An Investigation into the State of Cybersecurity Preparedness with Respect to Operational Technology

Farouk Akrama and Hamid Jahankhani

Abstract The importance of software-level communication security in ICS is growing as these systems become more automated and connected to the outside world. This chapter provides a secure-by-design approach to ICS application development, where design-time abstractions known as secure links are used to meet criteria from security protocols like ISA/IEC 62443. Secure links are a proposed addition to an IEC 61499 design standard that makes it easy to integrate both lightweight and conventional security measures into software. Automatic compilation into completely IEC 61499-compliant software is possible for applications that use secure links. To keep up with this demand for greater adaptability. Nowadays, in the revolution of digitalization, automation plays significant role to achieve a sufficient level of security and reduce the use of both human resources and static processes. Therefore, it is crucial to model all security related capabilities and functionalities. In this chapter a unique requirements repository model for Industrial Control System that applies the LPGs (Labelled Property Graphs) to form and store standards based and system specific requirements using well-defined relationship types are highlighted. In addition, the researcher integrates the proposed requirements repository with the Industrial Control System design tools to determine requirements traceability. A wind turbine case study demonstrates the entire workflow within the proposed framework.

Keywords IEC 62443 · ISA/IEC 62443 International Electrotechnical Commission · ICS Industrial Control System · NIST National Institute of Standards and Technology

F. Akrama · H. Jahankhani (✉)
Northumbria University, London, UK
e-mail: Hamid.jahankhani@northumbria.ac.uk

H. Jahankhani and A. El Hajjar (eds.), *Wireless Networks*, Advanced Sciences
and Technologies for Security Applications,
https://doi.org/10.1007/978-3-031-33631-7_10

1 Introduction

Top-down analysis is not the only option, though; industry frameworks offer another perspective. A consensus amongst experts in a field is used to develop a "prototype" for a business in that field, and this is what industry frameworks give. In general, the frameworks identify typical functional and business process breakdowns that may correspond to capabilities. It may be more comprehensive and unbiased than a value chain tailored to a particular company. Naturally, every organisation will be unique due to its own specific set of circumstances and methods of operation, and these distinctions may provide a competitive edge in some sectors.

The capabilities of an industrial framework tend to coincide with their respective implementations in commercial enterprise software and outsourced services, which is a definite plus. A well-defined standard value chain should not be abandoned in favour of an industrial framework; rather, it can provide even more insight into the description of shared capabilities when used together. It is possible that a company's data model is part of the framework for its industry. This paper serves as a stepping stone to addressing security by design approaches by describing security capability levels and requirements across the Industrial Control System zones. Moreover, the paper examines why it is important to have a standard, enterprise-wide logical data model by following an adapted case study method. A safety critical wind turbine system was deployed and modelled to examine several security issues of monitoring and managing cybersecurity requirements in Industrial Control System. There are two primary arguments in favour of seriously considering the use of a structural data model early in the process of creating a CBA for such a given business. To begin with, the CBA transformation will be delayed and the cost of getting a model will be more than the cost of developing a suitable corporate logical data model. Second, there will be fewer data transformation issues when exchanging data between services because the framework data model will likely be similar with competitive software systems and technical service as well as regulatory requirements.

2 Literature Review

Different networks system like control processing, manufacturing of robotic system, automation system for both home and office, intelligent system on transportation and aircraft, spacecraft in advance. Sometime these types of network system are typically made up of a significant number of interconnected devices, the management of which can either be centralised or decentralised, depending on the requirements of the application. Routable data communications protocols like Ethernet (IEEE 802.3) and Wi-Fi are typically placed in homes and workplaces, but due to modern demands for adaptability, decentralisation, simple work for continuity, and reduced minimal cost for operations, their incorporation into network control systems has become increasingly common. Because of this shift, maintaining a high level of security within industrial control systems is now more vital than ever. Confidentiality is given the utmost priority in traditional information technology (IT) security regulations, while network availability receives the least amount of consideration [1]. In contrast, critical infrastructure ICSs and ISCI (ISA Security Compliance Institute) must always maintain both high availability and operational resilience. This is necessary for a variety of reasons, including those pertaining to the economy, the environment, the safety of humans, and the security of the nation. It is unacceptable, with regard to many different procedures, to suffer a decrease in performance for the sake of security [2]. In order to arrive at such a conclusion, a risk–benefit analysis must first be performed on each system. It is necessary to incorporate security safeguards in a manner that will preserve the integrity of the system both when it is functioning normally and when it is under attack from a computer network.

Alber and Prince [3] emphasised that industrial control system security needs to incorporate both network security and features of robust physical architecture (such as redundancy and physical adaptability) to maintain the appropriate level of system availability. A comprehensive risk assessment and methodical system engineering are the processes that are used to establish such requirements. Based on the concepts of precise measurement science, the Industrial Control System (ICS) testbed provides guidance on how to implement security in an ICS via the course of testing.

According to Green et al. [4], the purpose of the Industrial Operation System (ICS) Cyber Security Test Bed is to showcase the value of security in a variety of contexts, such as the management of a chemical plant, the dynamic assembly of complex parts with the help of robots, and the centralised management of vast WANs. As indicated, the testbed's major goal is to show how industrial control system security standards like NIST SP 800-82 can be applied to a networked control system and how the standards might affect the system's performance, if at all [5]. This test bed will also serve as a guide for implementing security measures without sacrificing efficiency. One of the testbed's secondary purposes is to assess how well industrial control systems function in the midst of a cyber-attack; this is important because no system can be rendered fully secure from network assaults [6]. The ability of systems to withstand attacks will be one of their primary concerns. The test bed will be available to universities, government organisations, and commercial businesses for the purpose of conducting research and evaluations on new technologies designed to improve remote monitoring systems and enhance procedures more resilient to attacks. A total of five years' worth of research will be supported by the testbed.

Numerous commercially available tools exist to safeguard systems built on top of industrial standards. Products like the CISCO Adaptive Protection Appliance (ASA) and the Tofino Protection Appliance are examples of NG firewall devices that offer a high standard of security and a plethora of security functions [7]. The primary purpose of these solutions is to prevent network perimeter exploits against programmable logic controllers (PLCs). However, these technologies do provide valuable network protection. The delay, the jitter, and the payload integrity of data packets are the metrics that make up this set. This means that each enclave's starting point for measurement will be based on deliberately generated delay, jitter, and noise, and that the performance of the processes under study would be analysed in relation to these factors [8], this document offers directions for the establishment of safe control systems for industrial machinery (ICS). This type of industrial control system (ICS) is widely used in manufacturing and similar fields. Industries that frequently employ ICS include the ones dealing with electricity, water, wastewater, oil and natural gas, transportation, chemicals, pharmaceuticals, paper products, food and beverages, and other types of discrete manufacturing (e.g., transportation equipment, aeronautical machinery, and long-lasting products) [9]. SCADA systems are typically used to control dispersed assets because of the centralised data gathering and performance monitoring that provide [10]. Controlling production systems in a localised region such as a factory through the use of supervisory and regulatory control is a typical use for distributed control systems (DCS). Programmable logic controllers (PLCs) are commonly employed to carry out regulatory control and perform discrete control for a wide range of applications. Control systems are crucial to the smooth running of the United States' essential infrastructures, which are increasingly interconnected and reliant on one another. Almost 85% of the nation's critical infrastructures are owned and operated by private enterprises [11], which must be taken into account. Postal Service mail sorting and air traffic control are just two instances of the aforementioned ICS that are also run by the federal government. This article provides a general introduction to ICS, describes common system topologies, discusses common security threats and vulnerabilities, and suggests solutions to reduce these risks. The following are examples of events that an ICS could potentially face: The flow of information over ICS networks being obstructed or slowed down, which could cause ICS to stop working, changes to alarm levels, instructions, or directives that could lead to the malfunction, shutdown, or destruction of machinery due to unauthorised tampering; cause harm to the environment; endanger people's safety [12]. Franceschett et al. [13] has highlighted that incorrect information relayed to operators of the system, with the intention of either disguising unlawful changes or prompting the operators to take activities that are not appropriate, both of which could have a variety of adverse outcomes. Alterations were made to ICS software or configuration settings, or malware was introduced into ICS software, any of which could have serious consequences. Creating an unsafe environment by interfering with safety systems that would otherwise keep people alive.

2.1 Industrial Control System (ICS)

The electric, water and sewage, oil and natural gas, chemical, pharmaceuticals, pulp and paper, foodservice, and discrete manufacturing industries are just some of the many that use ICS. The document presents a long number of strategies and approaches for protecting ICS, which is necessary given the wide variety of ICS and the wide range of risks and consequences that each form of ICS may provide. This paper is not meant to be used as a simple checklist to ensure the safety of any given system. Readers are urged to conduct a risk analysis of their systems and modify the suggested guidelines and remedies to match their unique security, business, and operational needs. The scope of use for the fundamental concepts for protecting control systems provided here keeps growing [14].

Industrial control system (ICS) is a broad term that includes several different types of control systems. These include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other industrial automation configurations like Programmable Logic Controllers (PLC), which are often used in industrial sectors and critical infrastructures. An ICS is a group of control parts (such as electrical, mechanical, hydraulic, and pneumatic) that work together to reach a business objective. The process is the portion of the system that is mostly responsible for making the output. In the monitoring part of the system, you tell it what output or performance you want. Control can be done by machines alone or with a person in the loop. Systems can run in open-loop, closed-loop, or manual mode, depending on how it has been set up. In open-loop control systems, the output is monitored by the settings that have already been made. In closed-loop control systems, the output affects the input in a way that keeps the goal the same. When the system is in manual mode, it is completely controlled by people. The part of the system that is mostly responsible for making sure it stays in line with specifications is called the controller. A typical ICS may have many control loops, Human Machine Interfaces (HMIs), and secluded diagnostic testing and maintenance tools built with a variety of network protocols.

2.2 Comparing ICS and IT Systems Security

IT systems take care of data, while ICS control the nature of reality. ICS are distinct from traditional IT frameworks in many ways, such as having different threats and priorities. Some of these are a massive threat to people's health and safety, serious environmental damage, and significant financial loses like lost production and bad reputation on the economy of a specific country. ICS have different requirements for performance and reliability, and the use operating applications and systems that are not always common in an IT network environment. Security measures must be configured in a way which keeps the system's integrity both when it is running normally and when it is under attack.

At first, ICS did not have much in common with IT systems because it was separate systems with its own control protocols and hardware and software. Older proprietary technologies are being replaced by Wireless and Internet Protocol (IP) devices that are easy to find and don not cost much. This makes cybersecurity security flaws and incidents more likely. As ICS use IT solutions to improve corporate connectivity and remote access, and as it is designed and implemented using industry-standard computers, operating systems (OS), and internet protocol, it is started to look more like IT systems. This integration allows for new IT functionality, but it opens up ICS to the outside world much more than previous systems did. This makes it more important to secure such systems. Even though security mechanisms have been made to deal with all these security problems in normal IT systems, it must be used with extra care in ICS environments. In some cases, the ICS environment needs new security solutions that are made for it [15].

The following table demonstrate the key differences between IT and ICS security systems with the practice of cyber security.

