 GOOSE messaging the use of soft isolation is the most common method. The lack of physical isolation is a big change for technicians that have only worked with conventional wired systems. Therefore, this group of technicians would still prefer to use a physical switch, which enables an IED or the whole bay to be in test mode. Local indication of isolation, for example via an LED, can be used for visualisation.

Once again, as described in chapter 7, the importance of qualifying teams must be highlighted, in order to understand the digital environment in which they operate and the domain of the tools to be used, to understand the diagnostics of the system, the intervention procedure and the necessary tests after any maintenance applied.

15.6.2 Tools for Maintenance and Testing

Test tools and systems are needed for functional tests after corrective maintenance or modifications. Common interoperable test tools are available but routines to locate the faulty part of the PACS are needed. Fault diagnosis work is typically done by maintenance staff, which may have limited knowledge in IEC 61850 and thus need quite intuitive tools and clear step-by-step routines to identify the faulty component. Easy-to-use tools are also required for additional fault tracing, as new types of errors may occur that did not exist with earlier technologies (communication errors, comm. parameter errors, etc.).

The tools should include comprehensive configuration error checking and data entry validation, audit trail, debugging and compare facilities, as well as import/export of SCL files to allow interoperability between different vendor IEDs, consistency checking of the complete SCD file and comparison features to manage the different file versions.

The testing of IEC 61850 PACS requires digitalised testing tools. In addition to the existing current/voltage injection function, the testing tool should have at least the four basic functionalities (SV monitoring, GOOSE monitoring, IEC 61850 client simulator and IED simulation). Additionally, the testing tool should preferably also be able to inject SV streams.

15.6.3 Use Case Example: Fault Diagnostics in the PACS After an Erroneous Breaker Failure Protection Trip

In this example, taken from [2, Reference TB 819], the stakeholder interactions after an erroneous trip from a Breaker Failure Protection (BFP) scheme are demonstrated. A BFP disconnects surrounding breakers in the event that a circuit breaker fails to clear a fault. In this use case, this functionality is implemented in the IEC 61850 station bus with GOOSE protocol and it has caused an outage due to incorrect configuration in an IED or in the system configuration (SCD file). The stakeholder interaction is illustrated for this case.

The Network Operator identifies the outage in the SCADA system. As a first action, the Network Operator calls out maintenance staff to the substation. They conclude that there is no fault in the circuit breaker which means that the breaker failure trip was undesired. Thus, there must be a fault in the PACS. The Network Operator will then contact the Asset Management Department for a fault analysis in the PACS.

Before the fault analysis can start, the protection engineer at the Asset Management Department has to contact the PACS system administrator to get access to all necessary configuration files and disturbance recorder files from the PACS platform of the substation. After access to these files, the protection engineer starts the disturbance analysis work. After these files have been analysed, the protection engineer knows the reason for the erroneous trip.

The reason to the erroneous trip could include:

- Incorrect logic configuration in the line protection IED;
- Incorrect parameter setting in the line protection IED;
- Incorrect logic configuration in the transformer IED;
- Incorrect GOOSE configuration, which could depend on:
  - Incorrect data set,
  - Incorrect GOOSE control block,
  - Incorrect GOOSE matrix (where the connections between the IEDs are made); or
- Malfunctioning IED.

If the reason to the fault is incorrect configuration or wrong parameter setting, which are not related to IEC 61850, the maintenance and service staff have to be sent out to the substation to fix the cause of the problem in the IED tools. Before the maintenance and operation staff can do their work, they have to be approved by the PACS system administrator to get access to the PACS files and tools from the platform. In some cases, the maintenance and operation staff need support from the OEM. The OEM becomes involved in the stakeholders' interaction when the fault is in the IED. The OEM is contacted by the maintenance and service staff in this case. In other cases, the OEM could directly be involved by the Asset Management Department. As an example, the problem with the breaker failure protection

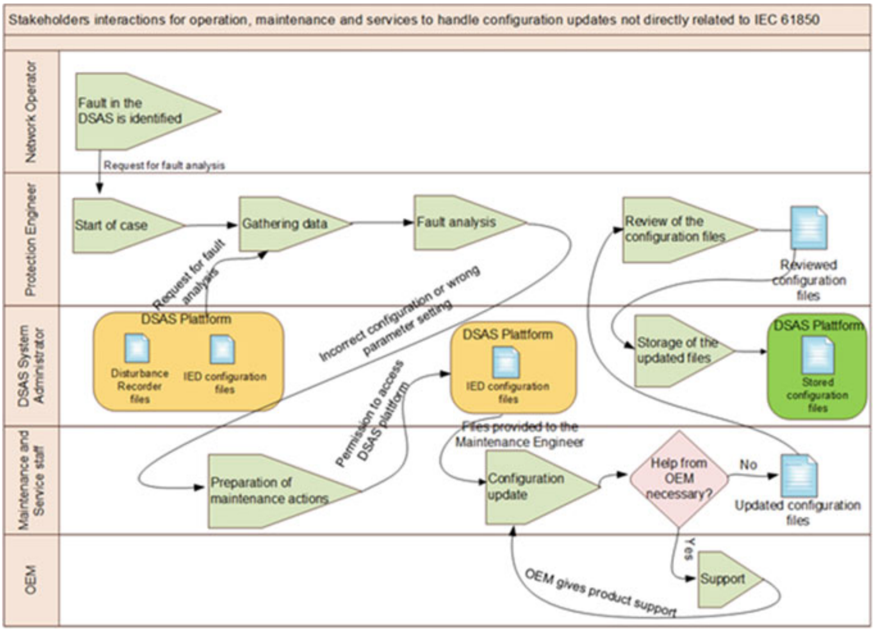

Stakeholders interactions for operation, maintenance and services to handle configuration updates not directly related to IEC 61850
Network Operator
Protection Engineer
DSAS System Administrator
Maintenance and Service staff
OEM
Fault in the DSAS is identified
Request for fault analysis
Start of case
Gathering data
Fault analysis
Review of the configuration files
Reviewed configuration files
Request for fault analysis
DSAS Plattform
Disturbance Recorder files
IED configuration files
Incorrect configuration or wrong parameter setting
DSAS Plattform
IED configuration files
Storage of the updated files
DSAS Plattform
Stored configuration files
Permission to access DSAS plattform
Files provided to the Maintenance Engineer
Preparation of maintenance actions
Configuration update
Help from OEM necessary?
No
Updated configuration files
Yes
Support
OEM gives product support

Fig. 15.3 Stakeholder interaction for configuration updates not directly related to IEC 61850

could be of general type. Then the Asset Management Department should, sometimes with the support of the OEM that have delivered the protection relay to the TSO/DSO, identify all other substations with the same type of protection relay.

When the maintenance actions are performed, the updated configuration files have to be sent to the protection engineer at the Asset Management Department for review. After the configuration files have been approved by the protection engineer, the files can be stored in the PACS platform by the PACS System Administrator. The process is demonstrated in Fig. 15.3.

If the fault depends on an incorrect IEC 61850 configuration, e.g. a missing data object in the data set and an error in the GOOSE matrix or in any IEC 61850 functionality of the protection relay, the Asset Management Department must also involve a System Design Engineer to support the maintenance and operation staff. After the IEC 61850 configuration is corrected, the files have to be sent to the Asset Management Department. But in this case also, the PACS asset management specialist must be involved in the review. Of course, the OEM must also be involved if necessary. After the configuration files have been approved by the asset management experts, the files can be stored in the PACS platform by the PACS System Administrator.

If the fault depends on a communication error, i.e. in switches, communication cards or fibres, then a Communication Engineer must be involved. The process with incorrect IEC 61850 configuration is illustrated in Fig. 15.4.

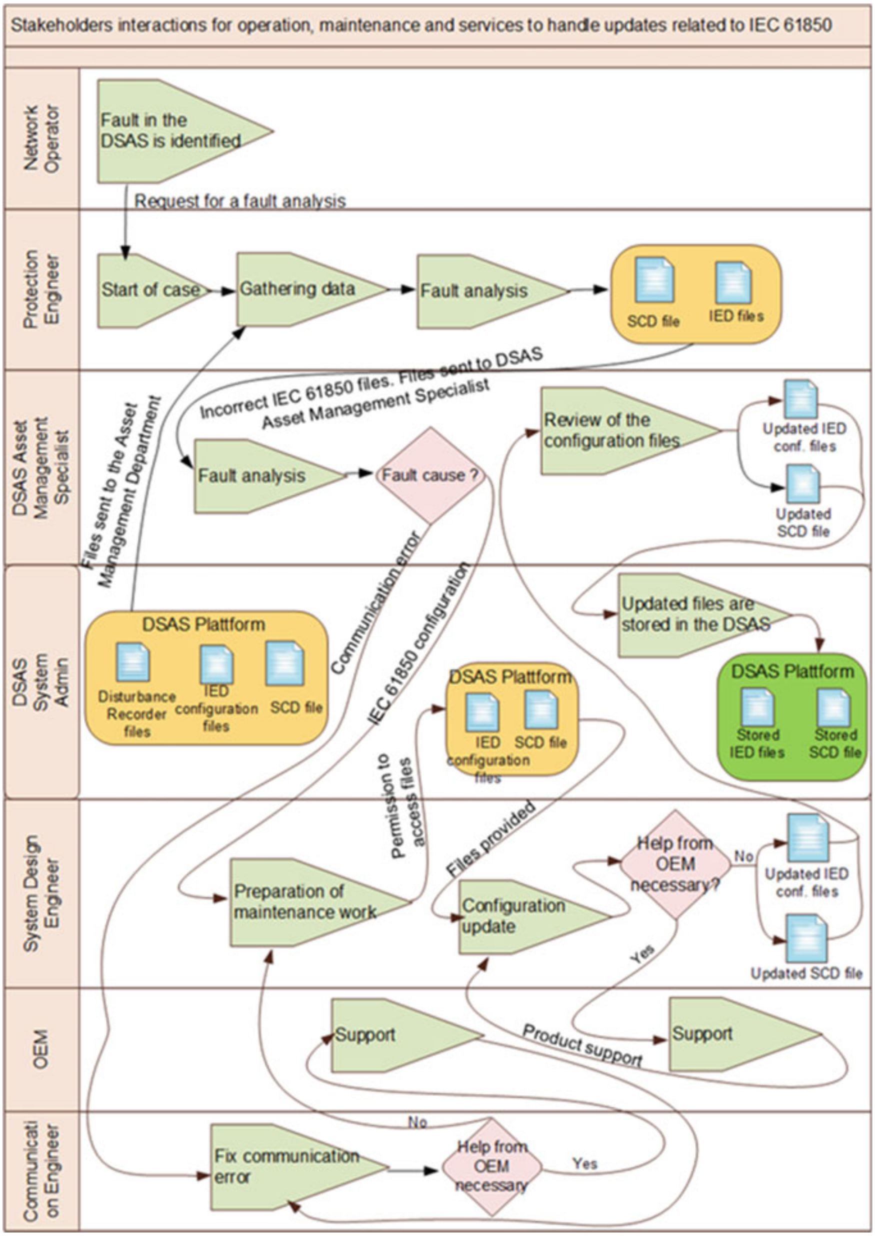


Fig. 15.4 Stakeholder interaction to handle updates related to IEC 61850

References

1. CIGRE: Protection, Automation and Control System Asset Management, CIGRE Working Group B5.63 Term of Reference, Paris, France (2017)
2. CIGRE Technical Brochure TB 819 IEC 61850 based substation automation systems—Users expectations and stakeholders interactions https://e-cigre.org/publication/819-iec-61850-based-substation-automation-systems--users-expectations-and-stakeholders-interactions

Applying IEC 61850 Applications Beyond Substations

16

David Hewings, Anders Johnnson, and Pablo Humeres Flores

Abstract

The IEC 61850 architecture is enabling wider innovations in power system protection and control, and finds applications beyond its core use in three-phase transmission and distribution networks. This chapter provides an overview of applications in electric traction systems, HVDC systems, storage and renewable energy generation, to demonstrate how these new ideas and concepts are emerging. It also takes a look into the future, and the role that IEC 61850 may play in the integration of future power systems.

Keywords

Novel applications • Electric traction • HVDC • Renewable generation

16.1 Introduction

The use of IEC 61850 in transmission and distribution has been seen to provide a dramatic change in performance, capability and flexibility to protection, automation and control systems. This chapter focuses on the growing application

D. Hewings (✉)
Network Rail, Cardiff, UK
e-mail: Dave.Hewings@networkrail.co.uk

A. Johnnson
Vattenfall Eldistribution, Solna, Sweden
e-mail: anders.johnsson@vattenfall.com

P. Humeres Flores
CGT Eletrosul, Florianopolis, Brazil
e-mail: hpablo@cgteletrosul.gov.br

P. Bishop and N.-K. C. Nair (eds.), *IEC 61850 Principles and Applications to Electric Power Systems*, CIGRE Green Books, https://doi.org/10.1007/978-3-031-24567-1_16

of IEC 61850 outside of conventional three-phase AC transmission and distribution systems, in particular use in electric traction systems, electric vehicles and also HVDC applications. This is not intended to be the definitive and exhaustive list of novel applications of the technology, but rather give some insight into how IEC 61850 has developed beyond its initial boundaries and how this may be expected to continue into the future.

As with three-phase systems, the past decade has seen a growth in the use of IEC 61850 systems to replace conventional hard-wired PACS in electric traction systems, on a like-for-like basis. Yet, more than this, new schemes are now emerging, which fundamentally change protection strategies and make use of a wide-area protection approach, well suited to the linear nature of electric traction systems. This is a major change, as the effect is not only a significant revolution in secondary substation systems, but is also now having a considerable impact on primary substation system design, and leading to "rationalised" protection and control systems for railway and other traction applications.

As well as traction, the onward growth of renewable generation creates further challenges. It changes the structure of transmission and distribution systems from top-down, hierarchical systems to distributed and interconnected AC and DC systems. Energy storage is also beginning to play a role in the wider power system structure, and all of this provides a new, rapidly changing, landscape for the protection and control engineer. The future PACS for these new evolving transmission and distribution systems will involve greater intelligence and be built upon modern communication technology. IEC 61850 is a natural partner for this evolution, and hence, it may be expected to become commonplace in each of these growing areas of future power systems.

This chapter focuses on current and future applications of IEC 61850 in these areas. It takes a detailed look at traction system PACS, and the applications of IEC 61850 that have led to rationalisation, as well as the direction of onward innovation of PACS in railways and other electric traction systems. It also then takes a look at HVDC, renewable generation and energy storage applications, together with a concluding leap into the future in which IEC 61850 is likely to be the catalyst that joins these emerging technologies together, and permits new complex, and previously inconceivable, integrated power system architectures.

16.2 Electric Traction Systems

16.2.1 Overview of Electric Traction Systems

Electric traction systems for main-line railways and light-rail rapid-transit systems need to take account of the high occurrence of faults in comparison with transmission and distribution systems. By the nature of the constrained spatial envelopes for railways, low bridges, tunnels, the desire for the largest possible trains, and traction overhead line systems bring high fault rates, and particular challenges to protection design. Conductors are sized not only for current-carrying capacity, but also mechanical dynamic performance, and for higher speed operation lightweight overhead line systems are essential for good current collection performance. Beyond all of this, traction current collection systems are designed to have a sliding electrical contact moving through feeders, at sometimes very high speeds, and this brings an inevitable increase in likely fault rates compared to three-phase transmission and distribution systems.

Historically, traction drives used DC traction motors since they were most easily speed-controlled, and so the use of DC traction supply systems dates back to the early years of the twentieth century. The challenge of AC systems was affected by the ability to operate these commutator motors at higher frequencies, and initially, 50 Hz operation could not be achieved, leading to considerable use in Western Europe of frequency converters to produce 25 Hz, or 16.7 Hz systems. Both these DC and low frequency AC systems pre-dated national electricity networks in many countries and established in some cases extensive associated single-phase transmission networks designed to provide long-distance network feeding to supply points along the railway.

Now, with modern AC drives and induction motors, such challenges are in the past, but the result is that older systems have the voltage and frequency characteristics of those earlier times. AC traction systems now standardise on one of two voltages: 25 kV at mains fundamental frequency (50/60 Hz), or else 15 kV at 16.7 Hz, which accepts the extensive use of this approach in Germany, Austria, Switzerland, Norway and Sweden. DC systems in urban areas operate at lower voltages, generally multiples of 750 V, so that 750 V, 1500 V and 3 kV DC systems are the modern standards. AC systems are single phase, to allow for simple single contact systems and the ability to electrify complex junctions, and given the relatively low voltages, particularly in urban systems, load current can often be high in comparison with three-phase distribution systems. Further complications exist in that traction systems by nature feed more than one parallel railway track and hence require parallel feeders. This then requires regular paralleling points which cannot be avoided in the power system architecture of a railway, but which would be normally undesirable in other distribution power systems. All of these factors bring challenges in applying standard protection principles to traction systems, and indeed all have generally required special protection relays, and now IEDs.

Figure 16.1 shows a typical double-track traction system, normally fed from one end to a "mid-point" sectioning location, and with intermediate sectioning locations between. Track feeder protection, which protects the contact system overhead line or conductor rail feeder which directly supplies trains, is generally based upon overcurrent or distance protection principles.

It should be noted that the single-phase nature of AC systems, and need for return in DC systems, means that in all traction systems traction return current generally flows from the wheels of the train and through the running rails back to the supplying substation. There are various AC/AC arrangements to then try and reduce this return rail current, but in all systems, this means that the conventional

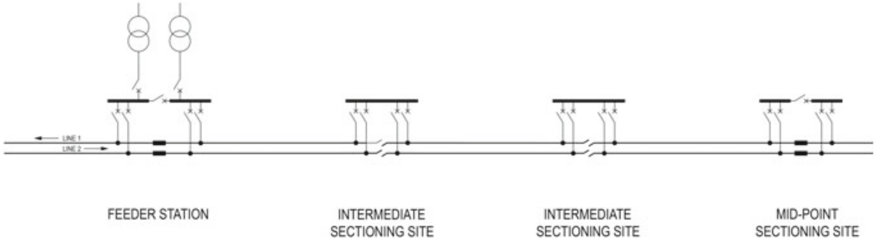

LINE 1
LINE 2
FEEDER STATION
INTERMEDIATE SECTIONING SITE
INTERMEDIATE SECTIONING SITE
MID-POINT SECTIONING SITE

Fig. 16.1 Typical double-track traction power system

view of protection design, and single-line diagram approach for three-phase systems, needs to be expanded to consider the effect of return current. This creates a return voltage drop along the running rail systems, and given that all lines are generally bonded at regular intervals, this means that feeder protection on unaffected lines sees this volt drop, which can cause under-reach on distance protection schemes and other associated issues.

Distance protection schemes are generally applied as in Fig. 16.2, with zone boundaries not dissimilar to the approach that would be taken on transmission and distribution systems.

Figure 16.3 gives a general protection arrangement for DC systems. Voltage drop to fault locations during faults in these systems, particularly with steel conductor rail systems at 750 V, can be significant, and DC overcurrent can often be supplemented by remote undervoltage detection, and the use of undervoltage intertrips, or by DC distance protection, which is used extensively on main-line DC railways in the UK. Alternative approaches, particularly employed on DC metro systems, make use of change in current (Delta I) protection and rate of change of current (dI/dt) protection.

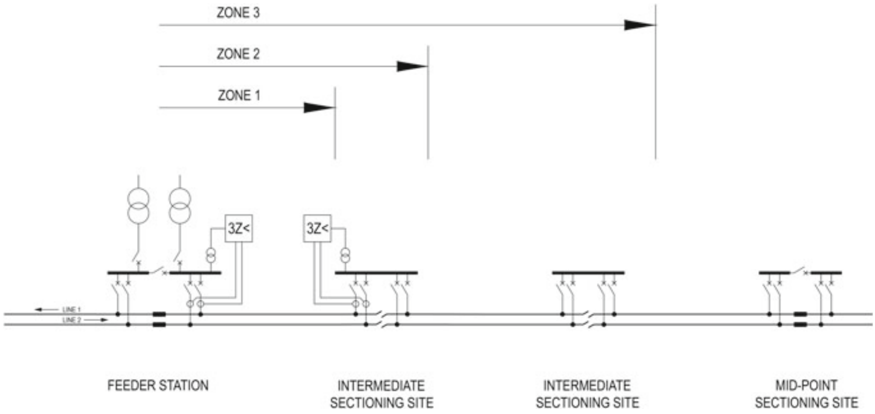

ZONE 3
ZONE 2
ZONE 1
3Z<
3Z<
LINE 1
LINE 2
FEEDER STATION
INTERMEDIATE SECTIONING SITE
INTERMEDIATE SECTIONING SITE
MID-POINT SECTIONING SITE

Fig. 16.2 Typical AC traction distance zone reach

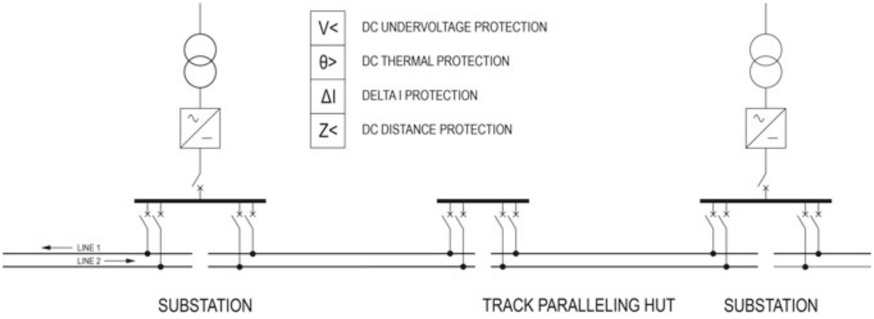


Fig. 16.3 Typical DC traction system architecture and protection functions

16.2.2 Replacement of Conventional AC Traction PACS

Given the unique complexities and challenges in traction protection design, the introduction of IEC 61850 technology brings very welcome possibilities for new protection schemes, and wide-area system intelligence, and to some extent, traction systems have been awaiting such a technology shift in order to provide new solutions to existing shortfalls. This has not yet progressed through all traction systems, partly due to the specialised nature of protection devices needed, but for AC single-phase systems, using devices which are product derivatives of three-phase devices, IEC 61850 IEDs are now readily available from many manufacturers.

The simplest form of introduction of IEC 61850 is direct replacement of conventional protection relays with IEDs, and replication of existing traction protection schemes with minimal intended change. One of the key challenges in implementing such a change, and in fact a challenge that existed previously with multi-function digital protection relays prior to IEC 61850 introduction, is the focused change from considering the device to considering the functions, their linkage, and to begin to consider design in terms of the logical nodes. Figure 16.4 gives an example diagram used to define the functions of a traction distance scheme and broadly based upon the principles of the Unified Modelling Language (UML) to graphically define the scheme design. Such scheme functional diagrams assist in providing clear definition and become more important as traction protection becomes more sophisticated, and wide-area schemes emerge from the conventional schemes. For any protection scheme, the starting point is a clear understanding of the performance, in terms of availability, selectivity and response times. The setting out of these principles for a traction protection scheme has been embedded in a recent European Standard, EN 50633 [1], and this fits well with the use of these structured design methods.

Even with this first-level simple approach to using IEC 61850 systems for traction protection as a like-for-like replacement for conventional protection, there emerge clear advantages, and additional functionality and facilities which can be provided more readily with the new technology. Firstly, it should be recognised

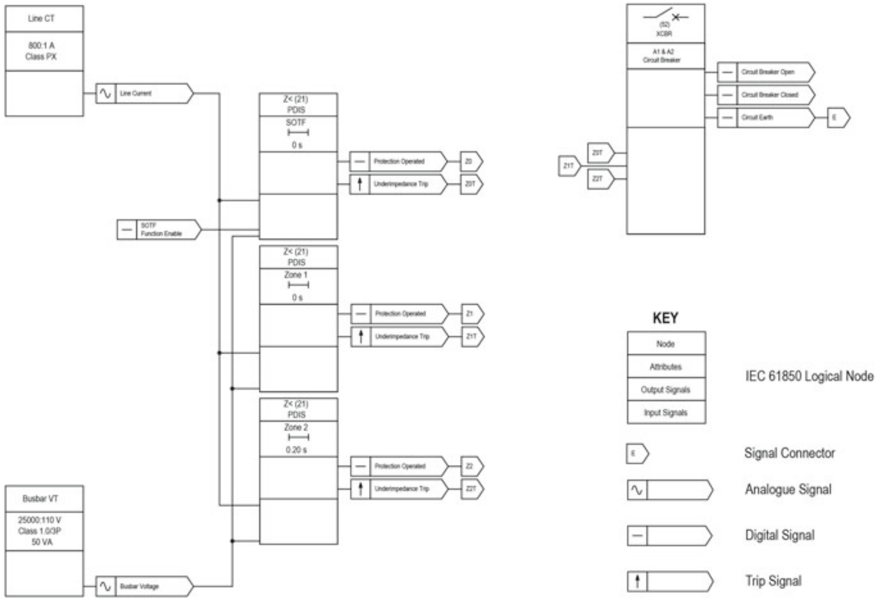


Fig. 16.4 Modified UML approach to function definition for a traction system IEC 61850 scheme (based on EN 50633)

that planned isolation on railway traction systems occurs very often compared to transmission and distribution systems. Instead of outages being infrequent events, the need to maintain not only overhead line and electrical systems, but also track, signalling, earthworks and other assets means that outages can be often required almost every night on some railway systems. This not only increases the duty on switchgear, but importantly means that switchgear controls are being exercised very frequently. With conventional protection and control, and separated control and protection wiring to switchgear trip and close circuits, there is a continued requirement for trip circuit monitoring. With IEC 61850 integrated protection and control, and single controls from one IED operated almost daily, the basis for such monitoring can be reviewed, particularly for full monitoring which requires additional circuitry beyond the functionality of the IED.

Aligned with this approach, circuit breaker failure can now be more easily protected by incorporating GOOSE back-trips to incoming supplies, or to provide mass-tripping of outgoing feeders, all without the additional wiring complexity that this would have previously required. In addition, simplified busbar protection can be provided using this approach, and this is a development in the UK, to avoid a separate busbar differential scheme, and instead make use of the existing IEDs to provide simplified power differential analysis.

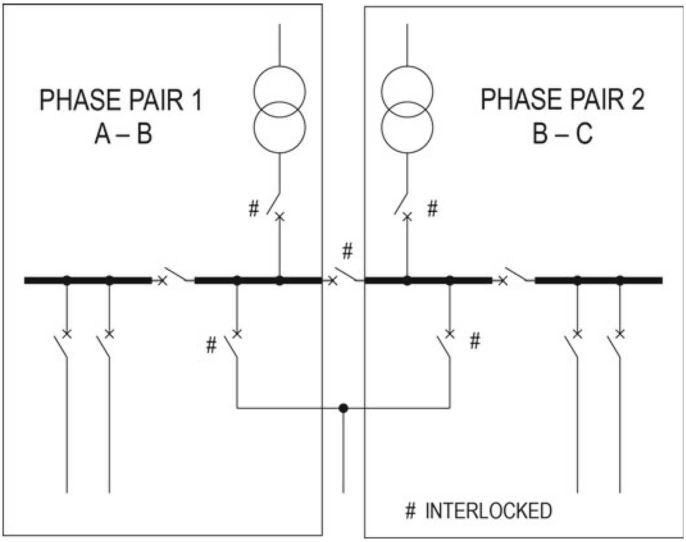


Fig. 16.5 Single-phase traction feeder station requiring complex interlocking

16.2.3 Application to Enhanced Interlocking

Following the approach taken to enhance functionality of replacement schemes, it is also possible to consider enhanced interlocking in a much-simplified way using IEC 61850. Consider an AC traction feeder station. This is the point of connection of incoming supplies to the railway and generally includes two supplies for resilience. These are often on separate phase-pairs, in order to reduce overall three-phase imbalance, and generally operate independently, but may be required to cover outage of the other incoming circuit.

Figure 16.5 shows a modern approach. More resilience can be achieved by meshing the busbar arrangement. This complicates the interlocking arrangements when the two busbars may be supplied from differing phase-pairs and is generally avoided in hard-wired schemes due to the complexity which results. However, such a scheme can be provided by GOOSE interlocking relatively easily, and without the additional wiring, and this in turn provides for a more resilient traction power system.

16.2.4 Application to Traction Wide-Area PACS

Whilst like-for-like replacement of conventional protection schemes can offer considerable advantages, IEC 61850 offers far more possibilities in rethinking the nature of traction protection schemes.

Traction systems are, inherently, linear multi-feeder systems. They also provide supplies to linear rail corridors, and when considered as a railway system, rather than a power system, the reliability and availability of the network need to be considered in terms of available train movements. Short protected sections, with multiple substations, do indeed shorten the length of feeder impacted as a result of a fault, but they do not necessarily shorten the length of railway service affected by the fault. If even a short section of the rail corridor is left without power, the railway may be inoperative over a much wider area.

Conventional traction system sectioning is often provided to match the reach limits of protection, rather than the operation of the network, and the continued use of discrete protection, i.e. separated decision-making by individual protection devices, fails to acknowledge the pooled knowledge which can be provided across many devices and substations at the time of a fault. By bringing this wider network knowledge together in a wide-area scheme, it is possible to develop faster responses, and improved selectivity and discrimination in new traction protection schemes.

The recent development of EN 50633 for new traction protection schemes has considered the design approach to such IEC 61850 wide-area schemes. It also starts to embed UML notation for better definition and description of protection functions, and protection sequencing, and is an example of how IEC 61850 is changing wider standards in other sectors of power systems, and becoming more naturally embedded.

Taking the wide-area scheme approach of EN 50633, the operation of the scheme provides for high-speed performance with improved selectivity. Consider Fig. 16.6, which shows a wide-area traction protection scheme. For a fault at A, protection at Substation 1 sees the fault in Zone 1 reach of its feeder distance protection on Feeder 1, whilst protection on Feeder 2 can restrain. However, for a fault at B, the paralleling sites mask the ability to provide selective protection at Substation 1. The wide-area approach uses a simple high-speed trip of all lines, whilst capturing the direction of current at the intermediate sites. That directional information allows a restoration permission message to be transmitted via GOOSE to the supplying end, so that unfaulted feeders can be restored. This permits restoration in less than five seconds. However, this approach brings another advantage, in that it removes the necessity for sectioning locations, and indeed circuit breakers, at the intermediate substations.

The overall concepts of application of IEC 61850 to traction systems may be considered systematically as progressive levels or extents of implementation. Figure 16.7 shows how these levels progress from traditional hard-wired systems, through replacement with IEC 61850 functions and then to full wide-area new functionality. It can be said that these may apply equally to transmission and distribution systems, but given that traction systems are often not as closely linked to the changes in this technology, it is useful to provide road maps such as this to assist organisations in assessing the appropriate application of the technology in overall network asset management strategy.

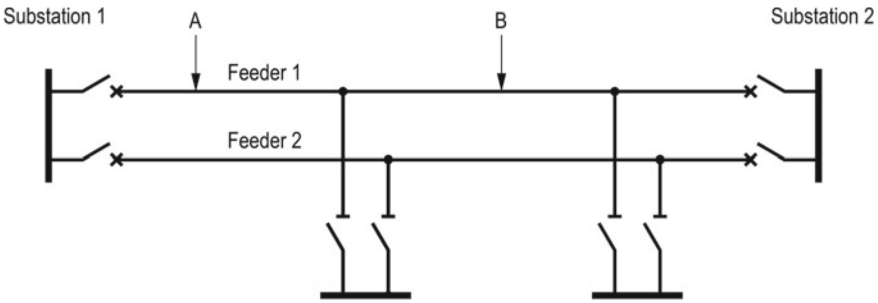
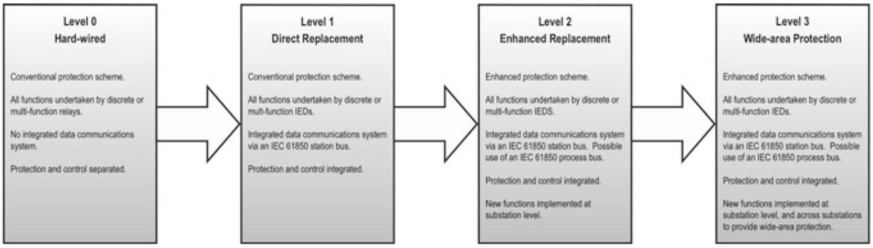


Fig. 16.6 Rationalised AC traction system design for wide-area IEC 61850 protection



Level 0
Hard-wired

Conventional protection scheme.