Requirement	IT security system	ICS security system
Performance requirements	Non-real time, the key to a good response is uniformity Required is a high rate of processing Having a lot of delay and jitter might be fine in the event of an emergency, this interaction is less crucial There is scope for implementing highly restricted access control, to the point where security-related interactions are possible It is possible to create a level of access control that is tight enough to provide the requisite level of safety	Rapid reaction is necessary Low throughput is fine High levels of latency cannot be tolerated and/or jitter It is crucial to act quickly in times of crisis There have to be tight controls on who can use ICS, but it does not mean, it should make it impossible for people and machines to work together
Availability (reliability) requirements	Reactions like restarting are appropriate Deficits in availability are often acceptable provided, it does not interfere with the system's functionality	Rebooting is not always an option, depending on process availability constraints It is possible that having duplicate systems is necessary due to availability needs Scheduled downtime needs to be prepared for days or weeks in advance Extensive pre-deployment testing is necessary for high availability

(continued)

(continued)

Requirement	IT security system	ICS security system
Risk management requirements	Keep data secure Maintaining data privacy and integrity is of the utmost importance In this case, data redundancy is less crucial, as brief outages pose little threat Delay in company operations is a major risk factor	The ability to manipulate the material universe First and foremost is ensuring the safety of the people involved, followed by safeguarding the actual process itself The ability to withstand failures is crucial, as even brief outages might not be tolerated Noncompliance with regulations, adverse effects on the environment, loss of life, property, or output is all potential catastrophes
System operation	In order to work with standard operating environments, systems have been built with the help of automated deployment tools, upgrades are a breeze	Various possibly proprietary, operating systems, many of which lack basic security features Due to the specific control algorithms and possibly updated hardware and software, patch management must be handled with care, and this is often the responsibility of software providers
Resource constraints	Systems are designed with ample capacity to accommodate the installation of optional software, such as security programs	In other cases, systems may lack the necessary storage space and processing power to properly implement security measures, as it was built to serve the needs of a specific manufacturing procedure
Communications	Protocols for regular communication Wire-based primarily with occasional wireless access Normal procedures for establishing and maintaining a network in the information technology industry	A wide variety of communication standards and proprietary protocols Networks are complicated and often call for the services of control engineers due to the wide variety of communication channels employed, including both hardwired and cellular options
Change management	When solid security policies and procedures are in place, updates to software are deployed promptly. Frequently, the processes are computerised	To prevent a control system's integrity from being compromised, software updates must be rigorously tested and rolled out in stages. It is common practise to schedule ICS outages several days or weeks in advance. ICS could be relying on unmaintained operating systems

(continued)

(continued)

Requirement	IT security system	ICS security system
Managed support	Afford a range of support methods	Single-vendor service support is the norm
Component lifetime	Approximately a 3–5-year lifespan	Ten- to fifteen-year lifespan
Components location	All parts are often stored in close proximity to one another	It may take a lot of time and energy to physically access an isolated, far-away, or difficult-to-reach component

2.3 Risk Assessment and Management in ICS

Risk management is an everyday occurrence for organisations. Financial risk, equipment failure risk, and risks to employee safety are just a few examples. Businesses need systems in place to help them assess the threats to their operations and determine the best course of action, taking into account internal and external priorities and restrictions. As part of routine business procedures, this risk management is carried out in an iterative, ever-evolving manner [16]. Traditionally, businesses that employ ICS have mitigated risk by adhering to sound safety and engineering principles. Most industries have long-standing practises of conducting safety evaluations, and it is often integrated into legislation. Management of the risks associated with information security adds an important dimension. Both physical and digital security risk assessments can make use of the risk assessment process and framework described in this section.

A company should implement a risk management process across the board, with a three-pronged strategy to handle risk at (i) the company level, (ii) the mission/business process level, and (iii) the information management level (IT and ICS). With the goal of ensuring that the organization’s risk-related operations are continually improved and that all stakeholders with a vested interest in the organization’s mission/business performance can effectively communicate with one another across all three levels, the risk assessment procedure is done out in an integrated fashion.

Frame, assess, respond, and monitor are the four steps in the process of risk management depicted in Fig. 1. These responsibilities overlap and require each other to be fulfilled effectively. As an example, the results from the monitoring part will be used in the framing part. Due to the dynamic nature of the business environment, managing risk must be an iterative procedure in which all phases involve ongoing actions. Keep in mind that these factors affect the control of any risk, whether it be financial, physical, safety, or informational.

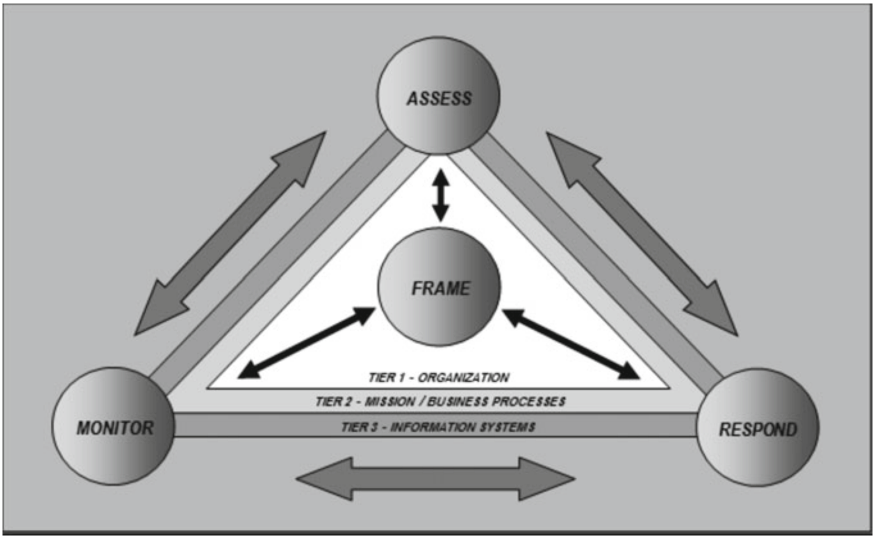

ASSESS
FRAME
MONITOR
RESPOND
TIER 1 - ORGANIZATION
TIER 2 - MISSION / BUSINESS PROCESSES
TIER 3 - INFORMATION SYSTEMS

Fig. 1 Risk assessment in different levels

2.4 ICS-Specific Security Policies and Procedures

The backbone of any reliable security system is its policies and procedures. Existing operational and management rules and processes should be linked with ICS-specific security procedures and policies whenever practicable. Consistent and up-to-date security protection against emerging threats is possible credits to policies and processes. Numerous suggestions for improving ICS information security policies may be found in the ICS overlay. After conducting a thorough risk assessment, the data security manager must evaluate the effectiveness of current security measures in mitigating threats to the ICS. Existing policies may need to be updated or replaced.

The organization's risk tolerance, or the level of risk it is willing to take, is determined and communicated by Tier 1 management. This information is used by the security manager to figure out how much of risk mitigation to implement in order to bring the remaining risk within acceptable bounds. An organisation can better minimise the risks posed by attacks if its security policies are based on a risk analysis and business modelling that establishes the organization's security priorities, classify assets, and identify business goals. In order to ensure that the rules are fully and correctly executed for the ICS, it is essential to create supporting procedures. Changes in policy, technology, and threats necessitate the documentation, testing, and continuous updating and improvement of security processes (Fig. 2).

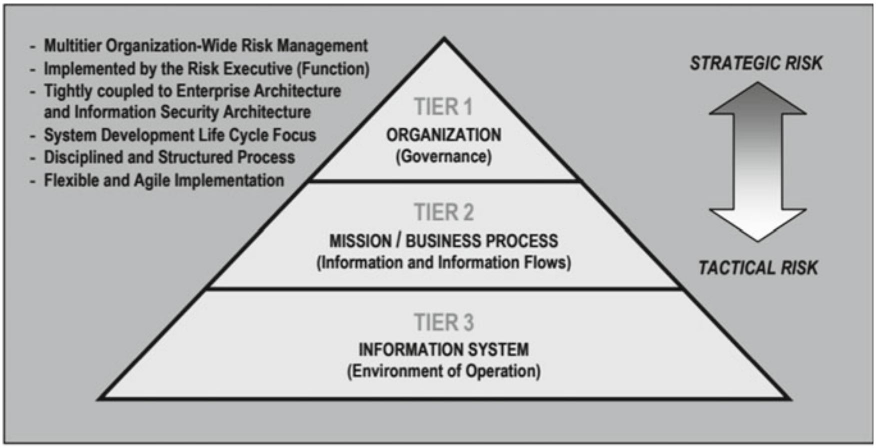

- Multitier Organization-Wide Risk Management
- Implemented by the Risk Executive (Function)
- Tightly coupled to Enterprise Architecture and Information Security Architecture
- System Development Life Cycle Focus
- Disciplined and Structured Process
- Flexible and Agile Implementation
TIER 1
ORGANIZATION
(Governance)
TIER 2
MISSION / BUSINESS PROCESS
(Information and Information Flows)
TIER 3
INFORMATION SYSTEM
(Environment of Operation)
STRATEGIC RISK
TACTICAL RISK

Fig. 2 NIST risk management system

2.5 ICS Security Risk Management Framework Implementation

From a more theoretical perspective, ICS risk management is just another risk that a company must consider. C management in charge of a particular mission or business operations must develop and implement a risk management plan in conjunction with the executive risk team at the company's highest priority. Information Security Risk Management is a Framework for assessing, mitigating, and migrating threats in today's organizations, missions, and Information Systems; NIST SP 800-39 having a point of view is essential to the success of any risk management initiative. When it comes to establishing and carrying out ICS global threat management and sharing information with enterprise management in support of effectively managing risks across the entire enterprise, the personnel involved to ICS apply their specialised subject matter knowledge, just as they do in the other task process areas. Implementing the framework for risk management is covered in NIST SP 800-37, guide for implementing the framework for risk management to Federal Information Systems. The next few paragraphs will briefly recap the procedure and then explain how to implement the RMF in an ICS setting.

There are several numbers of clearly defined organisational roles in the RMF process, each is responsible for a specific set of risk-related tasks within the organisation. It is important to note that many of the responsibilities outlined for risk management also exist in the ordinary life cycle of system development procedures. Processes in the RMF are carried out in parallel with, or as a part of, the system development life cycle (Fig. 3).

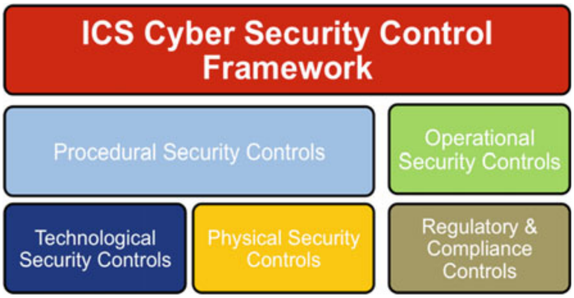

ICS Cyber Security Control Framework
Procedural Security Controls
Operational Security Controls
Technological Security Controls
Physical Security Controls
Regulatory & Compliance Controls

Fig. 3 ICS security framework with risk applied

3 ISA-99 Security

Cybersecurity Testbed verified the ISA/IEC-62443 principles and technological security standards. These criteria are similar to those found in NIST 800-82. Groups of related documents from the IEC series are displayed in Fig. 4. The documents in the 1-X series define the scope of the standard's application and explain why it was developed. The 2-X documents outline the necessities of an ICS security plan and how to put its policies and procedures into action. The 3-X series documentation outline the design criteria for solution providers and provides recommendations on various security solutions that may be relevant to an ICS integrator. Manufacturers of individual components are the primary targets of the 4-X series, which specifies the requirements they must meet in order to offer the vital functional hooks for a much more secure implementation. Meeting the standards is laid out in ISA/IEC-62443-3-3 [17].

3.1 Risk Management Framework (RMF) with Industrial Control System (ICS)

The steps necessary to implement RMF for ICS are outlined below. Each step of the procedure is outlined, and relevant NIST [18] documents are referenced. Although the following procedures are presented in a certain order, it can be performed in any order that is consistent with standard network and management development life cycle procedures.

3.1.1 Step 1: Classify Security Information System

Information system security classification is the most important step in RMF which include the process of categorising and labelling information based on its sensitivity level. This is done to protect the information from unauthorised access or disclosure. Information systems are usually classified into three categories: Confidential, Secret, and Top Secret.