All functions undertaken by discrete or multi-function relays.

No integrated data communications system.

Protection and control separated.

Level 1
Direct Replacement

Conventional protection scheme.

All functions undertaken by discrete or multi-function IEDs.

Integrated data communications system via an IEC 61850 station bus.

Protection and control integrated.

Level 2
Enhanced Replacement

Enhanced protection scheme.

All functions undertaken by discrete or multi-function IEDS.

Integrated data communications system via an IEC 61850 station bus. Possible use of an IEC 61850 process bus.

Protection and control integrated.

New functions implemented at substation level.

Level 3
Wide-area Protection

Enhanced protection scheme.

All functions undertaken by discrete or multi-function IEDs.

Integrated data communications system via an IEC 61850 station bus. Possible use of an IEC 61850 process bus.

Protection and control integrated.

New functions implemented at substation level, and across substations to provide wide-area protection.

Fig. 16.7 Suggested level definitions to assist in application of IEC 61850 to traction power systems

16.2.5 Application to DC Traction Systems

It is fair to say that, to date, DC traction systems have not advanced in use of IEC 61850 at the same pace as AC systems, and this is an area where specific IEDs, built for the application, could be considered necessary. At the same time, DC traction protection utilises many of the same functions as AC traction protection, such as overcurrent, undervoltage and distance protection, and so these can all be modelled with the same logical nodes used for AC systems. The principle challenge at this time is the development and production of traction IEDs with IEC 61850 capability.

Additionally, there are protection functions which are unique to DC traction protection, such as Delta I and dI/dt protection. These use the change of DC current, and the rate of change of DC current, respectively, as a means of discriminating between load and fault conditions. Specialist protection relays exist for these functions, and generally, integration of these into a DC traction IEC 61850 system can be undertaken by connection to using GGIO logical nodes. These provide a means of connecting generic inputs and outputs into the IEC 61850 system. Their use is often deprecated, since the generic nature of the node loses the description of its function, but nevertheless for limited application in areas where development is still progressing, such as DC traction systems, the GGIO offers the IEC

61850 system designer a means of working with existing specialist functions not yet developed in logical nodes.

Given that an IED vendor does not know the intended purpose of any specific physical input or output (I/O) to the IED, any system requires IEDs to be manufactured with a set of generic GGIO logical nodes. The GGIO logical node has various configuration options, from a single instance with multiple data objects, to an individual GGIO per physical I/O of the device. However, if this is widely applied a system with 100 IEDs each with 20 physical I/O may have 2000 GGIO instances with a wide variety of individual purposes. This is distinct from the clarity of a defined logical node such as PTOC LN, which is known to be an overcurrent function, and therefore makes for simpler description of the operation of the system.

In order to overcome some of these difficulties with the use of GGIO nodes, an extremely useful feature of some proprietary IED configuration tools is the ability to rename GGIO instances to a relevant logical node as defined in IEC 61850-7-4 and -7-3, or as a so-called private namespace logical node so that their functional meaning is inherently described.

Figure 16.8 shows a typical 750 V DC traction substation arrangement, with AC three-phase feeders, transformer rectifier, and DC traction feeders, with the specialist DC traction protection functions interfaced into an IEC 61850 network using an IED (such as an AC bay controller IED) such that both AC and DC functionality can be provided through an IEC 61850 approach.

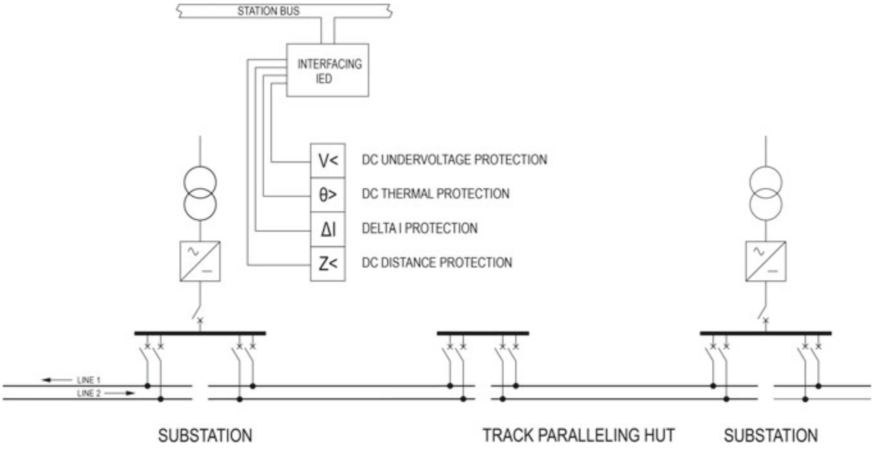


Fig. 16.8 IEC 61850 interfacing approach for DC traction protection

16.2.6 Advanced IEC 61850 Traction System Performance Monitoring

Beyond the like-for-like replacement, and even the enhanced wide-area traction protection schemes, application of full railway IEC 61850 systems has enabled new developments in advanced monitoring.

An example is the Great Western Main Line, in the UK, one of the first railways in the world, originally designed by Isambard Kingdom Brunel in the 1830s, then electrified between 2010 and 2019, and the first to be fully designed as a wide-area IEC 61850 system. This has involved provision of dedicated multi-core fibre cables throughout the 200 km of electrified line, giving enormous dedicated bandwidth for protection and control wide-area communications. Such telecommunication capacity for IEC 61850 systems is relatively easy to provide for traction power systems since railway utilities generally own their own telecommunications system and also have the land corridor to provide new systems. Also, electrification of existing lines inherently requires extensive modification to existing railway signalling and telecommunications systems to prevent electromagnetic interference, such that as part of any electrification project there is the opportunity to add dedicated fibre connections at relatively low cost.

The result is that such a network, once installed and providing protection and control functions, then provides inherent capacity for additional monitoring of energy, power quality, voltage regulation, traction conductor current loading, and that this is possible from station bus to a corporate office environment without the traditional need for these to be integrated into an overall SCADA control system. This allows changes to monitoring to be undertaken without directly affecting the availability of the SCADA control system, and hence the railway traction system. This work is now progressing on the IEC 61850 system of the Great Western Main Line, with the intention that by 2023 the use of the first wide-area traction protection scheme will be enhanced by process bus technology to provide new system monitoring, and hence enable reduced cost asset management of the traction power system.

Beyond this approach, there are developments in using IEC 61850-9-2 analogue measurements as Sampled Value streaming as a basis for further monitoring. The T-group logical nodes of IEC 61850-7-4 provide for a wide range of analogue sensor values such as temperature, wind, contact force and conductor tension, which can all be brought into a IEC 61850 data architecture, and as a result, the architecture can be used for overall traction system monitoring, and hence enabling new facilities such as dynamic conductor ratings, and hence dynamic train service provision. Table 16.1 gives an overview of these logical nodes.

Table 16.1 Analogue sensor T-group Logical Node data models in IEC 61850-7-4

Logical node	Analogue sensor	Logical node	Analogue sensor
TANG	Angle	TMGF	Magnetic field
TAXD	Axial displacement	TMVM	Movement sensor
TCTR	Current transformer	TPOS	Position indicator
TDST	Distance	TPRS	Pressure sensor
TECW	Measurement of electrical conductivity in water	TRTN	Rotation transmitter
TFLW	Liquid flow	TSND	Sound pressure sensor
TFRQ	Frequency	TTMP	Temperature sensor
TGSN	Generic sensor	TTNS	Mechanical tension/stress
THUM	Humidity	TVBR	Vibration sensor
TLEV	Level sensor	TVTR	Voltage transformer
TLVL	Media level	TWPH	Water acidity

16.2.7 Future IEC 61850 Traction Substations—Rationalised Electrification

For the future, the introduction of wide-area trip and reclose schemes allows for widespread rationalisation of switchgear. Based on the configuration given in Fig. 16.6, many intermediate sites in a traction feeding section do not require circuit breakers, as a result of the shift to wide-area protection and the use of IEC 61850 as the enabling technology for this shift. Consequently, these intermediate sites can be reduced to simple overhead line switches. Hence, many of the substations as "sites" are removed with this approach, replaced by overhead line integrated switching sites. This permits a more balanced approach to traction substation costs and indeed allows the important junction and feeding substations to be better provisioned for resilience. All of this results in a more robust traction power system, and hence a more reliable transport system for passenger and freight services. This is an example where the protection philosophy change, enabled by IEC 61850, then enables a significant change and reduction in switchgear and substations, and this has led to the concept of the Rationalised Traction System developed for electrification of the Great Western Main Line railway in the UK by Network Rail. It is expected that this approach will be further refined and developed across the traction power system industry, and as the benefits of wide-area traction protection become evident, IEC 61850 is expected to become a dominant architecture for future traction systems.

Additionally, the ability to use streamed data, and the introduction of process bus technology in traction systems as part of this development, also permits connection of new types of supply using converters, such as three-phase to single-phase converters. The typical arrangement for such a converter supply is shown in Fig. 16.9, where a three-phase system supplies a DC link which is then converted to a single-phase AC supply using a multi-level converter. The potential exists with

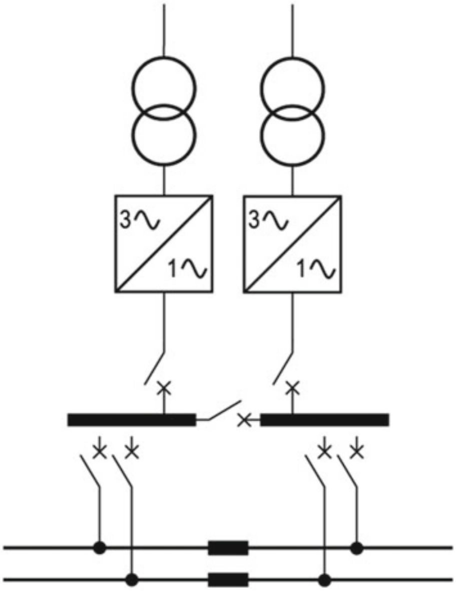


Fig. 16.9 Converter-based AC traction supply

such supplies to control phase angle and hence integrate with existing transformer supplies. The traditional limiting factor has been the capacity of communications and control systems purpose-built to operate with traction system demands and voltage regulation, and this is an area where the IEC 61850 process bus offers the possibility of a standardised approach. Further, such an architecture opens the possibility of integrating diverse supplies, such as from renewable sources, and storage, to traction systems, and hence enable more-optimised, lower-cost, low-carbon transport systems.

16.3 Hydropower Plants

Application of IEC 61850 to hydropower is provided in Part-7-410 of the standard [2]. Additionally, Part-7-510 [3] of the standard gives a Technical Report (TR) that gives explanations and suggestions on how to use IEC 61850 for applications in hydropower.

A hydropower plant normally comprises equipment and systems from a number of vendors. By applying a comprehensive data model, such as IEC 61850 for information modelling the systems (e.g. the turbine governor and water level measurement devices) can exchange data and interoperate in a defined way. The tasks of the Operator and Maintenance personnel are thereby simplified by offering them a uniform interface to all equipment and data. Control, optimisation, visualisation in SCADA/HMI and further data analysis in external systems all become easier when data from all subsystems are modelled in the same way.

Working Group WG18 of IEC Technical Committee TC57 that is responsible for development of IEC 61850 documents for hydropower. As of March 2021, this group is focusing on publishing an updated version Edition 2 of the TR (Part-7-510) by the end of 2021. In parallel with this, WG18 is constantly working on improvements of the IEC 61850 model for hydropower, as defined in Part-7-410 of the standard, with a new version planned for official publication in the autumn of 2022.

The IEC 61850 model for hydropower is an extension to the core IEC 61850 model, and Part-7-410 is built with the same principles and Common Data Classes (CDC) as the core standard. It defines many new logical nodes suitable for use in a hydropower station, and it also extends some of the logical nodes from the core part with additional data objects useful for application in the hydro domain. Logical nodes developed specifically for use in hydro reside in LN Group H.

The current version of Part-7-410 incorporates two data classes specific for hydro (CDCs RST and TAG), but TC57 WG18 is preparing to deprecate their use and replace the specific CDCs by other solutions using only CDCs from the core part of the standard in the next revision. The onward development of IEC 61850 for hydropower will continually aim to reduce domain-specific solutions and consequently re-use as many as possible of the modelling concepts and solutions from the core standard.

Some examples of hydropower domain-specific logical nodes defined in Part-7-410 are:

Production Unit: GUNT. The LN GUNT is used to represent the physical device of a production unit, typically consisting of a turbine, a generator and the associated control and ancillary equipment. The logical node holds information about the operational status of the unit and is also used for control commands to change the operational status. The LN GUNT is used to provide a standardised interface to a client for an entire unit.

The LN GUNT has mandatory defined enumerated statuses (DataObject UntOpSt) and operating modes (DataObject UntOpMod) that are required to be used to show the current status of a unit (e.g. Stopped, Starting, Synchronised) and operational mode (e.g. Generating, Synchronous Condenser or Pumping mode) to an external client. Additionally, LN GUNT has many optional data objects defined, such as for temporary power limitation settings, that can be used in the data model of a unit when suitable.

Water Level Indicator: HLVL. The LN HLVL represents the water level sensing device.

The LN has a mandatory data object LevM (MV, Measured Value) that is used to represent the water level at the point of measuring. The LN has defined optional data objects for level offset, and to indicate a problem with a stuck (frozen) sensor, which can be used when suitable.

Governor Control Mode: HGOV. The LN HGOV shall be used to present information about different control modes of a turbine governor. One LN HGOV instance is created for each Governor Control Mode.

The LN has a mandatory data object Out (MV, Measured Value) that shall be used to represent the output of the governor controller. Additionally, LN HGOV has several defined optional data objects used for example to indicate whether the Control Mode is active, and to set the Control Droop.

Even as the standardised information model offers many optional data objects, and includes many defined enumerations and listed items, it can never encompass all the needs of every real hydropower implementation. Therefore, an implementation in a real hydropower station may extend the standardised general model with additional parts according to specific requirements.

To enable compatibility with tools, and interoperability between systems, it is essential that there is documentation of the precise configuration of the logical nodes and data objects, including selected optionals and created extensions that have been implemented. This is done by defining a data type (DataType) that defines each object incorporated in their model.

By observing the rules and recommendations set forward in IEC 61850 regarding definition of types and extensions the resulting data model will still be compatible with the IEC 61850, and with all used optional parts and any extensions clearly defined in a uniform way. The rules for extension of the IEC 61850 model are explained in the guideline in Part 1–2.

To take further advantage of the application of the information model in hydropower, a naming system defined by the system owner (the power company) can be applied to the model. IEC 61850 allows for precisely this, as long as the naming system follows some of the rules defined in the international standard ISO/IEC 81346 [4], which gives reference designations and structuring principles (RDS). The forthcoming Part 10 of this standard (ISO/IEC 81346-10) gives the RDS for power systems (RDS-PS) and defines the reference designation codes for power system processes such as generators, pumps and transducers.

By applying a data model according to IEC 61850 together with a designation system according to ISO/IEC 81346 RDS standard, a standardised data model can be achieved with element names which can be defined independently of an IED structure. In this way, a company owning several hydropower plants can define common system names and apply them in SCL for all their hydropower units independent of the fact that each unit may have an individual structure of IEDs delivered by different vendors.

This concept applies the IEC 61850 process structure as defined in IEC 61850 Part-6 (SCL). An IEC 61850 model can be expressed as both an SCL process structure and an SCL IED structure. By defining the model as a structure of SCL process elements, it is possible to assign RDS designation codes for each process element. The process elements are mapped to the logical nodes in the implemented IED model.