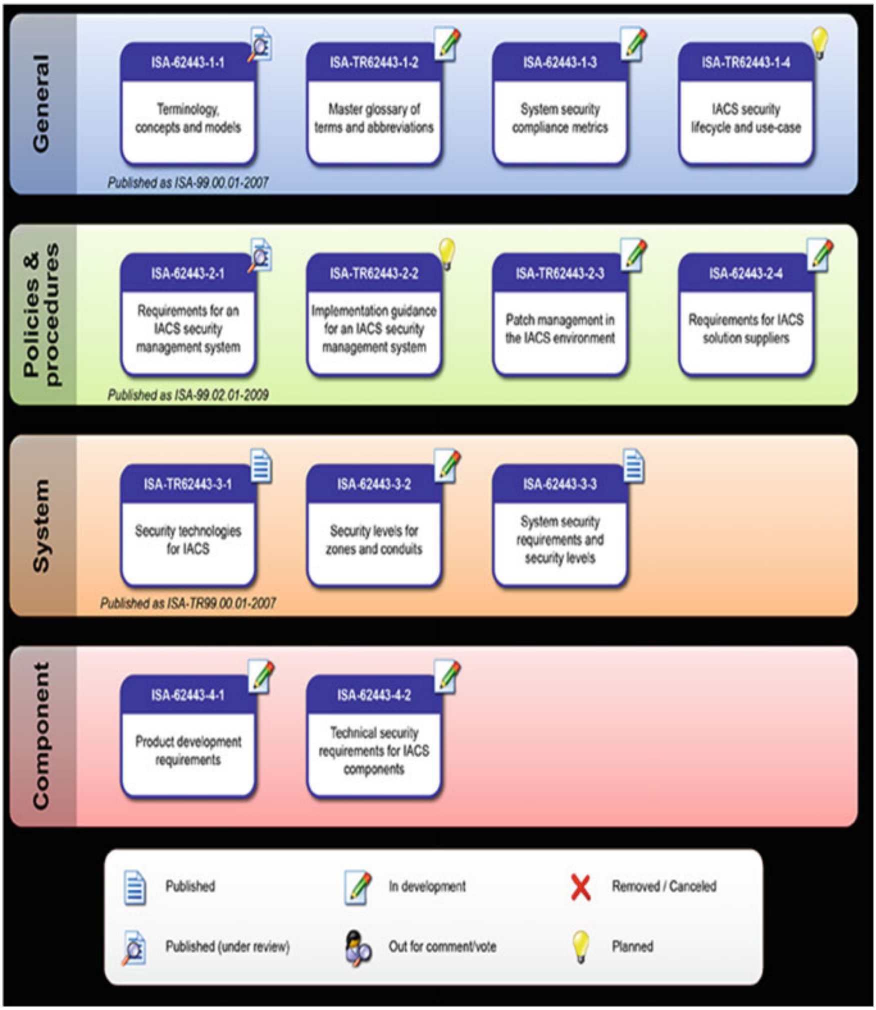

General
ISA-62443-1-1
Terminology, concepts and models
ISA-TR62443-1-2
Master glossary of terms and abbreviations
ISA-62443-1-3
System security compliance metrics
ISA-TR62443-1-4
IACS security lifecycle and use-case
Published as ISA-99.00.01-2007
Policies & procedures
ISA-62443-2-1
Requirements for an IACS security management system
ISA-TR62443-2-2
Implementation guidance for an IACS security management system
ISA-TR62443-2-3
Patch management in the IACS environment
ISA-62443-2-4
Requirements for IACS solution suppliers
Published as ISA-99.02.01-2009
System
ISA-TR62443-3-1
Security technologies for IACS
ISA-62443-3-2
Security levels for zones and conduits
ISA-62443-3-3
System security requirements and security levels
Published as ISA-TR99.00.01-2007
Component
ISA-62443-4-1
Product development requirements
ISA-62443-4-2
Technical security requirements for IACS components
Published
In development
Removed / Canceled
Published (under review)
Out for comment/vote
Planned

Fig. 4 ISA/IEC-62443 organization of standards documents

3.1.2 Step 2: Selection of Security Controls

The initial process of the set of requirements-based minimum security measures for the information system is part of this framework activity. The Federal Information Processing Standard 200 (FIPS 200) is a detailed document that illustrate a set of minimal security criteria for safeguarding federal data systems and the handled data in store, and in transport. These requirements span eighteen different security-related topics (Fig. 5).

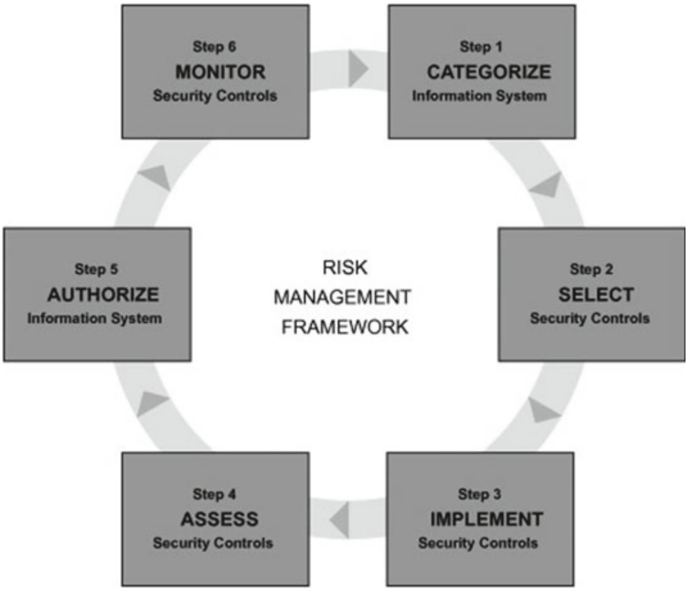


Fig. 5 Risk management framework step by step procedure

3.1.3 Step 3: Implement Security Controls

This process entails integrating new or existing security measures into an IT infrastructure. Both new development and legacy ICS can benefit from the adequate security selection approach outlined in this section.

Since new development systems do not yet exist, businesses doing initial security categorisations apply the cybersecurity selection procedure from the perspective of needs definition. The security controls outlined in the information system security plans act as a controlling and are meant to be integrated into the systems during in the Software development life cycle (SDLC) phases of design and implementation.

3.1.4 Step 4: Analyse Preventative Measures

Assessment of the information system's security measures is the process through which their efficacy in practise is measured. To verify that the security measures chosen from NIST SP 800-53 have been properly implemented, are functioning as intended, and have yielded the expected result in terms of meeting the system's security requirements, NIST has published NIST SP 800-53A to serve as a guide. NIST SP 800-53A aids in this endeavour by describing the assumptions of security assessments according to the FIPS 199 impact level, with the latter being based on assurance standards established in NIST SP 800-53.

3.1.5 Step 5: System of Authorised Data

A management decision is made to allow an information system to function and to accept the threat to agencies operations, federal assets, or personnel based on the application of an accepted set of security measures.

3.1.6 Step 6: Security Controls Monitoring

Monitoring and evaluating the efficacy of security measures is an ongoing process that keeps tabs on any updates to the data system that could affect such controls. Network security continuous monitoring is covered in detail by NIST SP 800-137.

4 Operational Technology Incident Response Plans

The term "operational technology" (OT) cybersecurity refers to the measures used to safeguard OT networks, systems, users, and data. The convergence of IT and OT to facilitate "big data" projects, combined with the growing importance of data gathering and analysis has necessitated a revaluation of cybersecurity best practises for defending OT environment.

The first Industrialisation in the 1700s marked the beginning of the era in which industrial controls became necessary. It takes generations to establish a regulator that could regulate the rate of steam—powered output and finally bring this new source of power under control, demonstrating just how challenging and critical the process of turning steam into useable energy was. Controls on complex processes have either prompted or been prompted by each industrial revolution.

4.1 Building a Business Case for OT Cybersecurity

The business case for keeping OT up to date is the same as it has been for and over 200 years; to get things done faster by improving productivity, safer by using sensors and other instruments to monitor the performance of various systems, and more efficiently for less cost, in addition to improve the ability to make more informed and efficient decisions. Throughout history, OT has become one of the most important ways to improve the quality of life and work. It has made it possible to provide treated drinking water, energy, and sewage treatment in a safe and cost-effective approach, as well as to many everyday life routines. Because of this, it should not be a surprise that OT features is being used by more people outside of its conventional industrial base. Businesses, governments, and sometimes even consumers are becoming more

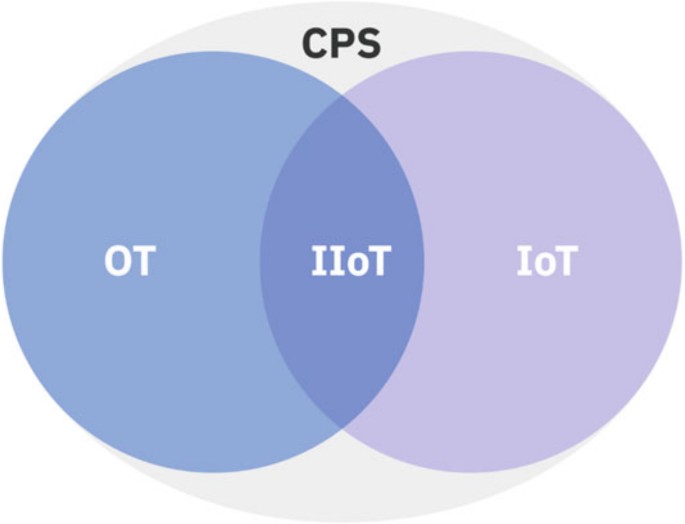


Fig. 6 Relationship among CPS, OT, IoT and IIoT

interested in the benefits of controlling and monitoring the physical environment. In the other hand, cybersecurity worries about OT are never higher because it is getting more complicated to keep OT systems secure (Fig. 6).

4.1.1 Concerns About Cybersecurity with the Integration of IT and OT

The widespread use of complex enterprise software, especially big data analytics, had also led organisations to integrate IT systems and OT infrastructure when industrial systems been connected with an IT network which makes possible to check on the performance and related of systems and equipment all the time via a life ERP dashboard. These benefits are very appealing, and it explain why involvement in IT/OT integration has grown expeditiously.

4.1.2 Importance of OT Cybersecurity

Traditional OT systems have a long list of security problems, such as the legacy equipment that lasts for decades; systems that cannot be patched, in addition to the lack of basic security features (user identification or encryption). In a perfect past, when these kinds of systems were "air-gapped" and completely isolated from the world at large these worries were thought to be acceptable risks. Complete isolation is almost impossible today, though, and organisations will need to use a combination of traditional IT information security products and services and OT-specific cybersecurity solutions to protect OT from new risks.

4.2 Purdue Model

Established in the middle of the 1990s, the Purdue Enterprise Standard architecture has gained widespread support in the business world as a means of comprehending the mandatory hierarchical system of OT systems. It is a part of the ANSI/ISA-95 standard, that depicts how the various high-level parts of a typical control systems are linked to one another (ICS).

4.2.1 Purdue Model Levels

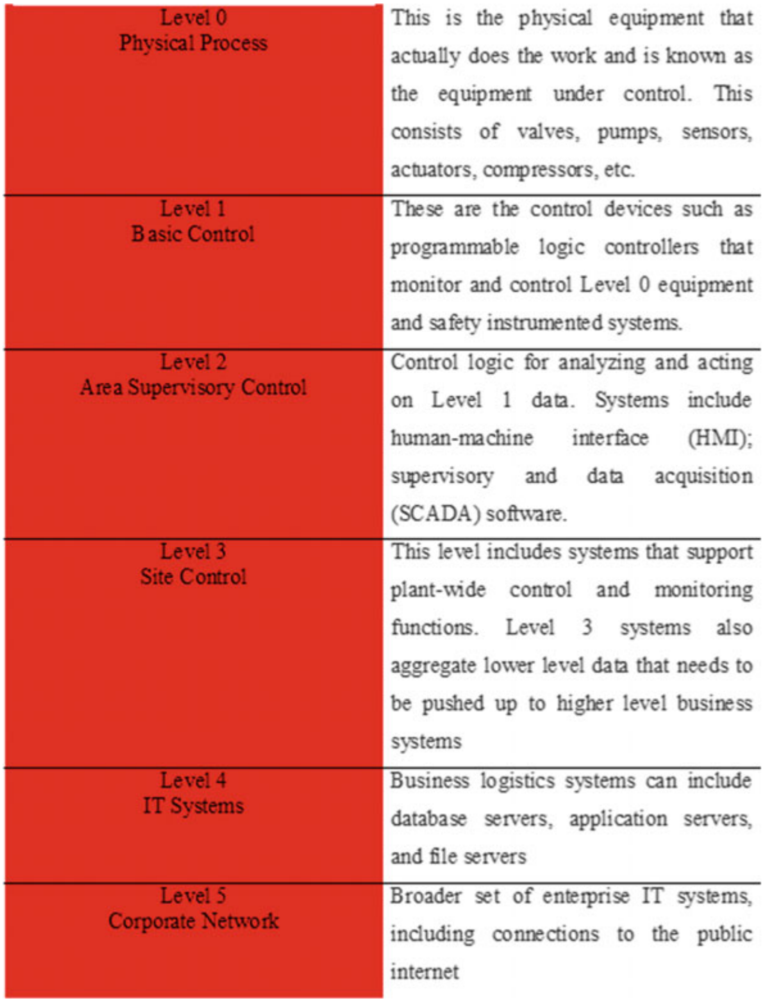
By outlining the model's foundational zones and tiers first, IT developments have made it much harder to implement the model's guidelines. Purdue's current model for OT and IT divides the two systems into three zones and six progressively more complex levels, from 0th level to 5th level (Fig. 7).