In the coming Edition 2 of technical report TR IEC61850-7-510, Working Group WG18 gives examples on how this can be achieved by applying a

Table 16.2 Mapping of RDS designation level to SCL process structure level

Level	RDS	SCL
0	Top node	Process<*Type TopNode*>
1	Functional (main system)	Process <*Type FunctionalSystem*>
2	Technical	Process <*Type TechnicalSystem*>
3	Component	Process<*Type ComponentSystem*>

Source IEC TC57 WG18

draft version of the coming ISO/IEC 81346-10 on an SCL process structure for hydropower. The example below is based on the forthcoming TR.

Table 16.2 shows how each level in an RDS designation (ISO/IEC 81346) structure can be mapped to one level in an SCL process structure (IEC 61850 model). The concept is to let each RDS designation level be represented by one SCL process element level. The SCL process element names are selected according to the RDS codes.

The implemented IEC 61850 IED model can be mapped to the RDS designation structure used. Inside the IEC 61850 SCL configuration file, the process section (structured according to RDS) corresponds to the IED section with the implemented logical node. The last level of the SCL Process tree is an SCL function element used to contain the logical node element.

Figure 16.10 shows in a schematic way how the SCL process elements (with names according to the RDS code) are mapped to the SCL IED section.

The implemented IED model, which differs between vendors and implementations, can then be referenced by a common set of RDS designation codes and an SCL process element tree structure. This is useful for setting up uniform data models across a hydropower unit fleet.

16.3.1 Practical Application of IEC 61850 in Hydro Power Plants

As already presented, a hydropower plant involves a variety of control systems, each with different objectives. The control and protection system of a hydropower plant can be defined by the following main systems:

- Supervisory system (local and remote)
- Control and protection of each generating unit

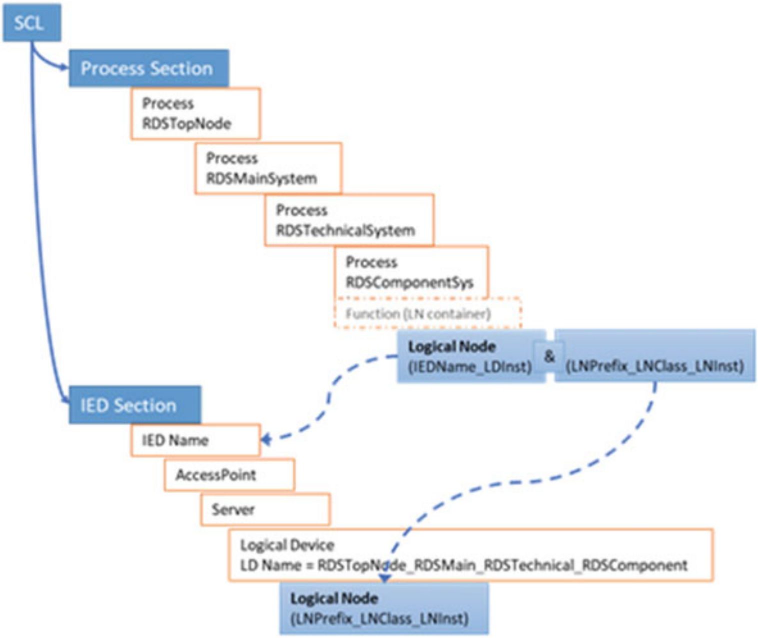


Fig. 16.10 Schematic mapping of SCL process and IED sections. *Source* IEC TC57 WG18

The control and protection of each generating unit then include the following functions:

- Turbine controller (speed regulator)
- Generator controller (voltage regulator)
- Generator group automation
- Generator group protection

Each of these systems applies different engineering solutions. They are defined by issues of legacy systems, costs and available technologies, and generally, the application of IEC 61850 solutions is not yet common. There are a few reasons for this. The first is that the devices must be able to apply the concepts of the standard and many currently cannot. Another aspect is that it is necessary to apply a data model as defined in the standard, and for many functions, the time taken to define them within the standard was either longer than anticipated or in some cases has yet to be defined and included. Finally, the changes impact the way in which hydropower applications have been implemented for decades, which would mean changing protection, automation and control devices, infrastructure and implementation routines.

But in many countries, for example in Brazil, there is now a process of modernisation of hydropower plants. This process is very complex, because it means replacing devices, signals and infrastructure of a plant that is in operation. As a result, they involve long implementation processes, possibly years, where it is necessary to take advantage of generator shutdowns to carry out the modifications. Some very interesting questions need to be evaluated:

- How to define a technological solution that remains valid until the end of the implementation of a project?
- How to integrate solutions implemented over time that can be provided by different vendors?
- How to maintain the technological domain of the project, maintenance and operation teams?
- How to make physical installation fast and decrease generation interruption times?
- How to perform tests safely without the risk of involuntary shutdowns?
- How to make future changes to functionality without requiring discontinuity of service?

The evaluation of many companies is that the answer to these questions is the application of a solution based on the IEC 61850 standard, which points exactly to these advantages in its implementation: time-proof solutions, interoperability between different vendors, technology based on data model concepts, virtual tools, implementation with a minimum of electrical cables, tests based on functionalities without the need for electrical insulation and with the possibility of alterations or implementation of new functionalities more easily (without the need for physical modifications).

A very interesting example of the application of IEC 61850 in hydropower plants is the experience of Itaipu in the Brazilian electrical system. It is a large plant, with 14 GW, which decided to modernise after starting its operation in 1984. The plant has 20 generating units. Figure 16.11 shows an overview of the systems in the Itaipu complex.

Upgrading each unit requires a few months of work, so the whole process involves years of implementation. This complexity of the project is mainly due to the need to upgrade at the same time as maintaining operation to provide adequate levels of power production, given that Itaipu Dam accounts for 15% of Brazilian electricity consumption and 90% of Paraguay electricity consumption. This is a rather different scenario than that of designing and building a new plant. For this reason, Itaipu has designed a strategic plan for this upgrade, which considers the long duration, the multiple phases of implementation and activities to be carried out and the need to maintain output.

Studies started back in 2006, with the definition of guidelines and criteria, analysis of equipment status and a basic version of a Technological Upgrade Plan. In mid-2013, the development of the upgrade strategic planning began, in which activities to be performed throughout the project, such as carrying out of studies, establishment of methodologies, project assumptions and previous definitions, were established and evolved over the course of planning.

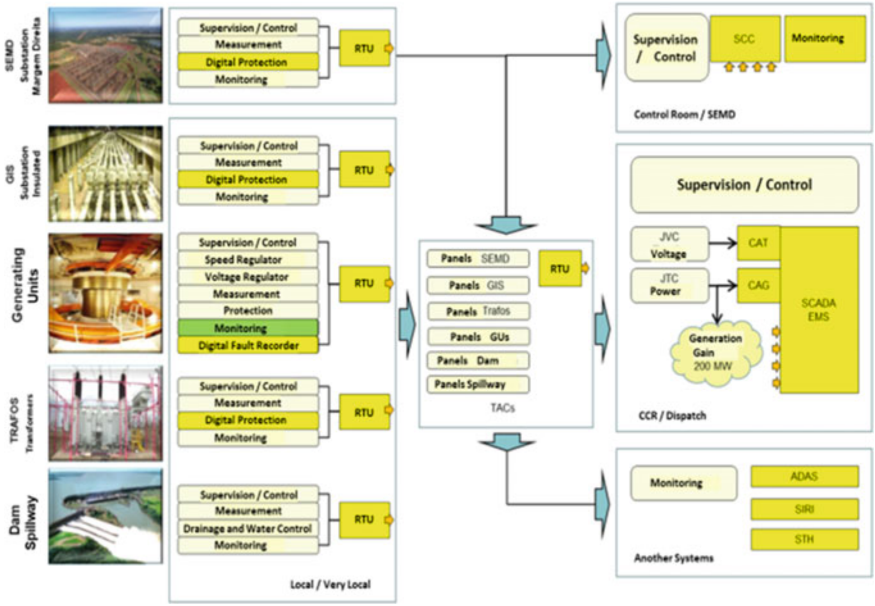


Fig. 16.11 Summary of systems of the ITAIPU complex. *Source* IEC TC57 WG18

In this stage, all functionalities were also defined in order to apply a model adhering to the logical nodes of the IEC 61850 standard. The application of the standard was the design option due to meeting the requirements defined by the complexity and duration of the project implementation.

The architecture of the project was also defined, which is shown with a simplified view in Fig. 16.12.

Between 2016 and 2018, the basis of the technological upgrade project was executed, consolidating study results, guidelines and technical specifications for the bidding process. In the second half of 2018, the first stage of the technological upgrade was carried out, namely a pre-qualification of bidders for project delivery, thus classifying Brazilian and Paraguayan companies or consortia that must compete for the bidding process. The implementation was divided into three contracts, and this is in an executive project phase. The physical works should start in 2023 in the central systems and from 2025, two generating units each year out of the 20 total units, ending in 2035.

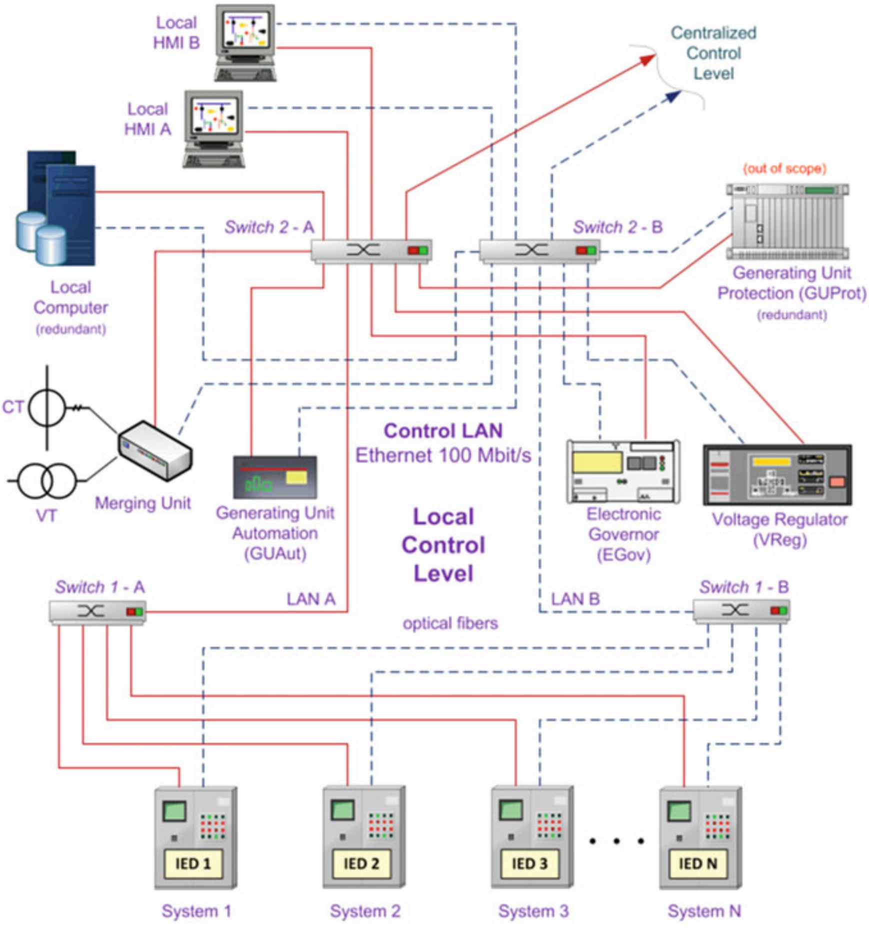


Fig. 16.12 Conceptual physical architecture of the local control level. *Source* IEC TC57 WG18

16.4 Wind Power Plants

16.4.1 The Wind Information Model, IEC 61400-25

This section describes the IEC 61850 domain extension for wind standardised as IEC 61400-25 [5]. Unlike other parts of IEC 61850, the information model is a connection standard from SCADA to wind parks, aiming to provide a standardised data connection between TSO, DSO, OEM maintenance centres and the wind farm power plants.

16.4.2 History

The standardisation work of IEC 61400-25 began in the year 2000. The aim was to have a data interface, supporting all customer use cases independent of vendors and the different versions of each vendor. At that point, in time all vendors had their proprietary system, which often required a vendor-supplied SCADA system at the Operations and Maintenance (O&M) control room. The portfolio of wind farms from different vendors often results in 20 or more different SCADA client systems in the O&M control room. An example of this is shown in Fig. 16.13 from Vattenfall surveillance centre where 11 OEM-specific SCADA systems are installed requiring an additional supervising SCADA system to manage the fleet of 1500+ turbines in five countries.

The primary objective was, and still is, the data model, which defines the structure of data in an object hierarchy. The next objective was defining access to the data. An exchange model from IEC 61850 was copied and slightly modified. However, it was almost impossible to agree on a single communication protocol. IEC 61850 used MMS, but this was not at all used by any vendors at that time. The only way to move forward was to standardise mapping to 5 different protocols, namely MMS, Web Services, OPC XML-DA, IEC 60870-5-104 and DNP3. This was done in the full knowledge that only MMS and Web Services were able to support the complete exchange model.

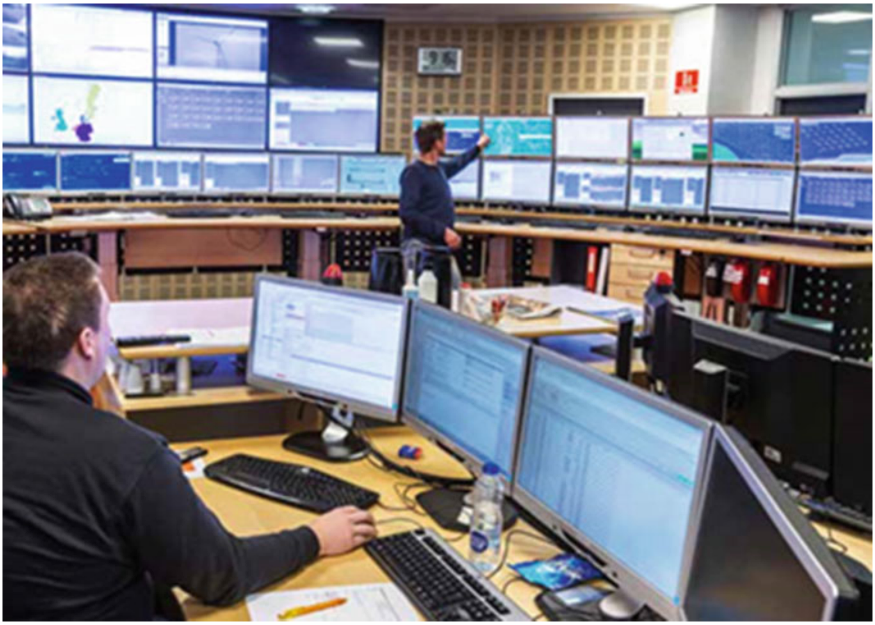


Fig. 16.13 Wind Power Surveillance Centre monitors and operates all turbines. *Source* Vattenfall Eldistribution

In the year 2000, several frameworks or systems were discussed. The OPC UA work was evaluated, but the roadmap and architecture were too immature at that time. Also, the standardisation work for substation components was discussed and this work seemed to be also well suited to the use cases and requirements for wind power.

In 2004, the various parts of IEC 61850 started to be published. A Tissue (Technical Issues) database was created to handle errors, mistakes and inconsistencies in the standards.

In 2006, six parts of IEC 61400-25 (1: Introduction, 2: Data Model, 3: Exchange Model, 4: Mappings to Communication, 5: Conformance, 6: CMS Data Models) were published and the standards were also included in the Tissue system for maintenance.

To follow the IEC 61850 standard development, the working group for IEC 61400-25 started to work on Edition 2. The main goal was to correct any errors and thus make the standard much more workable and at the same time try to harmonise with IEC 61850. It was deliberately decided to postpone major changes regarding the basic structure of IEC 61400-25 with its "nested CDC", incompatible with IEC 61850, until development in other domain extensions of IEC 61850 such as hydropower and distributed energy resources would put sufficient focus on required expansion of IEC 61850. During the years 2015–2017, Edition 2 of the IEC 61400-25 was published.