4.2.2 Purdue Model Zones

Typically, the levels are divided into three logical zones: an enterprise zone/demilitarised zone (Levels 4 and 5), a manufacturing zone (Levels 0–3). This simplistic paradigm makes it easy to determine which systems must be in constant contact with one another. Although it was not designed to be a cybersecurity framework, it has been adopted by security experts as a means of creating more secure networks as the demand for increased communication between enterprise and manufacturing zones has grown (Fig. 8).

4.3 Cybersecurity Measures Tailored to OT

Complicating existing options is the fact that several typical IT cybersecurity technologies cannot be employed in OT contexts. Scanners designed to detect flaws in OT equipment, for instance, might cause major interruptions in production. Similarly, testing upgrades to security patches on backup systems is generally impossible in production scenarios. This is particularly troubling because technology with known vulnerabilities might be functioning for decades. Nevertheless, given the worries about system interruption, there is an intuitive reticence amongst operational teams to make modifications to their OT settings.



Level 0 Physical Process	This is the physical equipment that actually does the work and is known as the equipment under control. This consists of valves, pumps, sensors, actuators, compressors, etc.
Level 1 Basic Control	These are the control devices such as programmable logic controllers that monitor and control Level 0 equipment and safety instrumented systems.
Level 2 Area Supervisory Control	Control logic for analyzing and acting on Level 1 data. Systems include human-machine interface (HMI); supervisory and data acquisition (SCADA) software.
Level 3 Site Control	This level includes systems that support plant-wide control and monitoring functions. Level 3 systems also aggregate lower level data that needs to be pushed up to higher level business systems
Level 4 IT Systems	Business logistics systems can include database servers, application servers, and file servers
Level 5 Corporate Network	Broader set of enterprise IT systems, including connections to the public internet

Fig. 7 Prude model levels

4.4 *Best Practices of OT Cyber Security*

4.4.1 A Well-Defined Chain of Command Is Necessary for OT Cybersecurity’s Adoption into Risk Management Plans

There must be a well-defined chain of command with specific roles and responsibilities in order to implement an OT security plan that receives adequate funding while complementing rather than undermining larger safety and reliability efforts. A Chief Safety Officer (CSO) should also have responsibility for both IT protection and OT security and should directly report to the Chief Operations Officer (COO); it will

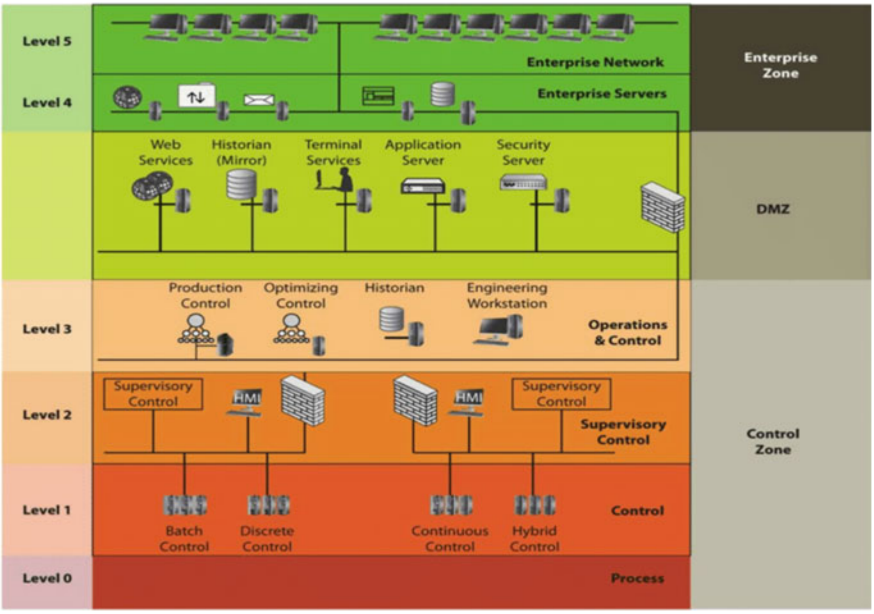


Fig. 8 Six Purdue enterprise reference architecture zones for OT

help to safeguard security expenditures and operational authority. The objective is for every company to have a responsible team for OT security working in the C-suite, and for it to be widely acknowledged that OT protection is an issue that increasingly merits board-level debate (Fig. 9).

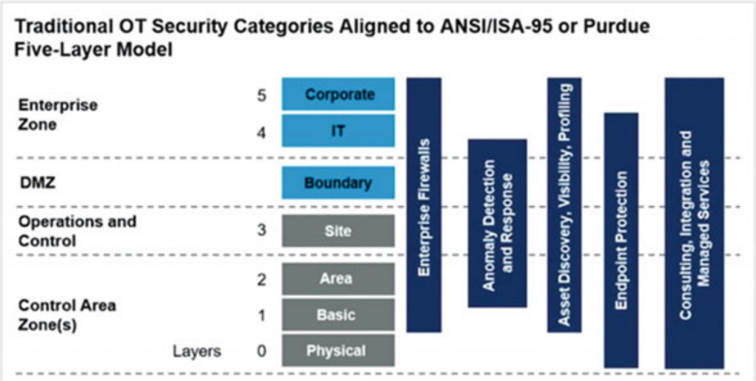

Traditional OT Security Categories Aligned to ANSI/ISA-95 or Purdue Five-Layer Model
Enterprise Zone
5
Corporate
4
IT
DMZ
Boundary
Operations and Control
3
Site
2
Area
Control Area Zone(s)
1
Basic
Layers
0
Physical
Enterprise Firewalls
Anomaly Detection and Response
Asset Discovery, Visibility, Profiling
Endpoint Protection
Consulting, Integration and Managed Services

Fig. 9 Purdue 5 layer model with traditional OT security

4.4.2 The Importance of Multi-disciplinary Teams

The National Institute of Standards and Technology (NIST) suggests assembling a multidisciplinary OT cybersecurity team with representation from management, physical security, information technology, and control system operation. It is crucial, for operational staff to understand the potential implications on systems from OT cybersecurity related activity.

4.4.3 Procedures Suggested by the Computer Security Industry Association

CIS Critical Security Protocols and the CISA Suggested Cybersecurity Practices, both are beneficial for organisations to start up a set of security baseline. CISA suggests ten best practises at a high level:

- To verify, rank, test, and deploy ICS security updates.
- Keep your system's information and settings in a safe place.
- Recognise, reduce, and protect all network links to ICS.
- Maintain constant vigilance in evaluating the safety of ICS, protocols, and connections.
- It is important to turn off any protocols, ports, and services that are not in use.
- Incorporate strong configuration management standards and activate all applicable security mechanisms.
- Use whitelisting to restrict which programs can access sensitive data and antivirus software's to keep harmful code from even getting installed.
- Make sure all managers and employees in charge of industrial control systems have taken a course on cyber safety.
- Keep an incident management plan up-to-date and test it.
- Secure ICS hosts and networks using a risk-based, defense-in-depth strategy.

4.4.4 Design Principles of NCSC

CISA recommends the UK National Cyber Security Centre's (NCSC) Design Principles and Operational Technology for organisations that want to start from the ground up. Here is a summary of the NCSC's design principles:

- Set up the context before creating a system.
- Make it hard to compromise.
- Make it hard to disrupt.
- Make it easier to find compromises.
- Lessen the effect of compromise.

4.4.5 CIS Critical Security Controls

The CIS 20 Controls are a good starting point for cybersecurity, and it can be changed to fit ICS and IoT network. The controls are put into three groups: basic, foundational, and organisational. According to Boehm [19], the top five critical security controls in ICS are:

CIS Control #1: Inventory of Hardware Assets and Control of Them.

CIS Control #2: List and Management of Software Assets.

CIS Control #3: Continuous Assessment and Repair of Vulnerabilities.

CIS Control #4: Use of Supervisory Privileges in a Managed Way.

CIS Control #5: Software and hardware on mobile devices, notebook computers, workstations, and servers can be set up to be secure.

4.4.6 How to Use Gartner's Flexible Security Model to Protect OT Cyberspace

Cybersecurity is often described as a process. It should also be continuous and change over time, which is why Gartner made the Adaptive Security Architecture (ASA). Traditional IT security was mostly about finding threats and stopping them, but the ASA prototype adds forecasting and response to make a cycle. The model can be broken down into four stages:

Predict—This involves identifying potential threats or vulnerabilities through risk assessments and AI intelligence gathering. By predicting potential risks, organizations can better prepare for and mitigate them.

Respond—This involves having a strategy for how to handle a security breach or incident or when it happens and consider other essential measures to minimise the impact of the incident.

Prevent—This involves implementing measures to prevent security incidents from occurring in the first place which include implementing security controls as well as educating users and employees about cyber security best practices.

Detect—This involves monitoring for events of a security incident and detecting it as fast as probable. This can include monitoring tools and protocols to identify and respond to security incidents in a timely manner.

PRPD strategy was first proposed by MITRE (ATT&CK) and Lockheed Martin (Cyber Kill Chain). And it aims to protect organizations from harm by predicting and preventing potential security incidents and responding effectively when it does occur. By learning more about early signs of an attack, it is easier to predict, which helps with strategy and makes other parts of the cycle easier.

4.4.7 Cyber Threat Awareness in OT

Participating in cyber threat awareness programmes, like the U.S. Department of Homeland Security's ICS-CERT and the Industrial Control System Information Sharing and Analysis Center's ICS-ISAC, is another important best practise for spotting threats early on.

4.4.8 Cybersecurity in OT

CISA gives each organisation a risk assessment document that tells them to do the following things:

- Ensure that VPNs and other remote management systems are fully patched.
- Improve system monitoring so that unusual activity can be caught early, and an alert sent.
- Use multi-factor authentication.
- Ensure that all machines have firewalls, anti-malware, and intrusion protection software installed and properly set up.
- Ensure continuity of operational processes or contingency planning are up to date.
- Raise awareness of IT support options for employees who work from home.
- Update incident response strategies to consider changes in the workforce in a distributed environment.

4.5 Preparedness and Response to Incidents: The NIST Framework

The United States Department of Commerce's National Institute of Standards and Technology (NIST) is a non-profit organisation that develops and publishes norms and guidelines for several fields of IT. The Information Technology Laboratory (ITL) at NIST creates benchmarks and tests for the IT industry, including data protection. An important framework for incident handling and response (IR) was created by ITL, Computer Security Incident Management Guide.

The NIST incident handling process is an iterative activity with built-in opportunities for learning and improvement in the pursuit of optimal security. There are four main phases preparation; detection and analysis; containment, eradication, and recovery; and post-event activity.

4.6 Plan for Incident Response (IR)

Incident management is an organisational process that lets people respond to cyber-attacks quickly and effectively. The incident response procedure involves finding an attack, figuring out how bad it is and how important it is, investigating and stopping it, putting things back to normal, and taking steps to make sure it does not happen again.

Furthermore, an incident response plan (IRP) is a written list of the steps that should be taken during each phase of a response to an incident. It should have rules for defining roles and responsibilities, plans for communication, and standard protocols for how to respond.

4.7 Key Roles of a Team that Responds to an Incident

An incident response team is crucial for carrying out an incident response plan. Full-time personnel or teams may be responsible for these tasks in a large firm, whereas in a smaller one, staff juggling many responsibilities may be asked to step up. The following are essential roles within the team:

When an event happens, it is the responsibility of at least two individuals to approve the incident response strategy and coordinate the necessary actions. After then analysts in this field are responsible for reviewing alerts, determining the likelihood of occurrences, and conducting preliminary investigations into the scale of attacks. Researchers in the field of threats are tasked with supplying further details about a given threat by sifting through data from many sources (the internet, threat intelligence feeds, security tools, etc.) to piece together a complete picture. Others who have a vested interest include executives, board members, human resources professionals, public relations experts, and top-level security personnel like Chief Information Security Officer (CISO).