From 2016 to 2020, the wind power standard was re-engineered from the bottom up. The extremely compact and database-friendly nested structure with arrays of historic values was scrapped as implementations were less than hoped for and standard SCADA clients and software tools lacked support for the wind functionality. Functionality was, and always had been, insufficient to efficiently model wind parks of hundreds of megawatts and thousands of alarms. Consequently, the focus was expansion of IEC 61850 alarm, counter and timer functionalities in order to be able to use standard IEC 61850 common data classes. This work was initiated in 2015 in the form of a joint TC88/TC57 IEC 61850-9018 alarm handling package with included alarm and counter common data classes. With initial circulation of IEC 61850-90-8, the third edition of IEC 61400-25 was issued in February 2021, including full harmonisation to IEC 61850.

16.4.3 Difference Between 61850 Systems and Wind Power Systems

IEC 61850 sub-system controllers are mostly embedded systems, with a limited storage capacity and thus not able to create all of the functionality required by customers. Often these systems have one single SCADA system to monitor and operate the substation. Sensors and signals are often monitored by this single SCADA system which then raises alarms if signals depart from normal operation. Also, historical logs of data are often created within a single SCADA system. To reduce the risk of data loss in case of disconnected communication lines for a period, simple logging and retrieval functions to catch up have been added in the IEC 61850 standard.

Wind power is different. Each wind turbine must be able to produce power independent of communication to a SCADA system, and thus, reporting and alarm handling must also be done at a turbine level.

A wind turbine can be seen as a single sub-system consisting of various embedded components, which work together with a central controller at a turbine level. This controller corresponds to the substation SCADA functionality regarding alarm handling and data logging.

At site level, a central SCADA system is often located to support the customer with power plant functionality based on the data from each wind turbine.

The trend is a continuous increase in the amount of data points from each wind turbine, typically around 50,000 unique data points per turbine. Together with an increase of turbines in a wind power plant, this results in a large amount of data to be handled by the site level SCADA.

Generally, customers require standardised access to real-time data and historical data, such that many wind power vendors are using a standard relational database for historical data storage. This gives great flexibility in the retrieval and calculation of data during retrieval by use of the SQL language. Often customers are offered a simple access to historical data by use of an ODBC connection, but it should be recognised that wind power use cases regarding historical data access are not supported in IEC 61850.

16.4.4 Modelling Approach of the Wind Information Model

The wind information model uses IEC 61850 logical nodes for organisation of real-time data into standardised objects in order to provide a robust and consistent overview for the users of the data.

The view is from a control or surveillance centre through a wind park controller with specific wind park functions for active (WAPC), reactive (WRPC) and frequency control (WHZW), using centralised containers for alarm status (WALM) and availability information (WAVL).

Whilst modelling inside the park is defined to IEC 61400-25, the boundary to IEC 61850 is defined as shown in Fig. 16.14. This approach provides sufficient granularity and functionality through IEC 61850 commands and metadata. The SCL language enhanced in IEC 61400-25-71 enables a process structure to describe entire wind parks and is used in the wind power domain for configuration.

16.4.5 Future Outlook

Security is not an inherent part of IEC 61850. It may be added, but it is not immediately obvious how this is achieved, and given the ever-increasing significance

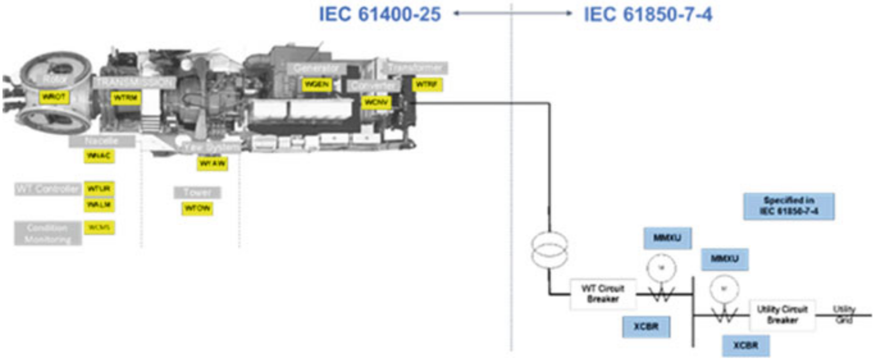


Fig. 16.14 Boundary between wind and substation information models. *Source* IEC 61400-25-2:2015 figure 3

of wind to global power systems, security is becoming an essential and inevitable part of the control of wind power plants.

A lack of a single communication profile agreement creates complications for vendors and customers. As an example, the IEC 61850 feature which offers remote configuration of data logging and statistical value calculation is generally implemented by OEMs, but not opened up for customers. Consequently, there is no standardised support for the statistical features in IEC 61850, which causes unnecessary complexity to the architecture. This lack of standardised support of access to historical data results means that generally only catch-up functionality is supported.

Given the difficulties with IEC 61850 integration, the current view of almost all OEMs and most wind park operators that the OPC Unified Architecture (OPC UA) will, if not already, become the standard approach in the wind industry. OPC UA has matured and has already been adopted widely by different industrial areas. In future, it is expected that the mapping of the wind information model will make full use of the functionality defined in OPC UA and that the modelling features of OPC UA will be utilised to implement the 61400-25 models. Use of the historical data support provided by OPC UA for database access is of specific importance. Due to the security features intrinsically built into OPC UA, it is expected that OPC UA will be the sole mapping for the wind information model in coming years. The highest priority for the IEC TC 57/TC88 Joint Working Group 25 is now the expansion of the OPC UA companion mapping standard to cover more than CDC mapping and include full protocol mapping support to realise this vision.

16.5 Distributed Energy Resources

16.5.1 Introduction

Modern power systems, particularly at distribution network level, are increasingly characterised by an array of generation, much of it renewable, and the need to manage a mix of distributed generation from diverse energy resources, as well as storage. This is accommodated within IEC 61850 by IEC 61850-7-420 [6], which specifically considers Distributed Energy Resources (DER). The defined DER logical nodes cover generic generators, reciprocating engines, fuel cells, converters including rectifiers and inverters, photovoltaic devices and arrays, combined heat and power systems, and battery systems, including chargers.

A specific, over-arching part of the standard was released as IEC 61850-90-7 "Object models for power converters in distributed energy resources (DER) systems" [7].

16.5.2 Photovoltaic Applications

Photovoltaic generation is covered as a DER application and provides for both individual PV modules, and a full PV array. The DVPM LN provides the ratings and characteristics of an individual PV module, whilst the DVPA LN gives the characteristics of the array r sub-array. There is then a PV controller LN, DVPC and the DTRC tracking controller, which provides the functionality to follow movement of the sun. Combined with the wider set of DER and other logical nodes, PV generation gives an excellent example, since logical nodes cover protection, switchgear, measuring, metering, converters, operational control and optimisation, energy storage, islanding and meteorological monitoring.

16.5.3 Battery Storage

Battery technology is one of the fastest-growing areas across power systems and is also set to form a core part of future electric traction technology, with battery trains emerging on several networks. An IEC 61850 battery model is already included within the DER model, defined by the ZBAT logical node. This allows detailed battery characteristics to be stored as well as measurement data for ongoing battery performance. The battery LN also aligns with the associated LN for a battery charger, ZBTC. It should be noted that the battery model was originally intended for use with auxiliary battery systems, rather than extensive storage arrays, and so it currently lacks the array-combining data model applied to photovoltaic systems, and also to fuel cells. However, the DER model for fuel cell stacks may be adapted for use in this area. A further part of the standard has been released in 2020 as IEC 61850-90-9, "Object models for electrical storage systems".

16.5.4 Fuel Cell Storage

The use of fuel cells also continues to grow appreciably across power systems, including the growth of hydrogen train technology. As for battery systems, a fuel cell model already exists within the DER model, but moreover consideration is given to fuel cell arrays or stacks, and a stack model is also included. The fuel cell LN is given by DFCL and stack LN by DSTK, respectively.

16.5.5 Ultra-Capacitor Storage

For very fast charging systems, ultra-capacitor technology is emerging as a potential alternative to, or as a technology in parallel with, battery systems. Traction ultra-capacitor systems have already been used to provide light urban rail energy with charging at each stop. The time characteristics of ultra-capacitors are significantly different to batteries during both charging and discharging. Nevertheless, as a functional device they exhibit similar characteristics to chemical batteries, and so the ZBTC model provides a means of modelling ultra-capacitors and providing ultra-capacitor monitoring in an overall energy system.

16.6 Electric Vehicles

16.6.1 Electric Road Vehicle Applications

As carbon reduction in transport continues apace across the globe, future power systems will increasingly need to meet a demand for electric vehicle charging, and of course with it, the challenge of night-time demand on distribution networks. At the same time, many vehicles will be in a state of partial or full charge whilst still connected to the network, and so the possibility of new uses for this storage by the network, as vehicle-to-grid (V2G) connections, will be developed in the coming decade. This is another area of advanced power system application which will be interdependent on developing an associated robust, and standardised, data network.

16.6.2 Existing IEC 61850 Integration

Electric vehicles, or e-mobility, are effectively considered an extension of the DER models of IEC 61850, set out initially in IEC TR 61850-90-8 [8] for incorporation into the DER standard 61850-7-420. New logical nodes for charging stations and vehicles are defined, as well as a wide range of coverage of operation of such systems. Figure 16.15 gives an overview of the e-mobility object model as defined in IEC 61850. The defining standard for the interface between charging station

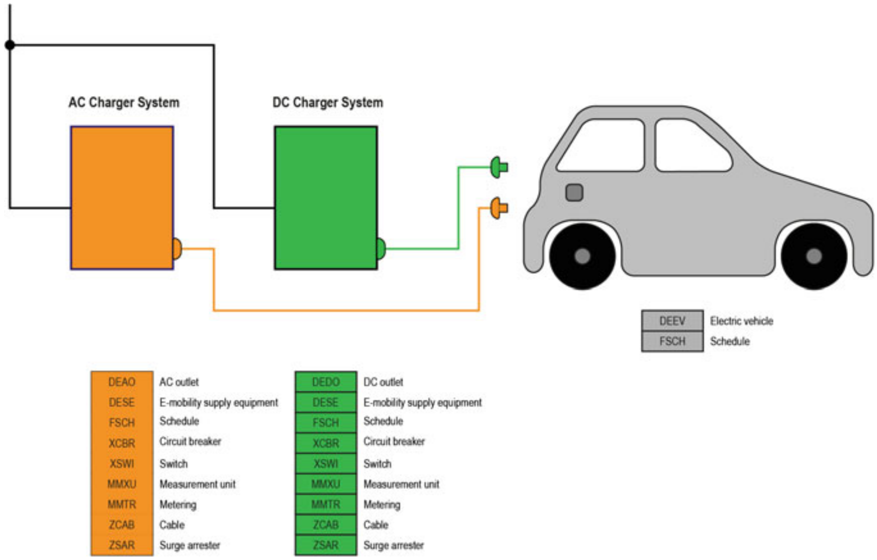


Fig. 16.15 Overview of IEC 61850 e-mobility object model

infrastructure and electric vehicles is IEC 61851 [9], and in addition, the vehicle-to-grid (V2G) communications interface is defined in ISO 15118-2 [10].

16.6.3 Vehicle-To-Grid

Vehicle-to-grid, or V2G technology, incorporates electric vehicle battery systems into overall grid system management, so that smart charging, and the use of vehicle batteries for grid demand response, becomes possible. Such technology is still developing, but as electric vehicles, and hence the connected capacity of vehicle batteries on grid systems, continue to grow then the constraints of charging from the network become greater. At the same time, the potential benefits of utilising the connected storage also become more significant, and so this is an area destined for significant development in coming years.

16.7 HVDC Systems

A typical HVDC system consists of at least two converter stations, with valves using either thyristor or IGBT device technology, and a connecting HVDC circuit. Given the wide range of available logical nodes across the application areas, the use of IEC 61850 for HVDC systems brings together existing subsystems. Converters, transformers and AC circuits may be monitored, controlled and protected from the range of AC logical nodes. Control is also dependent on communication between converter stations, and this is where IEC 61850 has found application in having a defined approach for synchrophasors, and the integration of existing PMU data for communication via IEC 61850.

16.8 Future Novel Network Integration

This chapter has described the range of IEC 61850 data models for networks beyond the predominant three-phase AC transmission and distribution systems. There may yet be some gaps still to cover in terms of full sub-system and component coverage in these models, but overall these are small, and there now exists a very wide range of interfacing models which can be used to bring renewable generation, energy storage, electric vehicles and traction systems into an IEC 61850 network. The future advantages of doing this will undoubtedly be considerable, and as such, IEC 61850 will surely be an enabling technology for integrated energy systems. In particular, the traditional boundaries between traction and vehicle systems, and power system networks may be expected to be diminished and removed. As a result, in the future electric railway systems, light rail and urban mass transit systems, electric road vehicles through heavy goods vehicles to cars and even electric bicycles may be expected to be considered part of the wider power system data network and overall energy architecture of the future.

The use of V2G technology has been discussed. Beyond this, however, there are wider possibilities. In the conventional traction power system, protection systems at the substations are required to be selective and avoid traction load trips, whilst covering all possible faults on the traction system. As traction load grows, this often requires additional substations to provide shorter sections. The concept of the load moving, and being connected to the feeder, does not align with conventional feeder protection concepts and, to take an example, would rule out the use of differential protection.

This traditional approach, with substations independently attempting to discriminate between load and faults, and dealing with the problem of a load along a feeder, limits the capacity of the network, and therefore the transport system. However, consider Fig. 16.16. This shows part of the IEC 61850 object diagram, with UML representations of Substation, Voltage Level and Bay. The Substation is considered to be a fixed installation, but in a conceptual extension it need not be. By adding a descendent of the Substation object, as a Dynamic Substation, there could be a future concept in which substations, with all of the normal IEC 61850 functionality and attributes of substations, may be added and removed dynamically to a network. If this were possible, then there would exist a mechanism to create a Train object as a type of Dynamic Substation. By taking this approach, and extending the network and communication system architecture to trains, the train fully becomes part of the power system network. It can be modelled as a dynamic substation and contains many elements of substations, including transformers, protection, metering and converters.

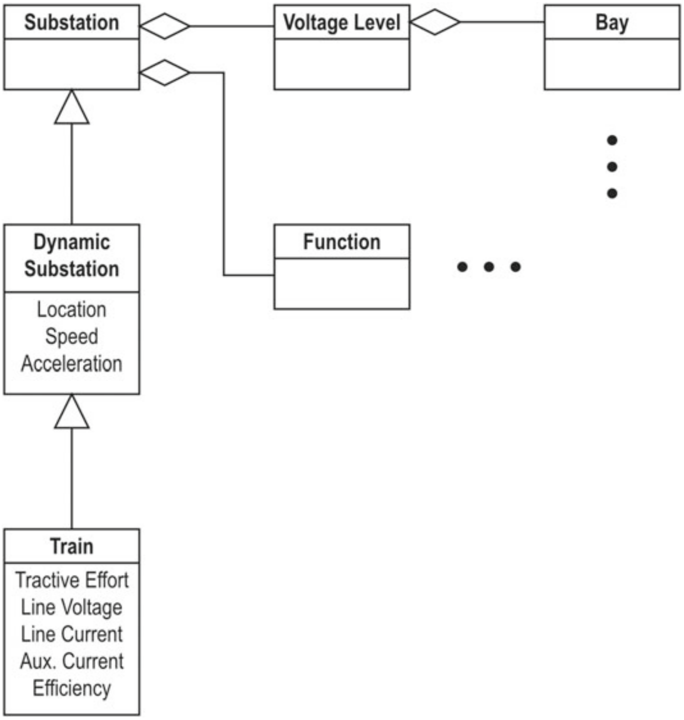


Fig. 16.16 Dynamic substation concept for traction vehicles

By bringing the train into the overall network model, it is now possible not only to assess train faults from the wider network, but also now to consider a three-terminal digital differential protection approach in which traction system faults may be more readily determined, and the location more quickly determined. The result is a more reliable, and higher performance, transport system, but all enabled by the extended application of IEC 61850. Inherent in this is the requirement for wireless communication within the overall power system network, and the concept that logical nodes may not have to be predefined, but may present dynamically to an existing network, and likewise remove themselves from an existing network. This is but one of many possible directions of novel development of IEC 61850, but demonstrates that the most significant changes may be yet to occur.