4.8 ICS Implementation for NIST SP 800-73-3

4.8.1 Limiting Who May Access the Industrial Control System (ICS) Network and What They Can Do on It

Separate authentication techniques and credentials are provided for users on the corporate and ICS networks, and demilitarised zone (DMZ) network architecture is used to block communication between the two types of networks. The ICS should also have a multi-layered network architecture, with the most crucial communications occurring at the highest security and reliability layer [20].

4.8.2 Limiting Who Can Go In and Out of the ICS Infrastructure

Physically tampering with the ICS's components without authorization could cause serious problems; Use of locks, contactless cards, and security staff are only few of the many possible physical access restriction methods that should be considered.

4.8.3 Reducing the Risk of Attack on Individual ICS Components

Disabling unused ports and services, restricting ICS user permissions to only what is necessary for each position, keeping a close eye on the audit trail, and using security controls like antivirus and file integrity checking software whenever possible are all part of this strategy to avoid, hinder, predict, and mitigate malware.

4.8.4 Carrying Out Normal Operations Under Trying Circumstances

To achieve this goal, the ICS must be built with redundancy in mind. When a component fails, it shouldn't trigger a chain reaction that affects other parts of the system or create unnecessary traffic on the Industrial Control System (ICS) or other networks.

4.8.5 Accidental System Restores

Problems will always arise, which is why it is necessary to have a plan to respond to them. One of the most important aspects of an effective security programme is the speed with which a system may be restored after an attack or breach has taken place.

In order to analyse and lower risk to an industrial control system, it is essential for a cross-functional cyber security team to exchange their different domain expertise and experience. After that, proper ICS security measures can be implemented. The cyber security team should consist of at least one person from management, one from IT, one from control engineering, one from control system operations, one from the field of information and computer security, and one from the field of physical protection. In order to maintain consistency and ensure that all bases are covered, the cyber security team ought to confer with the vendor of the system's controller or integrator. Full responsibility and accountability for the ICS's cyber security should rest with site management (such as the facility superintendent) or the company's CIO or CSO. When designing a cyber security plan for an ICS, it is essential to take "defense-in-depth" into account. This strategy entails stacking many security measures so that the failure of any one layer has minimal effect on the system as a whole [21].

4.9 Key Components of Industrial Framework

Key components include the following:

Control Loop—A control loop consists of actuators such control valves, breakers, switches, and motors, and the transmission of variables. Other types of controller hardware include PLCs. The sensors send the controlled variables to the controller so that it can make the appropriate adjustments. The controller is responsible for interpreting the signals and generating the associated controlled variables, which are then transmitted to the actuators, based on the set points [22]. Alterations to the process brought on by disturbances result in the generation of new sensor signals that, once again, are sent to the controller to identify the condition of the process.

Human–Machine Interface (HMI)—Both operators and engineers rely on HMIs to keep tabs on controller settings, such as set points and control algorithms. The HMI also displays real-time data and information about the past performance of the process.

Tools for Remote Inspection and Repair—Tools for diagnosis and upkeep are used to spot and correct malfunctions before it causes serious damage, and to get back up and running after an accident with reference to the standard IEC 62443 [23].

4.10 Industry Framework

Another method for conducting top-down analysis is provided by industry frameworks. Industry frameworks offer archetypal designs of businesses operating within a given industry, and it arrange the basis of an agreement reached by representatives from that industry. Normalised functional and business process breakdowns that may map to capabilities are typically defined by these frameworks. It might provide greater granularity and impartiality than a value chain that is exclusive to a business. Not surprisingly, individual circumstances or the way a company chooses to conduct its operations and business needs can make each entity distinctive, and these distinctions can serve as a foundation for achieving a competitive advantage in particular markets.

One of the benefits of an industry framework is that contains capabilities typically align with implementations of capabilities in commercial corporate applications and outsourcing services. This is one of the advantages of an industry framework. The use of an industry framework does not imply that a conventional value chain that is well-defined should be abandoned; rather, the two working together define greater insight for the definition of shared capabilities [24].

4.10.1 Authentic, Real-Time, Safety-Certified Kernels

A considerable number of built-in safety mechanisms are available with the SCIOPTA 61508 kernel and IEC 61499, which are a pre-emptive multi-tasking high performance real-time kernel. SCIOPTA is an excellent alternative for use in applications that must conform to stringent safety criteria since it employs a kernel that directly passes messages. This makes it an ideal candidate for use in such applications [25].

4.10.2 Safety Certified Data Transfers

By performing checksum validation on message data areas, the SCIOPTA kernel is able to monitor the movement of data between processes. The workload of the creator of safety software is significantly reduced thanks to these verified functions. When it can be delegated this responsibility to the kernel, the overall development time and costs are cut down significantly.

A header, a data region that can be any size, and an end-mark that is validated by the kernel make up the SCIOPTA message and ETFA [26]. The sender, owner, and addressee of the message all have their respective process IDs included in the message's header.

4.10.3 No Shared Memory

Traditionally, shared memory has been used as the inter process communication protocol in real-time operating systems. Users are responsible for assigning semaphores to specific data areas and kinds, as well as implementing semaphore protection for shared memory.

No form of shared memory is needed in a SCIOPTA-based system. Direct communication provides a safer method of transmission. Information is packaged in messages, and the kernel is responsible for their security by managing data ownership.

4.10.4 Controlled Storage of Information

SCIOPTA modules can be used to organise and manage a collection of related processes. Each module has the potential to have a maximum of 128 pools available to store SCIOPTA messages. Modules and pools might share the same section of memory or be located in different sections. Using a Memory Management Unit and the SCIOPTA Memory Management System (SMMS), full memory protection can be attained (MMU) [27].

4.10.5 Certified by TÜV

SCIOPTA has been given approval for use in systems up to SIL3 by the TÜV in Munich in accordance with IEC61508/EN50128 [28].

4.11 IEC 61508

IEC 61508 is the name of the international standard that focuses on safety-related systems that mix electrical, electronic, and/or programmable electronic (E/E/PE) instruments and devices. The full title of the standard is the International Electrotechnical Commission Standard for Safety-Related Systems that Combine Electrical, Electronic, and/or Programmable Electronic [29].

Despite its origins in the automation and process control industry, IEC 61508 is finding increasing acceptance in other sectors, like the automotive and medical industries, where safety and dependability are of paramount importance.

The 7 Parts of IEC 61508

- IEC 61508-1 Defines common requirements.
- IEC 61508-2 States all the safety-related systems requirements.
- IEC 61508-3 Gives software requirements.
- IEC 61508-4 Defines all the definitions and abbreviations.
- IEC 61508-5 Some techniques for determining the level of safety integrity.
- IEC 61508-6 By using IEC 61508-2 and -61508-3 correctly gives some suggestions.
- IEC 61508-7 Defines an outline of methods and procedures.

4.11.1 Market Guide for Operational Technology Security

The convergence of IT, IoT, and OT environments has increased the complexity and vulnerability of previously isolated OT/ICS networks and newly designed cyber-physical systems (CPSs). As a result, there is a necessity for an all-encompassing, automated approach to asset discovery, risk assessment, and helping to avoid downtime. "*By 2025, 70% of asset-intensive organizations will have converged their security functions across both enterprise and operational environments*"—by Gartner [30].

Report to Discover

- The factors that are driving the transition of the OT security market from a focus on OT networks to a focus on CPS assets.
- Market dynamics such as increasing threats, exposing vulnerabilities, a continuous skills deficit, and growing laws, directives, and frameworks.

- Suggestions for "anchoring security efforts to operational resilience" in the face of growing threats, by implementing an integrated security strategy that goes beyond legacy OT systems.

4.12 Differentiation Between ISO/IEC/IEC 62443, NIST Cybersecurity Framework, and ISO/IEC 27001

A set of standardised risk mitigating strategies is needed in order to take a methodical approach to the implementation of a cyber security programme. These strategies should be developed through the collaborative efforts of regulatory institutions, industry associations, government agencies, and technology specialists. Organizations are able to not only reduce the risks to an acceptable level with the assistance of a single well-defined procedure or a combination of procedures that are also well-defined, but they are also able to track the progress, evaluate any gaps that exist between the current and targeted security levels, and improve the overall efficiency of their security system.

International standards like as ISO-27001, NIST Cyber security Framework, and ISA/IEC 62443 are a few illustrations of those that are extensively used and widely embraced. These standards offer a comprehensive guidance and absolute effectiveness in safeguarding IT and OT systems.

4.12.1 ISO-27001

Beginning around the turn of the millennium, several independently developed industry standards began to converge into what is currently known as the ISO set of guidelines for security management of information. The International Organization for Standardization (ISO) is now widely recognised as one of the most thorough standards for establishing and maintaining an effective information security management system. Information security is the primary focus of the ISO-27001 standard, and it helps businesses prioritise and solve their needs for keeping data private, secure, and accessible [31].

A plan-do-check-act cycle, which is more often known as the PDCA cycle, lies at the core of it. This cycle can trace its origins back to quality assurance in production contexts (Fig. 10).

The cycle of plan-do-check-act can provide assistance in establishing the framework of the organisation, defining the scope and objectives, determining the requisite competence, and creating a written policy. This is supplemented further by the evaluation of risks, the planning of treatments, the selection of available controls, and the

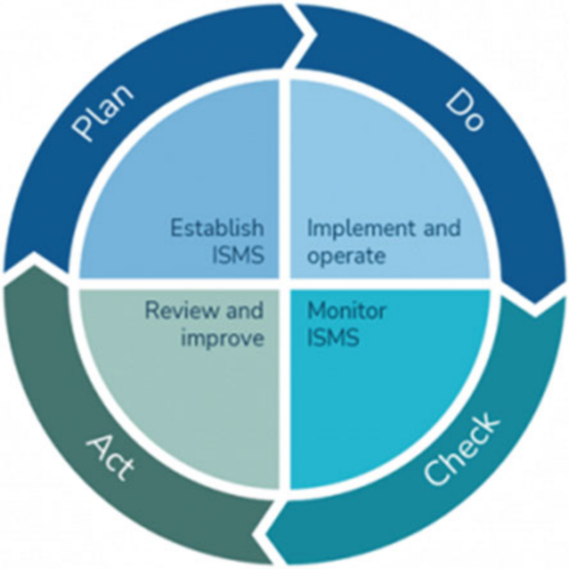


Fig. 10 PDCA cycle for quality assurance

implementation of those controls [32]. In addition, constant innovations and improvements are able to fulfil the ongoing demand for risk reduction. In a nutshell, ISO-27001 provides businesses with a step-by-step guide that assists in effectively implementing the necessary security capabilities and minimising risks using an approach that is iterative and scalable for successive degrees of development.

The Need for OT Security Standards

IT and OT systems are often different in terms of the technological nature and scope of their operations. Murray et al. [33] stated in their work that the approach to security that is taken with an OT system needs to be adapted to the specific demands of that system. Since many of the controls that were implemented to manage the security of IT systems are not relevant to OT systems, a distinct set of industry standards is required in order to satisfy the safety needs and limit the risks that are connected with them. Both the NIST Common Security Framework (CSF) and the ISA/IEC 62443 standard were developed expressly for the for the sake of establishing guidelines to ensure the security of industrial control and automation systems.

4.12.2 ISA/IEC 62443

By deriving from the controls defined in ISA/IEC 62443 delves even further into the particulars of the application process. The set of standards known as ISA/IEC 62443 provides a framework for managing and securing operational technology (OT) systems, as well as for monitoring and preventing potential attacks in the future. It enables organisations to identify their assets and keep track of their asset inventory, to group assets with similar security requirements into zones, and to define conduits for the establishment of a secure communication channel within and among these zones. Afterwards, the zones exposure to danger is evaluated, and the proper levels of security are implemented there. Controls are decided upon and put into place in accordance with the predetermined levels of safety that are associated with each zone. In light of raising concerns over the safety of industrial control systems, the International Society of Automation (ISA) has established norms to guarantee their security; Using the knowledge of experts in industrial automation and control systems, the Industrial Systems Association (ISA) developed a set of standards (ISA/IEC 62443) to detect and eliminate any security flaws (IACS) [34].