This chapter has taken a snapshot of novel uses of IEC 61850 and shown how the technology is enabling far wider system change than merely the replacement of conventional protection and control schemes. Each of these areas of development is significant active areas of research and development, and so a single chapter cannot realistically cover the range and depth of all of these applications. Nevertheless, this snapshot provides a view of the expanding and integrating nature of IEC 61850. In providing a single, integrated, communications architecture for power systems, the standard is bringing together the most diverse elements of energy networks, and in doing so is enabling the intelligent, deeply integrated energy networks of the future.

References

1. European Committee for Electrotechnical Standardisation (CENELEC): Railway applications. Fixed installations. Protection principles for AC and DC electric traction systems. Ref. EN 50633:2016, August 2016
2. International Electrotechnical Commission (IEC): Communication networks and systems for power utility automation. Part 7-410. Basic communication structure. Hydroelectric power plants. Communication for monitoring and control. Ref. IEC 61850-7-410:2022, February 2022
3. International Electrotechnical Commission (IEC): Communication networks and systems for power utility automation. Part 7-510. Basic communication structure. Hydroelectric power plants. Modelling concepts and guidelines. Ref. IEC/TR 61850-7-510:2012, April 2022
4. International Organisation for Standardisation (ISO)/International Electrotechnical Commission (IEC): Industrial systems, installations and equipment and industrial products. Structuring principles and reference designations, ISO/IEC 81346, 2010–2021
5. International Electrotechnical Commission (IEC): Wind energy generation systems. Communications for monitoring and control of wind power plants. IEC 61400-25, 2015–2021. Copyright © 2015 IEC Geneva, Switzerland. www.iec.ch
6. International Electrotechnical Commission (IEC): Communication networks and systems for power utility automation. Part 7-420. Basic communication structure. Distributed energy resources and distribution automation logical nodes. Ref. IEC 61850-7-420:2021, November 2021
7. International Electrotechnical Commission (IEC): Communication networks and systems for power utility automation. Part 90-7. Object models for power converters in distributed energy resources (DER) systems. Ref. IEC/TR 61850-90-7:2013, March 2013
8. International Electrotechnical Commission (IEC): Communication networks and systems for power utility automation. Part 90-8. IEC 61850 object models for electric mobility. Ref. IEC/TR 61850-90-8:2016, April 2016
9. International Electrotechnical Commission (IEC): Electric vehicle conductive charging system. Ref. IEC 61851, 2014–2021
10. International Organisation for Standardisation (ISO): Road vehicles. Vehicle-to-Grid Communication Interface. Network and application protocol requirements. Ref. ISO 15118-2:2014, 2014

Conclusions 17

Peter Bishop, Nirmal-Kumar C. Nair, and Rod Hughes

Abstract

This chapter concludes this Green book on IEC 61850, the very first comprehensive compact book from CIGRE B5-Protection and Automation Study committee of CIGRE International. It summarises the main contributions of the 16 Chapters that have been progressively arranged. It identifies the future challenges and opportunities for enabling widespread adoption of IEC 61850 based systems and technologies globally.

Keywords

IEC 61850 overview • Summary of concepts and implementation • Future challenges

17.1 Overview

The purpose of this Green Book is to provide a practical compact study on IEC 61850 principles and applications to electric power systems using CIGRE Technical Brochure and technical paper documents that are based on existing practice.

P. Bishop (✉)
Transpower NZ Ltd., Wellington, New Zealand
e-mail: peter.bishop@transpower.co.nz

N.-K. C. Nair
University of Auckland, Auckland, New Zealand
e-mail: n.nair@auckland.co.nz

R. Hughes
Rod Hughes Consulting, Aberfoyle Park, SA, Australia
e-mail: rgh@rodhughesconsulting.com

P. Bishop and N.-K. C. Nair (eds.), *IEC 61850 Principles and Applications to Electric Power Systems*, CIGRE Green Books, https://doi.org/10.1007/978-3-031-24567-1_17

It is intended to give stakeholders from different disciplines and levels of knowledge and understanding of systems in use, their features, how they are applied and approach for planning, design and implementation. The standard and indeed this Green Book should be considered along with other key-associated standards such as:

- IEC 60255 series broader protection function requirements,
- IEC 61869 series for instrument transformers as applied for current and voltage sensors under the overall IEC 61850-9-2 Sampled Value definitions,
- IEC 62771 for high-voltage switchgear/controlgear digital interfaces,
- IEC 61400 for wind farms,
- IEC 61588 for precision clock synchronisation protocol for network measurement and control systems,
- IEC 62439 industrial communication networks—high-availability automation networks.

IEC 61850, the international standard applicable to the engineering and implementation of protection, automation and control systems, has continued to evolve since it was introduced in 2004 and is being applied across the power system in a wide range of applications. IEC 61850-based systems provide users with the opportunity to review primary and secondary functionalities they wish to implement and their existing philosophies, not just in the area of communications but in all areas of existing and emerging power systems. These changes will impact on many areas such as primary system design, protection design, SCADA design, system architecture, governance, operational work and field commissioning. It is crucial that all involved are not only aware of its capabilities (and are exposed to the changes IEC 61850 may make), but also have the ability to understand where they fit in and feedback their experience, ensuring the maximum benefit of any changes.

IEC 61850 has the features and conveys benefits to meet the challenges of our changing and emerging power systems and to provide better solutions to traditional power system protection and automation. Instead of individual copper cables, the communication between substation IEDs can be realised using digital communication over an Ethernet Local Area Network. This can provide both cost and effort savings for utilities, in particular, the aspect of the time and cost to install, test and commission the wire-based schemes. Other benefits also include some simplifications of protection and automation schemes as the Local Area Network can be used in a more optimised way for signalling between substation IEDs. This may help to economically justify some improvements in substation protections and automation schemes such as adding new functions and more redundancy to reduce the risk of critical failures, guarantee safe operation in degraded conditions and increase system availability that would not be feasible in wire-based schemes.

The purpose of the IEC 61850 standard can be said to provide.

> A defined engineering process with defined tools for different roles at different stages, with defined files to exchange engineering information between the tools using defined data models and defined communication services for the configuration of the IEDs and functions to communicate interoperably over industry standard protocols and networks

Ultimately, the success of an IEC 61850 implementation starts with specification of requirements: for the system as a whole, for the functions to be provided, for the IEDs that need to be procured to satisfy all of that. The experience shows that if a function does not work the way it was expected, the first point to check is the completeness and depth of the specification. It is important that users take time to consider and specify their requirements to ensure IEC 61850 systems meet their needs. The specification should focus on functionality, performance, reliability, evaluation, project management and services to enable a fair participation and evaluation of the bidders. It should also provide all the functions that are required and incorporate compatible communication interfaces. This book explains the different types of functions, specification of standard schemes plus tools and documentation for engineering.

With the IEC 61850 LAN-based systems, many user selectable options exist for network architectures and associated services. Aspects discussed include communication network architectures, time synchronisation services, cybersecurity integration. Considerations, present practices and specific use case examples have been included in the book. However, with learnings on present practices and new technology being developed, new features and practices in these areas are being developed and solutions are emerging. The planning and design considerations for a complete IEC 61850 system lifecycle tend to be very different to traditional wire-based systems and impact on existing utility processes. New utility processes and approaches may be needed for aspects such as architecture, security, documentation, testing, commissioning and maintenance. The book explains considerations and steps involved with planning and designing IEC 61850 systems across their lifecycle, from evaluation of benefits and impacts on company procedures to selection of functionality and network requirements in the design to commissioning and maintenance features.

A wide range of IEC 61850-based functional schemes involving both GOOSE and sampled value messaging have now been implemented between devices in a substation and externally. The book explains implementation considerations and includes examples. With multi-vendor interoperability being a key goal of the standard, expectations and aspects to ensure this are explained and covered in examples.

Testing and commissioning is important to ensure that a system operates as intended, ensuring its reliability and security. Particularly with fibre-based Ethernet network and the use of sampled values, IEC 61850 systems require a different test approach compared to transitional wire-based systems. This Green Book covers typical test considerations, test methods and tools.

The main aspects related to asset management include useful life, performance management, risk management, maintenance processes and asset information collection. An important difference with IEC 61850 PACS asset management compared to asset management in general is that the built-in intelligence of the PACS can be used to easily provide status information on the assets in operation. Asset owners can monitor performance, history, availability in real time and apply preventive maintenance policies with greater security.

During the first 15 or so years of the life of the standard (2002 to 2017), most implementations have mainly focused on protection functions and SCADA implementations. Notably, wind, hydro- and "distributed energy resources" were already incorporated in the standard. However, since 2017, there has been a significant expansion in the extent of deployments particularly in regards to Sampled Values and indeed the use of so-called top-down engineering processes starting with the SSD file. There is much more to come in both the standard itself and the range of applications, as reflected in the change from the original title "Communication networks and systems in substations" to "Communication networks and systems for power utility automation". Although the title refers to "power utility", this is not sufficiently broad enough to encompass any electrical infrastructure automation, e.g. the mechanical operation of wind, hydro-, DER and for example in applications in end-user industrial and mining contexts. While this book will remain as a basis of consideration of general practical implementation, the future of IEC 61850 as at the time of writing this book includes the following,

- Edition 3 and beyond
- Logic modelling
- IED procurement specification SCL files
- Revenue metering
- The "digital substation"
- Wide area systems
- Solar photo-voltaic models
- "Grid battery" systems
- Distribution "pole top" applications
- Remedial action systems
- Intelligent switchgear
- Industrial automation interface
- Domestic solar and battery integration
- Electric vehicle management
- Enabler of low-power (a.k.a non-conventional) instrument transformer CT/VT
- Smart grid and "big data" enabler
- Increased "as operating" asset management information
- Automated SCL-generated test plans

17.2 Summary

This section summarises the contributions from the 16 chapters of this book using the activity themes defined in the preface.

17.2.1 Needs, Benefits and Concepts

Chapter 1 identifies the backdrop of broader electrical power system infrastructure issues and drivers that require new technology deployments and investment to address more flexible, economic, reliable and resilient network operations. These include changes in society composition, environment, technology and social licence that impacts power and energy use. It further describes the operating environment challenges like climate change, utility challenges, technology proliferation and expectations from society. CIGRE's ten issues to address network supply system of the future have also been described. Thereafter, it introduces IEC 61850 that helps provide some answers to the above drivers and challenges for protection, automation and controls systems (PACS).

Chapter 2 outlines the history of this standard, its motivations and explains basic concepts. It begins by the conceptual drivers behind the IEC 61850 series of standards for PACS. Detailed timeline on the history of this development and initial 14 parts followed by the additional parts, editions, amendments, forward and backward amendment compliance and the role of training have been described.

17.2.2 User Specification, Architecture and Services

Chapter 3 identifies the typical functions that could be defined as specification standards by utilities for IEC 61850 PACS systems. A typical specification process outlining scheme template, definition, application, instantiation is firstly described. Thereafter, specification tools for the engineering process and the various IEC 61850 files like SCL, SCD, ICD, CID, SSD, SED, ICD, SST are defined and described. The documentation of these engineering stages has been thereafter described in detail. The chapter ends with identification of various end-user groups from transmission, generation, other learned bodies like IEEE PSRC and user feedback groups, who have been active over the past 15 years or so. These groups have been very useful to have IEC 61850 system sharing opportunities through workshop, conferences and developmental activities.

Chapter 4 introduces and explains the station bus and process bus of PACS. It describes the PRP and HSR architectures of the IEC 61850 system and explains the various well-known services like GOOSE, MMS, SV, etc. This provides good learning material for well-established features and deployments of IEC 61850 PACs systems across the world.

17.2.3 Time Synchronisation and Cybersecurity Aspects

Chapter 5 starts off with the definition of the synchronisation and follows it up with accuracy needs, availability of reference clocks and performance testing. It is a deep dive into time synchronisation needs from a PACS viewpoint which is one of the onerous and exacting requirements for digital substations.

Chapter 6 discusses cybersecurity imperatives across electricity networks broadly. It identifies certain aspects worth considering for IEC 61850 systems, recognising the fact that relay IEDs are categorised under Operational Technologies rather than general Information Technologies (IT) that are used across the business and other operational views and applications. The perspective from CIGRE D2 which looks broadly across information systems and telecommunication presents this view. There have been some joint D2/B5 working groups and technical brochures which informs the presentation of this chapter.

17.2.4 Planning and Design

Chapter 7 outlines the step-by-step process that needs to be followed by a utility. The impacts on yard equipment, control room and utility operations have been identified at the start of this chapter. It then proceeds with revisiting the project steps and definitions for deploying IEC 61850 followed by sections on selection of uncertainties, requirements, communication network, network requirement, time synchronisation, cybersecurity considerations, certification and homologation requirements of the engineering processes. It also identifies the complete project cycle from installation, commissioning, maintenance and decommissioning/retirement for IEC 61850 systems within utilities.

17.2.5 System Implementation and Testing

Chapter 8 starts off with well-documented recommendations for realising IEC 61850 schemes in actual practice. This is done systematically by describing the semantics of logic, logical device grouping, instance modelling and optimising datasets associated with multiple logic node instances associated with a particular scheme. The exemplar of a large utility is then shared for their IEC 61850 PACS model with a few functional examples. Other functional exemplars for SCADA/automation application, transparent interlocking and primary distribution substation bus transfer functional scheme are detailed through the rest of this chapter showcasing how IEC 61850 functional schemes can be implemented.

Chapter 9 outlines the testing requirements, tools, methods and their important features. This chapter has been compiled using CIGRE technical brochures, developed by many experts in various working groups.

Chapter 10 extends Chapter 9 with focus more on assuring vendor interoperability from viewpoint of IEDs from different manufacturers. This chapter has outlined several practical utility case studies. It looks at interoperability considerations at various lifecycle stages and recommends measures to help ensure interoperability.

17.2.6 Sampled Value and Process Bus Applications

Chapter 11 outlines the digital data acquisition chain, particularly relevant for developing PACS implementation. It captures nicely the development and trends of the latest requirements to ensure reliable and accurate measurement of primary currents and voltages. The characteristics of instrument transformers, Rogowski coils and the assessment of the frequency dependence of these new sensor technologies through bode plot assessment have been described in detail. The dynamic range for measurements has also been illustrated. The role of future developments like travelling wave has been described in this chapter.

Chapter 12 illustrates through actual projects the substation architecture options available and those actually deployed. Some real-life examples from across the world have been richly described, some of which have been presented and published previously through CIGRE publications and brochures. The choice of PRP and HSR has been discussed and emerging trends of software-defined network identified. Some recommendations have also been identified, based on utility experience of deploying process bus applications.

17.2.7 Inter-substation and SCADA Applications

Chapter 13 identifies the synergies of PMU deployments and development around sample value implementation. It starts with synchrophasor concepts, communication, timestamp and potentially deploying R-GOOSE for centralised remedial action schemes and multi-terminal transfer trip. Other innovative wide area visualisation and monitoring examples have been identified. Some special applications like oscillations monitoring and fault location are also illustrated.

Chapter 14 explores the integration of IEC 61850-based PACS systems towards the control centre and IT systems of transmission Energy Management Systems and Distribution Management systems. It highlights some possibilities in future.

17.2.8 Maintenance and Asset Management of IEC 61850 Systems

Chapter 15 is a targeted chapter that outlines the typical scope of how IEC 61850 systems that are being deployed could be maintained and how their asset management cycle can be managed alongside typical processes used for other substation equipment and devices. It also draws from working group documents, technical brochures and utility documentation around this and provides good information for utility readers to better understand how they can handle IEC 61850 systems.

17.2.9 Applications Beyond Substations

Chapter 16 is an interesting chapter that captures the non-traditional use of this standard. The use of IEC 61850 for electric traction systems has been described at length and is mature in its usage for the example illustrated in this chapter. Other use of this in hydro-plant control, wind power plants, distributed energy resources, HVDC networks and electric vehicle charging infrastructure has also been identified.