ISA 62443 is a set of standards, technical papers, and supporting materials whose overarching goal is to create a flexible framework that permits addressing current and future vulnerabilities in IACS and applying essential mitigations in a methodical, defensible manner. Standards, technical reports, and other supporting materials can all be found inside ISA 62443. It is imperative to have a clear understanding of the purpose of the ISA 62443 series, which is to create extensions to enterprise security that adapt the needs for business IT systems and integrate them with the particular requirements for robust availability that are needed by IACS [34].

According to Fachot [35], the main sections of the series are as follows:

- General (62443-1): This category contains items that discuss themes that are present throughout the entirety of the sequence.
- Policies and regulations (62443-2): The components of this set pay special attention to the rules and regulations surrounding the protection of IACS.
- Requirements for the System (62443-3): The elements that make up the third group are those that deal with requirements for the method.
- Requirements for components (62443): More specific and precise requirements for the development of IACS products are covered in the fourth and final group of elements.

The following sections of the standard demonstrate a detailed definition of the security requirements across the software development life cycle (SDLC) for industrial control systems:

- **ISA-62443-3-3**—Specific operational and technological criteria for IACS safety are established in this sequel. Within the scope of the standard's definitions are located seven sets of foundational requirements (FR), as well as four tiers of security levels (SL). The level of security that must be maintained by the system is established through the use of risk analysis. System requirements, or SRs, can vary widely depending on the amount of security desired. The standard defines SRs by referring to the applicable FRs in various places. Some of the SRs contain modifications to the requirements that apply to all the SLs, while others only apply to a subset of the SLs.

- **ISA-62443-4-2**—Includes detailed descriptions of embedded parts, network parts, host parts, and software parts, and more. The standard consists of a total of seven fundamental requirement groups and four security level groups (SL-Cs). This standard's requirements are derived from ISA-62443-3-3 (system security requirements); however, they are more narrowly focused on parts of the control system rather than the entire system [36].

In addition to ISA 62443, there is also NIST Special Publication 800-82, which is an alternate framework. In compliance with the Federal Information Security Modernization Act (FISMA) that was passed in 2014, the National Institute of Standards and Technology (NIST) designed and developed this [37].

4.12.3 NIST 800-82 Standard

Guidelines for National Institute of Standards and Technology Cyber security offers asset owners a comprehensive roadmap for securing operational technology (OT) systems in their organisations. It is basically built to assist companies in streamlining the required processes, defining and prioritising the security level for both existing risks and anticipated hazards, and managing the budget in accordance with these considerations [38]. Users of the NIST Cyber Security Framework are given general guidance toward the implementation of cyber security measures that are in keeping with the framework's five basic functions (Fig. 11).

Among the many different NIST standards, the NIST 800-53 and the NIST 800-82 are two that stand out as particularly important. While NIST 800-53 is utilised across the industry for the purpose of managing the cyber security needs of information systems, NIST 800-82 is utilised for the purpose of managing the privacy and security controls of operational technology (OT) systems. Through the use of an "overlay," which is made possible by NIST 800-82, businesses are able to modify certain controls from NIST 800-53 so that they better meet the requirements of OT. The written recommendations of the NIST provide an overview that is both comprehensive and detailed of all the security capabilities of these standards.

Stouffer et al. [39] found a guide for ensuring the security of industrial control systems may be found in the Special Publication 800-82 that was published by the National Institute of Standards and Technology. It is feasible, as stated in the executive summary of Publication 800-82, to consider it an "overlay" to Publication 800-53. Guidelines for applying the security measures detailed in NIST Special

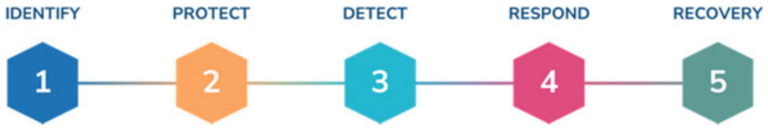


Fig. 11 NIST cybersecurity framework's five functions

Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, have been developed by the National Institute of Standards and Technology (NIST) in collaboration with the community of ICS professionals working in the public and private sectors. A significant number of the controls in Appendix F of NIST SP 800-53 can be directly applied to ICS as written, however, many of these controls also require ICS-specific interpretation and/or augmentation [10].

In fact, NIST SP 800-82 cites multiple other NIST SPs throughout the document and offers "ICS-specific Recommendations and Guidance" for every possible scenario.

The Importance of Security Policies

The lifetime of control systems includes not only the creation, testing, and release of systems and software, but also the accompanying rules and procedures. The absence of a security policy in and of itself might create conditions that are conducive to the introduction of vulnerabilities in industrial control systems.

To define roles and duties, provide direction for programme implementation, and outline how violations will be handled, a thorough and well-documented security policy is required. One of the most important factors that determines whether a security programme is successful is the level of support and governance that it receives from management. In-depth discussions on policies and procedures are presented in both ISA/IEC 62443 and NIST SP 800-82; however, the two documents take somewhat dissimilar approaches to the subject matter [40].

This subject is covered in depth by the IC4F and 62443-2 category, which is organised into four subparts that focus primarily on developing a management system for cybersecurity is suitable for IACS settings [41]. This is also known as an IACS security programme or, more generally, an IACS security management system, according to the standard. These two terms are synonymous with one another. Moreover, the requirements for a successful IACS security system are outlined in the first part (62443-2-1), and assistance for developing such a system is provided in the second part (62443-2-2) of this document. Although, the third section (62443-2-3) details the best practises for the system's patch and change management, while section four (62443-2-4) restates the security programme criteria with an emphasis on the responsibilities of IACS service providers [42].

The National Institute of Standards and Technology's Special Publication 800-82 is another helpful reference for drafting and implementing policies and procedures. In fact, it devotes an entire section in Appendix C to the topic of detecting vulnerabilities and predisposing factors that are related to the absence of policies and procedures.

4.13 Selecting the Right Standard/Framework for OT Cybersecurity

Responses from a variety of industrial verticals to a survey conducted by SANS and titled "SANS ICS/OT survey 2021" revealed an interesting combination of OT Cybersecurity standards. The top 5 standards that control systems are mapped to are NIST CSF, ISA/IEC-62443, NIST 800-53, and NIST 800-82, and ISO 27001 [43]. There are also a few standards that are unique to the industry, such as the NERC CIP, as well as standards that are unique to the region, such as the NIS Directive and the Qatar's ICS security standard [44] (Fig. 12).

In most cases, a combination of these standards will be utilised in order to meet the specific requirements of certain business. These requirements might be affected by the region or the overall environment in which the company operates, in addition to other conditions or goals connected to your specific organizational context. It is possible that the implementation of these standards could successfully establish a cyber-secure industrial environment. This would make it possible for OT defenders to combat threats, while identifying areas-of-emphasis for the protection of a critical infrastructure in a vividly streamlined manner. The ISA/IEC 62443 standard and the NIST SP 800-82 standard provides exhaustive coverage and direction for industrial control system (ICS) security respectively [45]. Despite the presence of other

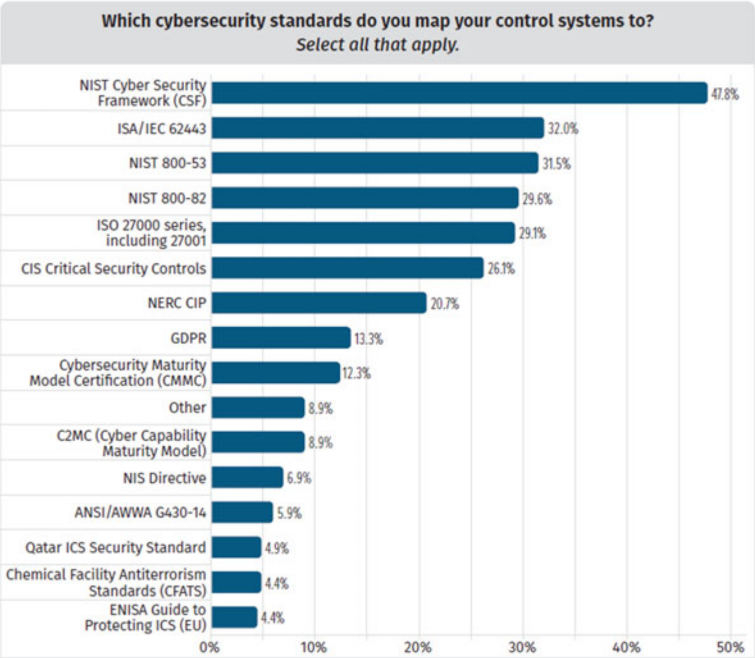


Fig. 12 Top utilised ICS international cybersecurity frameworks

security standards, initiatives, and best practises in this field, these two frameworks have gained the most traction and attention. Because connected systems are always susceptible to new risks, it is necessary to take a multi-faceted approach in order to counteract the many dangers. The implementation of a security framework is one way to assist enterprises in moving toward a more holistic strategy [45].

The choice of a framework will, in many instances, be determined by the industry and the accompanying regulatory drivers, which may require a particular framework. Therefore, because various regulators may need various organizational structures and each framework has a plethora of knowledge concerning the safeguarding of industrial control systems. For instance, organizations in the public sector are typically expected to adhere to the NIST standards.

5 Research Methodology

This part offers detailed of how the study was performed along with method used.

5.1 Research Process

The research process indicates to the process conducted by researchers to develop and put in writing feasible research. This often involves identifying, finding, evaluating, and analysing various information research related facts and information.

5.2 Research Methodology

Research methodology describes the methods' systematic analysis that be appropriate to a research field. Particularly, it is the phase where the researchers consider several models and methods that will be used in their studies. Irny and Rose [46] stated that Research methodology generally involves hypothesis, phases theoretical model and quantitative or qualitative techniques.

In this study, the results are established based on open-source data; mix methodology model is used: the qualitative and quantitative methods are used to investigate the available datasets required for the classifier training. Literature review was retrieved from online archives, such as: Google Scholar, Web of Science, Science Direct, and IEEE Xplore and so on. Additionally, news, articles, books, related industry descriptive reports and articles initiated by cybersecurity professionals in career were also utilised to enhance the background research. As mentioned earlier, the dataset chosen greatly affects the performance of the classifier. The dataset should be of moderate size and high quality so that the feature extraction procedure can train the algorithm efficiently.

5.3 Data Collection and Data Analysis

Researcher must determine the applicable methods and techniques to implement for the data collection and analysis phase. The date used to conduct this research secondary data that collected from several open-source online archives.

5.4 Legal and Ethical Consideration

Proposed study has to comply with relevant ethical and legal issues. The author has to take into consideration the academic policies and guidelines extremely and adhere to the academic codes of conduct for the duration of the research establishment. Research actions, events and elements involving data analysis methods, data collection and theoretical and practical studies all be required to fulfil with legal guidelines.

The research mechanisms, activities approach, Internet and computer uses must comply with legal obligations and responsibilities in the United Kingdom Computer Misuse Act 1990 (legislation.gov.uk),

The collected data will be used exclusively for this project and will be erased after use. Only data in English language will be compiled and evaluated and must obey with and the GDPR and DPA (2018) (Legislation.gov.uk).

6 Proposed Architecture for Automation Energy System Applying the IEC 62443 Standard

Cyber-attacks on critical infrastructure systems like Secondary Distribution Automation (SDA) systems have been in the news frequently as of late. The immaturity of their security architecture makes them vulnerable to cyberattacks. Because of the potential for significant financial losses, the potential loss of intellectual property, and the catastrophic damage to the company's reputation on the market, securing these systems from attacker actions has been an increasing area of focus. To approach the cybersecurity problem of these important systems comprehensively, an analysis based on the international standard IEC 62443 is warranted. For Industrial Automation Systems, this specification represents a worldwide consensus on the best security procedures (IACS). To protect against attacks from numerous directions, IEC 62443 employs a system called defence in depth, which has a variety of security layers and predetermined degrees of security. The aim of this proposed work is to test the implementation of the IEC 62443 Standard in a representative SDA energy system and to raise the level of security maturity in such installations to an acceptable level.