17.3 Future Challenges

Some areas of challenge (where future development is required) have been identified in the book, most of which is under consideration by the IEC TC57, WG10. The IEC 61850 series of documents and associated engineering tools are continuing to evolve with more and more experience and capabilities. Cybersecurity is important and requires being up to date with mitigations and requirements to response to future threats. Work is required on making sampled value systems suitable for high-frequency travelling wave and resonant earthed applications.

Chapter 13 highlights the expanding range of applications and the potential for the future. Applications from remedial action schemes to demand-side management and state estimation (that may be used to detect and initiate remediate incipient failure modes on the grid) are discussed. Other applications beyond the substation are also growing. Chapter 16 discusses the existing wide range of applications and their benefit beyond the substation, including traction systems, HVDC and electric vehicles.

Applying the standard to any system engineering and implementation requires that protection specialists, and others must acquire new technical knowledge and skills. Specific competency development programmes must be worked through to train utility staff in the concepts, jargon, processes and detail of the standard. Associated with this development is training on the complex tools which give users the capacity to configure, test and commission these new protection schemes based on IEC 61850.

For going further into the implementation journey, a book does not replace the need for coming to a thorough understanding of the standard itself or to study reference material that aids in that understanding and references “good industry practice”. CIGRE has been a key contributor to the body of knowledge with several technical brochures identifying “good industry practices” and many papers at many worldwide events discussing implementation experiences. Reference is made to Appendix A Bibliography and References. Many of these documents are also specifically referred to in-associated Green Book chapters.

Bibliography and References

A

Standards

Standards organisation	Standard number	Title	Web link
IEC	IEC 61850[a]	2010: Communication networks and systems for power utility automation ~~2002: Communication networks and systems in substations~~	https://webstore.iec.ch/
IEEE	IEEE 1686:2007	Standard for substation intelligent electronic devices (IEDs) cyber security capabilities	https://standards.ieee.org/
ISO			
IEC	IEC 62351-6:2019	Power systems management and associated information exchange—data and communication security—Part 6: security for IEC 61850	https://webstore.iec.ch/
IEC	IEC 62439-2:2016	Industrial communication networks—high availability automation networks—part 2: media redundancy protocol (MRP)	https://webstore.iec.ch/
IEC	IEC 62439-3:2016	Industrial communication networks—high availability automation networks—part 3: parallel redundancy protocol (PRP) and high availability seamless redundancy (HSR)	https://webstore.iec.ch/

P. Bishop and N.-K. C. Nair (eds.), *IEC 61850 Principles and Applications to Electric Power Systems*, CIGRE Green Books, https://doi.org/10.1007/978-3-031-24567-1

Standards organisation	Standard number	Title	Web link
IEC	IEC 61850 TISSUES	Database of technical issues related to IEC 61850 standard	https://iec61850.tissue-db.com/default.mspx
IEC	IEC 61869-9:2016	Instrument transformers—part 9: digital interface for instrument transformers	https://webstore.iec.ch/
IEC	IEC 61400-25-1:2017 IEC 61400-25-2:2015 IEC 61400-25-3:2015 IEC 61400-25-4:2016 IEC 61400-25-5:2017 IEC 61400-25-6:1016 IEC 61400-25-71:2019	Wind energy generation systems—communications for monitoring and control of wind power plants Overall description of principles and models information models Information exchange models Mapping to communication profile Compliance testing Logical node classes and data classes for condition monitoring Configuration description language	https://webstore.iec.ch/

Note [a]The first series of core parts of IEC 61850 was issued in 2002–2004. Since then, some parts have been issued as Edition 2 and some as Edition 2.1. Other parts have only been issued as Part 1, and other parts are still in development. It is therefore important to always reference which edition is being referred to. Equally, it is important to have access to older editions of the same part as there are many in-service IEDs that only comply to Edition 1 and hence may have different functions or implementation (e.g. allowable use of GGIO Logical Node or other TISSUES)

CIGRE Technical Brochures

http://www.e-cigre.org/

Staff of CIGRE member organisations and individual members can always download the PDF for free under strict copyright distribution restrictions.

Hard copy documents are generally around 100–150 Euro.

Note: Non-CIGRE members may now access and download free of charge all CIGRE publications (Electra and technical brochures) that have been published more than three years ago.

TB#	Year	Title
246	2004	The automation of new and existing substations: why and how
326	2007	The introduction of IEC 61850 and its impact on protection and control in substations

TB#	Year	Title
329	2007	Guidelines for specification and evaluation of substation automation systems
401	2009	Functional testing of IEC 61850 based systems
404	2010	Acceptable functional integration in HV substations
419	2010	Treatment of information security
427	2010	The impact of implementing cyber security requirements using IEC 61850
464	2011	Maintenance strategies for digital substation automation systems
466	2011	Engineering guidelines for IEC 61850 based digital SAS
507	2012	Communication architecture for IP-based substation applications
540	2013	Applications of IEC 61850 standard to protection schemes
603	2014	Application and management of cybersecurity measures for protection and control
615	2015	Security architecture principles for digital systems in electric power utilities
628	2015	Documentation requirements from design to operation to maintenance for digital substation automation systems
629	2016	Coordination of protection and automation for future networks
711	2018	Control and automation systems for electricity distribution networks of the future
740	2018	Contemporary design of low cost substations in developing countries
760	2019	Test strategy for protection, automation and control (PAC) functions in a full digital substation based on IEC 61850 applications
768	2019	Protection requirements on transient response of digital acquisition chain

CIGRE continues to develop further technical brochures through its working groups https://www.cigre.org/article/GB/cigre-active-working-groups.

WG#	Commenced	Title
WG B5.50	2012	IEC 61850-based substation automation systems—expectation of stakeholders and user interaction
WG B5.51	2012	Requirements and use of remotely accessed information for SAS
WG B5.56	2015	Optimization of protection automation and control systems
JWG C6/D2.32	2015	Utilization of data from smart meter system
WG B5.59	2016	Requirements for near-process intelligent electronic devices
WG D2.43	2016	Enabling software-defined networking for electric power utilities' telecom applications
WG D2.44	2017	Usage of public or private wireless communication infrastructures for monitoring and maintenance of grid assets and facilities
WG B5.60	2017	Protection, automation and control architectures with functionality independent of hardware
WG B5.63	2017	Protection, automation and control system asset management

WG#	Commenced	Title
WG B5.64	2017	Methods for specification of functional requirements of protection, automation, and control
WG B5.66	2017	Cyber security requirements for PACS and the resilience of PAC architectures
JWG D2_C2.48	2018	Enhanced information and data exchange to enable future transmission and distribution interoperability
JWG B5 D2.67	2018	Time in communication networks, protection and control applications
WG D2.46	2018	Cybersecurity future threats and impact on electric power utility
JWG B2/D2.72	2019	Condition monitoring and remote sensing of overhead lines

CIGRE Papers and Contributions

The subject of IEC 61850 covers a wide range of applications with electricity infrastructure. CIGRE provides various international and national events where papers are presented and audience contributions discuss their experiences.

Year	SC#/NC	Reference #	Title	Papers
2004	SC B5	Preferential subject 1	The use and benefits of information technology (IT) in substation automation, protection and local control	13 papers, 33 contributions
2005	SC B5	Preferential subject 2	Specification and evaluation of substation automation systems	15 papers, xx contributions
2007	SC B5		Acceptable functional integration in substation P&C for transmission system	21 papers, 42 contributions
2008	SC B5	Preferential subject 2	Impact of process-bus (IEC61850-9-2) on protection and substation automation systems	6 papers, 29 contributions
2010	SC B5	Preferential subject 1	Protection, control and monitoring for the next decade	17 papers, 59 contributions

Year	SC#/NC	Reference #	Title	Papers
2012	SC B5 SC B5	Preferential subject 1 Preferential subject 2	Impact of future network components on coordination of protection and automation systems Utilization and application of remote access for protection and automation systems	19 papers, 54 contributions 11 papers, 36 contributions
2014		Preferential subject 2	Expectations from stakeholders about IEC 61850	11 papers
2017		Preferential subject 1	Challenges of design and maintenance of IEC 61850 based systems	30 papers, 35 contributions
2018		Preferential subject 2	User experience and current practice with IEC 61850 process bus	16 papers, 63 contributions
2019		Preferential subject 2	Time in protection applications—time sources and distribution methods	19 papers, 36 contributions
2020		Preferential subject 2	Communications networks in protection, automation and control systems Pacs: experience and challenges	23 papers

CIGRE Papers

Tittle	Summary	Publication no.	Year
Experience of implementation, testing and operation of electronic instrument transformers, merging unit devices, power-system protection and automation devices realizing IEC 61850 process bus for the generator-transformer unit of Nizhegorodskaya HPP	The report presents the results of the factory acceptance tests and of the system acceptance tests at the hydropower plant, of trial operation and maintenance, which were carried out during 2015–2017 on the operating equipment of the generator-transformer unit of Nizhegorodskaya hydropower plant. The analysis of experience of implementation, testing and operation of electronic instrument transformers, merging unit devices and power system protection and automation devices realising the IEC 61850-9-2 process bus and the IEC 61850-8-1 station bus is also given. The presented results reflect the unique experience of implementing the requirements of the IEC 61850 standard for elaboration of protection and control systems of generating equipment	B5-216	2018
Experience feedback of testing and commissioning of a fully digital IEC 61850 based PACS	This paper describes a part of the experience feedback gained during the project. The challenges identified or encountered during the preparation and execution of qualification tests, factory acceptance tests (FAT) and site acceptance tests (SAT) and their mitigation are discussed. These challenges include tests of functions using sampled values (SV), FAT and SAT strategies for LPIT, interoperability issues under non-nominal operation conditions, testing of functions requiring global time synchronisation and tests to verify the robustness of functions in case of perturbations of the process and station bus	B5-215	2018
Design, concept, commissioning, maintenance, cyber security of a IEC61850 process bus brown field application	The paper shares the used tools and processes for protection and substation automation engineers working with IEC 61850-9-2 to prove a stable operation of the protection relays and merging units as a protection system. Steps that can be followed to ensure secure operations of a process bus implementation are also offered	B5-213	2018
Operational experience of IEC 61850 process bus systems deployed in POWERGRID, India	This paper discusses the performance evaluation studies conducted on the pilot project of process bus at Bhiwadi substation of POWERGRID	B5-211	2018

Tittle	Summary	Publication no.	Year
Experience with process bus in Statnett R&D project digital substation	Statnett has started an R&D pilot project related to digital substation automation and protection system (DSAS) based on IEC 61850-9-2 process bus. The process bus-based DSAS pilot (hereafter named “pilot project”) is installed in a live 300 kV line bay in parallel with an already existing substation automation and protection system (SAS). The objective of the pilot project is to gain experience with non-conventional instrument transformers. The experience gained during factory acceptance test (FAT) and site acceptance test (SAT) is included in this paper. The paper will also include some experience related to interoperability between solutions from different vendors due to options and flexibilities in the IEC 61850 standard	B5-203	2018
Implementation of digital substation automation systems in Brazil—challenges and findings	This paper describes the current state of the digital substation automation system (DSAS) implementation process, the possibilities of the projects to be implemented and the applications already made in Brazil. It also describes the main strengths and weaknesses of the DSAS implementation processes	B5-201	2018
IEC 61850 experiences and expectations from the renovated substations project in MEA’s distribution system substation	Metropolitan electricity authority (MEA) has been renovating existing substations with IEC 61850. The renovation is finished for thirteen substations and still 37 substations to go. In addition, MEA has already set a budget and been revising the SA technical specification for additional 40 substations intending to support MEA’s smart grid plan. MEA also hopes that IED capabilities recommendation and IED classifications will be available for avoiding procurement mistakes. This paper presents our experiences and expectations that MEA would like to share and discuss	B5-213	2014
IEC 61850 and distribution network utilities perspective: trials, tribulations and experiences from New Zealand	This paper revises the journey of IEC 61850 for NZ distribution networks primarily from the viewpoint of users. It will also provide insight into the existing tools, documentation and in-house developed standard practices and identify the role of help received from IED vendors and other IEC 61850 resource personnel. Challenges around testing and training of contractors towards these deployments in the network will also be highlighted	B5-212	2014

Tittle	Summary	Publication no.	Year
Increasing interoperability by IEC 61850 profiling—requirements and experience from end-user and vendor prospective	The paper gives an overview of past and ongoing activities of standardisation and industry user groups related to IEC 61850 interoperability. The basic definition of interoperability terms is given as well as an introduction of standard profile in general and in context of IEC 61850 and CIM. The main focus of the paper lies on the idea of standard profiling of IEC 61850. Based on the analysis of requirements and expectations of users, system integrators and vendors the requirements for IEC 61850 profiling are derived. It turned out that profiling poses the challenge to find the balance between profile restrictions and profile flexibility	B5-207	2014
The integrated tool for substation automation system based on IEC61850	Compared to the testing of conventional SAS, it usually takes the staff more time to test the SAS based on IEC 61850. In order to deal with these issues, it is necessary to develop an integrated tool that covers the complete data flow in SAS based on IEC 61850. A new description method of the secondary circuit is provided. The requirements of the tool are analysed in detail in this paper. The integrated tool increases the staff's work efficiency and makes it easy to implement SAS based on IEC 61850. A scheme of the integrated tool for SAS based on IEC 61850 is proposed in this paper. The tool has been implemented and used in China's projects	B5-205	2014
Brazilian utilities experience in acceptance, commissioning and maintenance testing techniques for protection and automation systems based in IEC-61850	The paper will address the changes and new practices from the point of view of electric utilities, with respect to testing procedures in various stages of implementing protection and automation systems based on IEC 61850. This work is the result of the contributions made by the Brazilian mirror group of WG B5.45: acceptance, commissioning and field testing techniques for protection and automation systems It will examine various aspects of the conformance tests (including interoperability tests), homologation or qualification tests, factory acceptance tests (FAT including interoperability tests), site acceptance tests or commissioning and maintenance tests	B5-203	2014

Tittle	Summary	Publication no.	Year
Substation to control centre communication based on IEC 61850: requirements, concepts and practical experiences	Featuring object-oriented data models and a standardised configuration language, IEC 61850 represents the state-of-the-art communication standard for substation automation systems. In order to overcome the limitations of those legacy protocols in terms of data conversions, elaborated data exchanges and proprietary configurations and to foster the use of a seamless object-oriented communication, IECTC57 is extending the current IEC 61850 specification to close the gap between substations and control centres. The paper gives an introduction into the topic and presents the relevant use cases and derived requirements. Furthermore, it discusses communication and modelling aspects in regards of the use case-specific requirements. These concepts are evaluated against industrial power system operator needs. Foreseen consequences for standardisation and practical realisation of projects are identified	B5-203	2012
Utility experience and future expectation from sub-station automation system based on IEC 61850	After introduction of IEC 61850 which is a standard for communication systems in the substation, POWERGRID has started specifying substation automation system (SAS) with state-of-the-art communication technology conforming to IEC 61850 since year 2003. Presently, more than 50 substations equipped with substation automation system have been ordered for implementation. In the paper, we discuss the specification of POWERGRID in brief, the reason of going for substation automation and their implementation. The issue of configuring the IEDs for IEC 61850 application through various configuring software from different vendors and their limitation to configure the other supplier's IEDs are also discussed	D2_B5_112	2010
Specifications, requirements and experiences using IEC 61850 in the Ibero-American region	The different experiences developed into the Ibero-American region; during the 2006 session of CIGRE, it was decided to start a joint working group in the scope of the RIAC, the Ibero-American region of CIGRE, formed by specialist of the B3, B5 and D2 study committees. The paper presents the finding of the JWG and the conclusion arisen form the experiences gathered during the development of the work	D2_B5_107	2010