The International Electrotechnical Commission (IEC) 62443 was developed by the ISA (the International Society of Automation) as a set of standards, technical

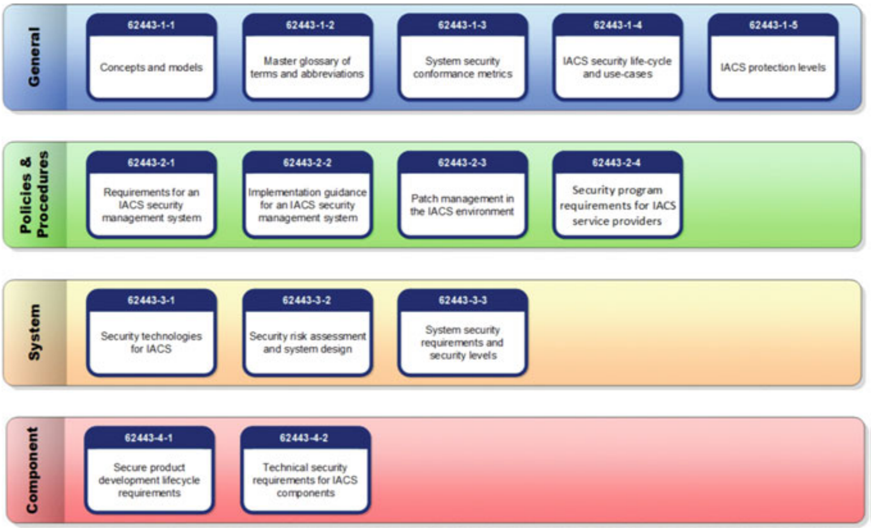

General
62443-1-1
Concepts and models
62443-1-2
Master glossary of terms and abbreviations
62443-1-3
System security conformance metrics
62443-1-4
IACS security life-cycle and use-cases
62443-1-5
IACS protection levels
Policies & Procedures
62443-2-1
Requirements for an IACS security management system
62443-2-2
Implementation guidance for an IACS security management system
62443-2-3
Patch management in the IACS environment
62443-2-4
Security program requirements for IACS service providers
System
62443-3-1
Security technologies for IACS
62443-3-2
Security risk assessment and system design
62443-3-3
System security requirements and security levels
Component
62443-4-1
Secure product development lifecycle requirements
62443-4-2
Technical security requirements for IACS components

Fig. 13 IEC 62443-standard

reports, and other materials that define the steps necessary to implement electronically secure Industrial Automation and Control Systems (IACS), in order to meet all concerned with entirely forms of industrial automation, application, control, and key infrastructure, including but not limited thereto SCADA, power plants, transmission lines, distribution networks, utilities for gas, water, oil, etc. This technical definition focuses on cyber security, which encompasses hardware, software, networks, and configuration settings.

As demonstrated in Fig. 13, IEC 62443 Standard covers a wide range of stakeholders involved in the manufacturing, design, deployment, and industrial automation management and control systems, including end users. The four main sections of IEC 62443 are "General," "Policies and Procedures," "System," and "Component." It is crucial to notice that while some things have been published already, others are still in the process of being created, evaluated, or planned.

6.1 Using IEC 62443-Based Safety Systems

6.1.1 Segmentation of Network

To safeguard a network, segmentation of network is a potent defence strategy. The essential concept is to place network components that require a similar level of security within the same zone and then to limit access to that zone in both a physical and logical manner. Network segmentation reference proposes a network separation that creates three distinct network zones [47]:

Trusted Zone—In order to meet the Trusted Zone's special communication requirements, further precautions must be taken. As a result, a firewall surrounds it, and trustworthy process networks are a part of it. In this context, "Trusted Zone" refers to the areas around the Control Zone, the Control Centre, and the primary Substations.

Demilitarised Zone (DMZ)—Between the safe area and the dangerous area is where the DMZ is set up. This is the area where all outside connections to the security zone are monitored and managed. When located inside the Command Centre or primary substations, the service PC is considered to be in a Demilitarised Zone (DMZ), which adds another degree of security for off-site personnel.

Untrusted Network—The security measures of the "untrusted network" are either undefined or insufficient.

6.1.2 Interfaces, Conduits and Data Flow

Human Machine Interfaces (HMIs) or physical interfaces can be used for the solution components' interaction. IEC 62443 requires, in general, that any vulnerable or unused interfaces be turned off. Safely connecting devices requires categorising IP-based communication protocols according to their purpose; Operation entails all protocols principally required for the operational functioning of the power utility. Various IEC and NTP standards are good examples; Engineering covers all processes that are implemented to manage product setup, upkeep, and problems. All engineering equipment is a good example; And lastly remaining protocols are classified under the "support" heading, the Simple Network Management Protocol (SNMP) and other remote access protocols are a couple of [13].

With the goal of protecting the integrity of data transmitted between different networks in mind, two methods have been established. First is secures data transmission between the SDA Control Area and the Control Centre/Basic Substation using Virtual Private Network (VPN) between gateways. Since just part of the communication line will be secured, this method is considered "bare minimum" security. Secondly is the communication channel between devices in the SDA control area and network devices in the Control Centre/Basic substation is safeguarded by a Virtual Private Network (VPN) using Internet Protocol Security (IPSec). By implementing that, secure communications end-to-end will be optimised.

6.1.3 Controlling Identity and Permitting Entry

The topology of the network within the design mandates two access methods, distant access (through DMZ) and public access in the field, for maintenance and engineering purposes. Services PCs are used to verify user identities in both environments, however after a project is handed over, it is advised that DMZ access be limited further.

6.1.4 Hardening to Lessen Vulnerability to Attack

To put system hardening into action, it must ensure that all unnecessary service's ports and connections are closed or deactivated on all network nodes (including switches, routers, RTUs, and computers). In other words, all engineering protocols and tools are mapped, and only those that are necessary for keeping the system running are allowed to be turned on.

A protected repeater is a crucial part of an IEC 62443-compliant secure solution. There is an absolute need for Hardening in this scenario. Blocking unused ports and using a MAC address filters to restrict access to the network to authorised devices are two examples of the precautions used to provide a sufficient level of security. Disabling Telnet remote access and HTTP, two examples of services and protocols known to be vulnerable, is a good place to start.

6.1.5 Security Against Malware and Other Attacks on OT Systems

Some generic and preferable product qualities were taken into account to ensure the system's continued functioning: digitally signed firmware that can continue to operate normally under attack; validation mechanisms to ensure that only valid setup commands and blog posts with the correct syntax are accepted; firmware that has been subjected to extensive security testing during development; firmware that can function normally regardless of whether or not it is connected to the internet. All these safeguards make it feasible to protect against firmware tampering, Denial of Service (DoS) attacks, unexpected product behaviour, and unauthorised modifications to the system's configuration.

To prevent devices from being exploited as a vector for propagating system viruses, anti-malware software is now required to be installed on all service PCs. It is expected in the strategy that the IT and industrial networks are partitioned at the control centre level to lessen the attack surface.

6.1.6 System Monitoring

It is vital to build a monitoring system in order to keep track of what is going on in the platform, such as unusual equipment actions (e.g., attempts to configure changes or erroneous logins) and the behaviour of your network (suspect packages and protocols). At the level of the control centre, it makes appropriate to implement a "Logging" server to receive such data. The syslog protocol can be used to send and map cyber security data to a SIEM or to transmit data from internal locations on the equipment using a normal distribution protocol (such as DNP3) to a SCADA system.

7 Data Analysis and Critical Discussions

7.1 Case Study

"Tracing security requirements in industrial control systems using graph databases for wind turbine cases."

Because there are numerous numbers of different system and security standards, it is crucial to record the interdependencies and hierarchies between them. As a result, the current techniques for specifying security requirements fail to adequately capture such structure, which in turn complicates currently existing and traceability and extends the time and money needed to construct certified ICS. This paper proposes a novel paradigm for ICS requirements repositories, one that makes use of LPGs (Labelled Property Graphs) to chain store both demands for standards-based and system-specific, with the latter being organised according to predefined relationship types. Finally, the document achieves the requirements traceability by integrating the proposed requirements database with ICS tools during the design phase. A wind turbine scenario study highlights the promote efficiency in our system. These papers illustrate that utilising labelled property graphs inevitably results in a solid requirements traceability matrix, although, its present adaptable requirements change management process that can be used to accommodate future modifications to both the development and certification processes.

There must be security in place for all the crucial parts used in ICS deployments. IEC 62443 is one of many ICS-specific security standards, provides stringent yet generic security criteria. Such requirements' applicability to a given project is not always obvious and can often be difficult to parse. Multiple organisations must reach consensus on a common set of product-centric security requirements in order to move forward with the certification process for security standards. Therefore, in a safety certification program, all parties (users, vendors, and certifying bodies) must reach consensus on a security needs engineering strategy that is practical for them. It is crucial to maintain the security of the entire process by correctly mapping required functionality to security standards requirements.

Modelling and implementing a security wind turbine system allowed researchers to examine the challenges inherent in monitoring and monitoring security requirements in ICS.

7.2 Contribution of This Research Work

The key contributions of this research are as follows:

1. With an emphasis on requirements structure and linkages, the papers demonstrate a unique repository approach that maintains the IEC 62433-4-2 specific security and Cyber Security Requirements Specification (CRSC) as Labelled Parameter Graphs (LPGs) in various subsets.
2. The papers propose and illustrate a method for integrating the repositories with Industrial Control System design tools in order to facilitate end to end supplies traceability.

7.3 Detail Study on Safety–Critical Wind Turbine ICS Standards

To illustrate the use of the repository and the related traceability procedure, a case study of a safety–critical Industrial Control System wind turbine is implemented. The wind turbine system makes use of a master–slave configuration of many Programmable Logic Controllers (PLCs). The nacelle's slave PLCs take orders from a master PLC located at the wind turbine's foundation. In addition, the PLCs send data to the control system, which in turn sends the information to SCADA or an enterprise system. Due to its central role in regulating the wind turbine's mechanical operations, the data exchange between the master and slave Programmable logic controllers is of the utmost importance. An attacker can compromise the control device system by injecting a rogue instrument in the middle of both the master and slave PLCs, blocking the nacelle and pitch gears from functioning properly. For an ICS to function, there must be reliable lines of communication between all its parts.

7.3.1 Step 1: Generation of Requirement Graph

The CSRS's recommendations for protecting wind turbines are incorporated into the case study.

Each requirement and sub-requirement, such as CRa, CRb, AR, IRa and IRb is treated as a node in the LPG that is generated from these specifications. This method of organising the security standards from several specification papers aids in drawing attention to the connections between the various levels of these hierarchical needs. To ensure that each system's CSRS graph is distinct, the LPGs are developed in isolation from one another. However, the same safety adjusted accordingly can be utilised with different CSRS graphs. In addition, the structure of the requirements is dependent on the specific CSRS graph [48].

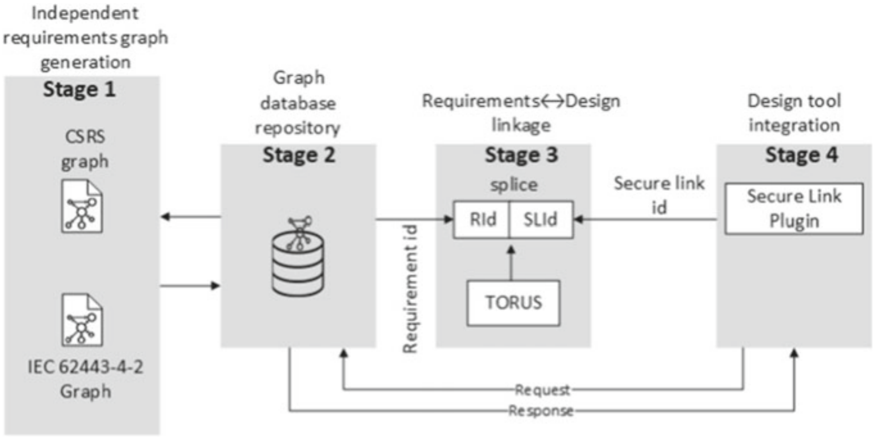


Fig. 14 Process overview of creating an LPG security requirements repository

7.3.2 Step 2: Repository for Graph Database

An LPG's organisation makes it possible to store and manage the repository more effectively. The relations between data are produced and put in storage for the duration of the database building step, which is a major benefit of utilising LPG. Complete needs can be queried from the repository using a variety of graph patterns including trees, chains, chain sets, and forests. In addition, the properties of nodes and edges in an LPG can be used to filter the result sets. Here, the graph database tool's has created querying features to use. It could be seen the entire chain of dependencies between each criterion under a security umbrella. As an added bonus, the proposed repository's numerous partitions are highly reusable by both manufacturers and the ICS developer community (Fig. 14).