Tittle	Summary	Publication no.	Year
Practical experience with IEC 61850 multivendor systems and foreseeable future applications—a system integrator and end-user perspective	In the paper, the authors, based on experience in Europe and South America, propose to establish and classify the current praxis in the application of IEC 61850 in multivendor systems by describing common physical and logical architectures as well as reporting on multivendor functional and engineering interoperability. The main conclusion is that IEC 61850 as a communications standard is solid, and its immediate cost and simplification benefits are effective. Notwithstanding there is still much untapped potential in the industrial application of the standard, achieving communication interoperability within the IEC 61850 system is viable, but functional integration and advanced engineering is still below what could be achieved, particularly in multivendor applications	D2_B5_103	2010
BHEL experience in implementation of IEC 61850 based sub-station automation system in India	BHEL has carried out implementation of IEC 61850-based SA systems for the various power generation and transmission utilities in India. Utilities in India have adopted the IEC 61850 technology in various ways. The paper brings out the variations in specifications and implementation methodologies adopted in the country. Starting from very basic implementations of IEC 61850-based SA systems, the Indian utilities have evolved to increasingly more and more functionalities	D2_B5_102	2010
Functional and interoperability tests using the IEC 61850 standard applied to substations—research and development in Brazil	The present paper focuses in the development and installation of a test laboratory for protection and automation of electric systems at the Rio de Janeiro State University—UERJ	B5-209	2008
A Practical IEC61850-9-2 process bus architecture driven by topology of the primary equipment	This paper presents a practical process bus architecture conforming to IEC 61850-9-2 that fits the task of protection and control of substations by drawing from the universal topology rules of substations	B5-105	2008
Process bus: experience and impact on future system architectures	Process bus defined with IEC 61850-9-2 is still largely unexplored. IEC 61850-9-2 is the part of the standard that brings non-conventional instrument transformer technology (NCIT) into play, breaking the shackles and constraints of conventional CTs and VTs with iron wound cores at their heart The purpose of this paper is to review the challenges, explain the results of pilot projects and identify the coming milestones for its widespread development	B5-104	2008

Tittle	Summary	Publication no.	Year
Interoperability challenge: Kahramaa experience with substation automation	The aim of this paper is to contribute as a utility's automation system integrators in identifying a common thread to interconnect those various systems together, benefit from the offered services/standards, and as a conclusion, a suggested guideline for future expansion	B5-103	2008
Optimized architectures for process bus with IEC 61850-9-2	IEC 61850, the standard for communication in substations, supports all tasks to be performed in the substation and provides by the process bus option which is also the link to the primary equipment like switchgear and instrument transformers. It is shown that the standard supports the trends in substation technology like the use of combined and non-conventional instrument transformers. It is discussed how different architectures providing the requested protection zones fulfil the requirements for flexibility, availability and dependency, minimise the number of devices (cost, failure rate) and communication components and facilitate the implementation of the time synchronisation needed for samples. How to get with these criteria; the optimised process bus architecture is shown on the example of the one-and-a-half breaker substation topology	B5-101	2008
Experience with IEC 61850 IN the refurbishment of an important European 380 kV substation	Following the publication of the standard IEC 61850 "communication networks and systems in substations", the partial retrofit of the 380 kV substation Laufenburg in Switzerland has been one of the first projects worldwide based on it. Seven out of the 17 bays are being retrofitted until the end of 2006. A stepwise approach has minimised service interruption. IEC 61850 was chosen to benefit from the future-proof features of this international standard Existing and new third-party equipment was integrated with the substation automation system. Valuable experiences in using IEC 61850 were gained, both by the substation owner and the manufacturer. The first bay was put into service in December 2004, followed by another three bays during 2005. All project goals were reached. Project execution and operational experiences are related, and an outlook on the future development of the standard is given	B5-109	2006

Tittle	Summary	Publication no.	Year
The University City SAS. First project within Iberdrola group using IEC 61850 for a complete substation. final experiences and future expectations	Iberdrola, a Spanish utility, has run a process to introduce the first SAS fully IEC 61850 based. This project, called "Ciudad Universitaria", will be the first one for the company, and will serve to test the effectiveness and impact this new standard proposes to go. Conclusions about what we have learned during the individual tests and the interoperability between IED's from different vendors are presented below	B5-108	2006
Implementation experience on IEC 61850-based substation automation systems	IEC 61850 enables control, protection and monitoring devices to communicate with each other without protocol convertors in substations. It also safeguards the investment of owners of substation automation systems in an environment in which communication technology changes rapidly. Since becoming international standard in 2005, it has increasingly gained acceptance from the utilities and industrial electricity consumers Experience has also revealed that the compatibility of devices from different generations in an installation has not been adequately specified, and the IEC working groups should address this issue as soon as possible to assure the continual success of the standard in future	B5-104	2006
Concept and first implementation of IEC 61850	IEC 61850 standardises the data names of and the services for all anticipated automation functions in substations. Separating communication from applications, IEC 61850 is future proof and safeguards the investment of the utilities. When Ethernet and TCP/IP are employed in the way the standard specifies, automation systems will benefit from leading-edge data transfer technologies within a substation as well as enterprise-wide. Compliant products are available from 2004 onwards. The verification projects of the last few years, some of which are still going on, are part of the foundation of this first implementation of the standard. Utilities have recognised the improvements which the standard will bring to their networks and are installing IEC 61850 systems in their substations	B5-110	2004

Tittle	Summary	Publication no.	Year
DOTS: an experience on interoperability in power substations	The present paper describes the experience of the authors on the definition of a model for distributed telecontrol networks at power substations, originated in the emergent standard IEC 61850 and CORBA suite. This experience has been carried out in the scope of the V Framework Programme, funded by the European Commission (IST-10258 DOTS project). The main objective of the DOTS project, to establish an open software model, built upon real time and minimum CORBA, and the emerging IEC 61850 standard, has been successfully achieved. The definition of the general model and the mapping of the ACSI to CORBA have been presented at the IEC TC57 meeting at Valencia on November 2000. Development of adequate tools, middleware and putting into operation a pilot telecontrol system have been also part of the project, in order to demonstrate the validity of the approach when facing real-world conditions. The field testing phase is just starting, but testing results at the laboratory are very positive, and it is expected to present performance results at CIGRE 2002 Session	34-205	2002
A pilot project for testing the standard drafts for open communication in substations—first experiences with the future standard IEC 61850	Deregulation will place greater demands for information acquisition on utilities than they have experienced before. IEC 61850 provides a timely, cost-effective and standardised solution to allow advanced IED functions and distributed systems to form the foundation for "next generation" electric utility protection, control and monitoring systems The project OCIS is an excellent example that every standardisation effort needs in parallel practical work to proof the theoretical approaches. OCIS has shown so far that the new approach of open communication systems, open functions and standardised function modelling applied in IEC 61850 and UCA.2 is feasible. Many comments on the IEC 61850 and UCA.2 drafts have led to the improvement of these specifications. From today's point of view, we expect the publication of IEC 61850 in the end of the year 2001	34-109	2002

Tittle	Summary	Publication no.	Year
Serial communication between process and bay level—standards and practical experience	The serial communication interfaces between the process and the bay level offer a number of advantages in the engineering and the design of substations. Novel technologies for instrument transducers depend on the availability of standardised serial communication interfaces. IEC recognised early the need for those interfaces, but standardisation takes a long time, because the content of the standard must be agreed by vendors and utilities all over the world. The elaboration of a system standard such as the IEC 61850 takes even longer, but in the meantime until the standard will be available, the utilities and the vendors can gain a lot of experience with the new technology even if proprietary communication interfaces are used	34-106	2002

Definitions, Abbreviations and Symbols

B

CIGRE Terms

Acronym	Phrase	Definition
TB	Technical Brochure	A publication produced by CIGRE representing the "state-of-the-art" guidelines and recommendations produced by an SC WG
SC	Study Committee	One of the 16 technical domain groups of CIGRE. https://www.cigre.org/GB/knowledge-programme/our-16-study-committees-and-domains-of-work
TG	Thematic Group	A supervisory group relative to a sub-topic within the scope of a particular SC
WG	Working Group	A select group tasked with developing a TB relative to a defined TOR; e.g. WG B3.40 is a WG within the SC B3 domain
JWG	Joint Working Group	A WG comprising collaboration between two or more SCs e.g. JWG C3/B3.20 involves both SC C3 and B3 and is led by SC C3
TF	Task Force	Generally, a sub-group of a WG tasked with investigation of a specific aspect within the overall terms of reference or a sub-group of a SC with a shorter term task that may ultimately lead some other CIGRE work
NC	National Committee	National entities responsible for local CIGRE activities and membership
TOR	Terms Of Reference	The scope of work defined for the WG as approved by the TC
TC	Technical Council	The group of SC Chairman and the Chairman of the TC

P. Bishop and N.-K. C. Nair (eds.), *IEC 61850 Principles and Applications to Electric Power Systems*, CIGRE Green Books, https://doi.org/10.1007/978-3-031-24567-1

Organisation Acronyms

Acronym	Full name	Web link
ANSI	American National Standards Institute	
CIGRE	CIGRE (previously a French acronym pronounced in English as "sea-grey")	https://www.cigre.org/
CENELEC	European Committee for Electrotechnical Standardization	https://www.cenelec.eu/
CIRED	International Conference on Electricity Distribution	http://www.cired.net/
ENTSO-E	European Network of Transmission System Operators for Electricity	https://www.entsoe.eu/
IEC	International Electrotechnical Commission	https://www.iec.ch/
IEEE	Institute of Electrical and Electronic Engineering	https://www.ieee.org/
IET	Institution of Engineering and Technology	https://www.theiet.org
NERC	North American Electric Reliability Corporation	https://www.nerc.com/
WECC	Western Electricity Coordinating Council	https://www.wecc.biz/

Specific Terms in this Book

General electrical terms are based on the IEC 60050 series known as the International Electrotechnical Vocabulary (IEV) which can be referenced here: http://www.electropedia.org/ (specific selections provided below)

Phrase	Definition
Substation (of a power system)	http://www.electropedia.org/iev/iev.nsf/display?openform&ievref=605-01-01
Switching substation	http://www.electropedia.org/iev/iev.nsf/display?openform&ievref=605-01-02
Transformer substation	http://www.electropedia.org/iev/iev.nsf/display?openform&ievref=605-01-03
Single busbar substation	http://www.electropedia.org/iev/iev.nsf/display?openform&ievref=605-01-16
Double busbar substation	http://www.electropedia.org/iev/iev.nsf/display?openform&ievref=605-01-17
Triple busbar substation	http://www.electropedia.org/iev/iev.nsf/display?openform&ievref=605-01-18
Ring substation	http://www.electropedia.org/iev/iev.nsf/display?openform&ievref=605-01-19
Mesh substation	http://www.electropedia.org/iev/iev.nsf/display?openform&ievref=605-01-20
Four-switch substation	http://www.electropedia.org/iev/iev.nsf/display?openform&ievref=605-01-21

Phrase	Definition
Three-switch mesh substation with bypass	http://www.electropedia.org/iev/iev.nsf/display?openform&ievref=605-01-22
Four-switch mesh substation with mesh opening disconnectors	http://www.electropedia.org/iev/iev.nsf/display?openform&ievref=605-01-23
Two-breaker arrangement	http://www.electropedia.org/iev/iev.nsf/display?openform&ievref=605-01-24
One-and-a-half breaker arrangement	http://www.electropedia.org/iev/iev.nsf/display?openform&ievref=605-01-25

Term	Full form meaning
AC	Alternating Current
ABTS	Automatic Bus Transfer Scheme
API	Application Programming Interface
APT	Advanced Persistent Threat
ASDU	Application Service Data Unit
BAP	Basic Application Profile
BCU	Bay Control Unit
BDS	Bei Dou Navigation Satellite System
CAD	Computer-Aided Design
CCGT	Combined cycle gas turbine
CF	Ceiling Factor
CIC	Central Interlocking Controller
CID	Configured IED Description file
CIM	Common Information Model
CP	Communication Protocol
CSV	Comma-Separated Value
CT	Current Transformer
DA	Data Attribute
DANH	Double Attached Nodes implementing HSR
DANP	Double Attached Node using PRP
DC	Document for Comments or Direct Current
DER	Distributed Energy Resources
DHS	Department of Homeland Security
DO	Data Object
DOE	Department of Energy
DSAS	Digital Substation Automation System
DSO	Distribution System Operator
EHV	Extra High Voltage
EPRI	Electric Power Research Institute

Term	Full form meaning
EU	European Union
FAT	Factory Acceptance Test
FRT	Fault Ride Through
FW	Firewall
FRACSEC	Fraction of a Second
FRT	Fault Ride Through capability
FSOC	Federated Security Operations Centre
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
GGIO	Generic Process Input/Output
GIS	Gas Insulated Switchgear
GNSS	Global Navigation Satellite System
GOOSE	Generic Object-Oriented Substation Events
GSSE	Generic Substation State Events
GW	Gateway (communication gateway to SCADA like RTU)
HMI	Human Machine Interface (sometimes also called OWS = Operator Workstation)
HSR	High-availability Seamless Redundancy
HV	High Voltage
IACS	Industrial Automation Control Systems
ICD	IED Capability Description File
ICS	Industrial Control Systems
ICT	Information and Communications Technology
IED	Intelligent Electronic Device—rather than Relay
IGMP	Internet Gateway Management Protocol
IID	Instantiated IED Description File
I/O	Input/Output
IOP	Interoperability
IOT	Internet of Things
IPP	Independent Power Producer
IRIG-B	Inter-Range Instrumentation Group timecodes
ISD	IED Specification Description file
ISOC	Information Security Operations Centre
IST	Interoperability Specification Tool (ENTSO-E tool)
LAN	Local Area Network
LED	Light-Emitting Diode
LN	Logical Node
LPIT	Low-Power Instrument Transformer—rather than NCIT
LV	Low Voltage

Term	Full form meaning
LVAC	Low-Voltage AC
MCMF	Multichannel Multi-Frequency
MIL	Maturity Indicator Level
MMS	Manufacturing Message Specification
MPLS	Multiprotocol Label Switching
MRP	Media Redundancy Protocol
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
MU	Merging Unit
MV	Medium Voltage
NERC	North American Electric Reliability Corporation
NTP	Network Time Protocol
~~NCIT~~	~~Non Conventional Instrument Transformer~~—Use LPIT
O&M	Operation and Maintenance
OCXO	Oven Crystal Oscillator
OEM	Original Equipment Manufacturer
PACS	Protection Automation and Control system—rather than SAS (Substation Automation System)
PC	Personal Computer
PDV	Packet Delay Variation
PEIPS	Power Electronic Interfaced Power Sources
PHY	Physical Layer
PICOM	Piece of Information for Communication
PPS	Pulse Per Second
PRP	Parallel Redundancy Protocol, a network protocol providing fault-tolerance
PTP	Precision Time Protocol
QoS	Quality of Service
RES	Renewable Energy Source
ROU	Related Organisation Units
RPC	Reactive Power Capability/controller
RSTP	Rapid Spanning Tree Protocol
RTU	Remote Terminal Unit (communication gateway to SCADA like GW)
~~SAS~~	~~Substation Automation System~~—PACS to be used
SAMU	Stand-Alone Merging Unit
SAN	Singly Attached Node
SAT	Site Acceptance Test
SCADA/EMS	Supervisory Control and Data Acquisition/Energy management system
SCS	Substation Control System
SCD	System Configuration Description

Term	Full form meaning
SCL	System Configuration Language
SCSM	Specific Communication Service Mapping
SCR	Short circuit ratio
SCT	System Configuration Tool
SDH	Synchronous Digital Hierarchy
SDN	Software-Defined Network
SLD	Single-Line Diagram
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SOE	Sequence of Events
SS	Steady state
SSD	System Specification Description file
SST	System Specification Tool
SV	Sampled Values
SVCB	Sampled Value Control Block
TAI	International Atomic Time
TCA	Temporary Cyber Asset
TCP	Transmission Control Protocol
TCXO	Temporary Controlled Crystal Oscillator
TDM	Time-Division Multiplexing
TSO	Transmission System Operator
TWFL	Travelling Wave Fault Locator
UCA	Utility Communication Architecture
UCAug	Utility Communication Architecture User Group
UDP	User Datagram Protocol
UFLS	Under-Frequency Load Shedding
ULTC	Under load tap changing transformer (the on load tap changing transformer, OLTC, is also known)
UTC	Universal Time Coordinated
UTP	Unshielded Twisted Pair
UVLS	Under Voltage Load Shedding
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRT	Voltage ride through capability
VT	Voltage Transformers
WAPS	Wide Area Protection Systems

Symbols

General electrical symbols are based on the IEC 60617 series https://www.iec.ch/.