7.3.3 Step 3: Requirement to Design

TORUS is an application for tracing requirements to their implementation, and it does so by employing splices. Splice meta data in TORUS keeps the repository link alive with a need identifier from the wind turbine system's CSRS. Traceability between the security repository's requirements and the design phase is facilitated by TORUS's integration with the repository.

7.3.4 Step 4: Design Tool with Security

The integration of secure connections and TORUS with a need's repository is briefly introduced in this secure-by-design technology for ICS. However, this article demonstrated the concept's actual applicability and consolidate it. Therefore, End-to-end requirements traceability is realised by encrypting the safe bond and the wind turbine Cyber Security Requirements Specification necessary identifiers in a TORUS splice. The verification and certification of security requirements is aided by the visible and complete traceability matrix produced by the proposed repository concept.

7.4 IEC 62443-4-2 Property Graph

Using the Neo4j graph database tool, it explains how the formalism can be put into practise in meeting the security standards laid out in IEC 62443-4-2 [49]. As demonstrated an LPG specification of FR3, one of the seven FRs in the specification, which is the foundation for realising the ICS integrity objective, FR3 is selected due for its pertinency for security integrity needs IRa and IRb for the wind turbine system, as shown in Table 1. IRa demands data integrity in the middle of both the wind turbine PLCs and peripherals, whereas IRb involves security integrity of data among master and slave PLCs. In cooperation are related to system integrity requirement FR3 as defined by IEC 62443-4-2 (Fig. 15).

Table 1 Wind turbine security requirements

Goal	RID	Example of security requirement (SR) of wind turbine PLCs	Security level
Confidentiality	CR	The master and slave PLCs shall ensure the confidentiality of the data in transmission and at rest	
	CRa	Data communication between master and slave PLCs shall use appropriate encryption algorithms	SL-C 2
	CRb	Critical parameters shall be not be persisted on the master and slave PLCs in order to ensure the confidentiality of data for discharged devices from the system	SL-C 4
Authentication	AR	Any access to the PLC (master/slave) shall be provided after appropriate authentication based on role-based identification	SL-C 1
Integrity	IR	The system shall ensure the integrity of ingress and outguess data	
	IRa	Communication between master PLC and external components shall use appropriate methods to ensure the integrity of the data	SL-C 4
	IRb	Communication between master and slave PLCs shall support communication integrity checks	SL-C 4

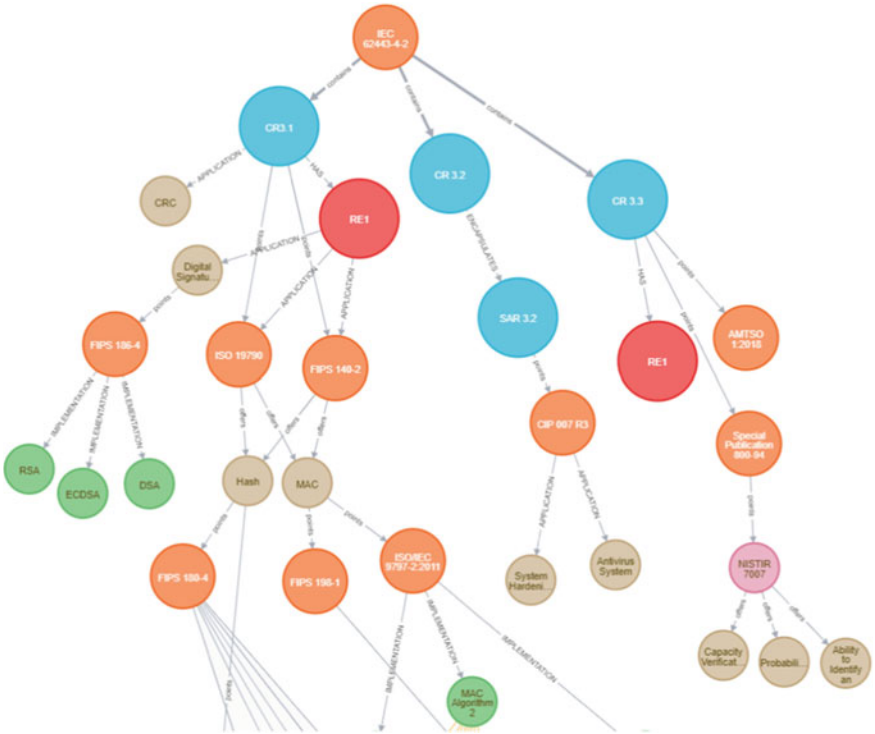


Fig. 15 Integrity property graph produced by Neo4j

7.5 Implementation of Security Standards

A single Neo4j above graph file includes the wind turbine case study's IEC 62443-4-2 and Cyber Security Requirements Specification parameter graphs, functioning the same as a logical repository [49]. Using Cypher queries, the author generated two distinct property graphs. A CSRS wind turbine's property described in Fig. 16, is generated using the Cipher query in Listing 1. Similar queries can also be used to construct the IEC 62443-4-2 graph. For instance, SL-C:4 on line 4 of Listing 2 describes the above label the edge of CR3.1 and its RE1. These are essential for sorting out the security standards. To reach CR3.1's desired level of capability security, level 4, this aids in defining a route to the necessary cryptographic primitives. The query fragment shown in Listing 2 is too long to be displayed in full here.

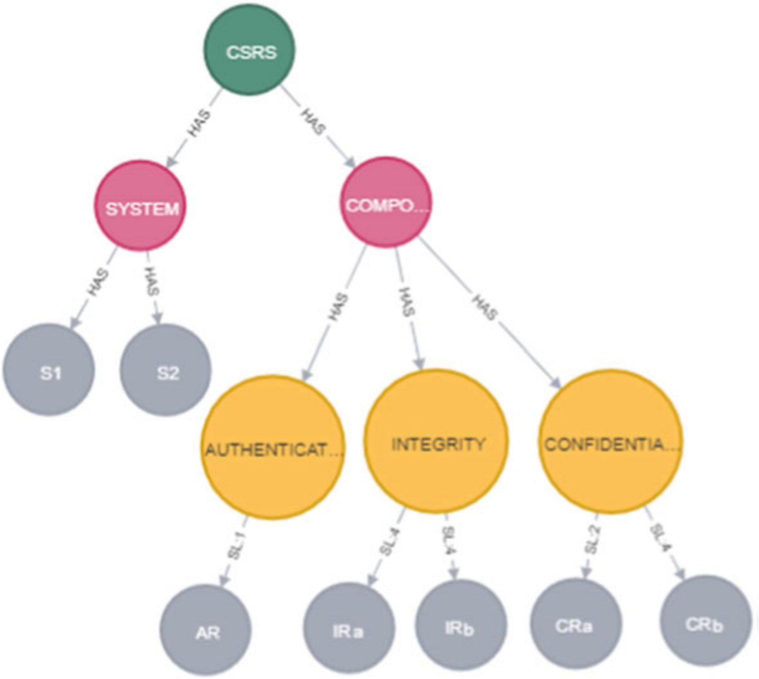


Fig. 16 A CSRS graph of a wind turbine system created in Neo4j

Listing 1

```
CREATE (cr:CSRS{name:"CSRS"})-[:HAS]->
(co:COMPONENT{name:"COMPONENT"}),
(cr)-[:HAS]->(sy:SYSTEM{name:"SYSTEM"}),
(sy)-[:HAS]->(:LEAF{name:"S1"}),
(sy)-[:HAS]->(:LEAF{name:"S2"}),
(co)-[:HAS]->(con:CONFIDENTIALITY
{name:"CONFIDENTIALITY"}),
(co)-[:HAS]->(auth:AUTHENTICATION
{name:"AUTHENTICATION"}),
(co)-[:HAS]->(inte:INTEGRITY
{name:"INTEGRITY"}),
(con)-[:SL-C{type:2,name:"SL-C:2"}]->
(:CON_REQ{name:"CRa"}),
(con)-[:SL-C{type:4,name:"SL-C:4"}]->
(:CON_REQ{name:"CRb"}),
(auth)-[:SL-C{type:1,name:"SL-C:1"}]->
(:AUTH_REQ{name:"AR"}),
(integ)-[:SL-C{type:4,name:"SL-C:4"}]->
(:INT_REQ{name:"IRa"}),
(integ)-[:SL-C{type:4,name:"SL-C:4"}]->
(:INT_REQ{name:"IRb"})
```

Listing 2

```
CREATE (s6244311)-[:contains]->(fr3),
(fr3)-[:points]->(s6244342),
(s6244342)-[:contains]->(cr31),
(cr31)-[:HAS {SL-C:4}]->(cr31RE1),
(cr31RE1)-[:APPLICATION]->(sISO19790),
(cr31RE1)-[:APPLICATION]->(sFIPS1402),
(cr31RE1)-[:APPLICATION]->(mDigitalSig),
(mDigitalSig)-[:points]->(sFIPS1864)
```

Another aspect of Neo4j that works well with our planned repository is its ability to execute and store a series of searches in a specific database. When a query is run, its results are stored in the database, opening the door to the possibility of saving several views of the data for later use. The graph database also stores the individual entities that resulted from the IEC 62443-4-2 FR3 and the wind turbine CSRS required inquiries in the listings. Thus, both graphs can be merged, in other word, the information can be obtained using additional Cypher queries. For instance, according CSRS, IRa, a security criterion for wind turbines, must be provided at SL-C 4. Recommendations for carrying out the security standards specified in IEC 62443-4-2 are existing in a structure of LPG nodes, which are stored in the repository that the report offer. This set of rules covers the use of common security methods and the corresponding cryptographic primitives. The existing set of rules is not comprehensive; for example, the IEC 62443-4-2 norm only specifies a small subset of the possible standard encryption protocols and procedures. For the library to be utilised in large-scale industrial control system (ICS) projects, the standard's LPG graphs must be exhaustive.

Ultimately. secure connection and repository act like anchors in the structure of cybersecurity algorithms/methods represented by the leaf nodes of the property graph of IEC 62443 in the repository and implementation of that functional block within the IEC 61499 Industrial Control System application. complement each other. To each protected connection is recognized by a unique identifier indicating to it [48].

End-to-end traceability of security requirements combines repositories with design patterns to enforce communication security constraints via secure connections [50], and the requirements traceability engine TORUS [51].

8 Conclusions

Establishing safe and reliable control systems in industrial settings is the focus of this article (ICS). Typical examples of these ICS can be found in the process control sectors, and they include SCADA systems, DCSs, and PLCs (among other control system types). This document gives an introduction to ICS and common system architectures, details common security threats and vulnerabilities, and suggests safeguards to implement to reduce those risks.

At first, ICS were separate networks that used their own control protocols and hardware and software that were not shared with other networks, bearing little resemblance to the more common IT networks. Many ICS elements were not linked to any kind of information technology network or system and were instead kept in specially guarded rooms. Internet Protocol (IP) components that are easy to find and inexpensive are gradually replacing proprietary products, which raises the stakes for cyberattacks. The increasing use of computers, operating systems (OS), and network protocols from the IT industry in the design and implementation of ICS has led to a convergence between the two types of systems.

Because of the critical role that cybersecurity plays in ensuring the safe and reliable functioning of today's industrial processes, ICS cybersecurity programmes must constantly be integrated into larger ICS safety and security plans at both construction plants and corporate cybersecurity programmes. Control systems are vulnerable to intrusion from a wide variety of causes, including as hostile nations, terrorist groups, individual employees, malevolent intruders, complications, accidents, natural disasters, and even intentional or inadvertent activities by insiders. Availability and integrity are the top priorities in ICS security, followed by confidentiality.

To organise and consolidate CSRS and IEC 62443-4-2 standard requirements, this paper suggests a decentralised LPG system requirement repository with several partitions. In order to help determine which standard cryptographic primitives are needed to implement a security needs, a formal specification of the IEC 62443-4-2 expanded requirement structure is provided. When the repository is used in conjunction with design patterns to record communication security restrictions via secure links and a requirements management engine like TORUS, full-stack security requirements traceability can be attained. The document also shows how the repository can be used to facilitate a process for adapting to new or altered needs. Using graph-query languages to query the repository is what makes the difference, further, to examine what this means for the security testing process and how the repository can be used.

References

1. Norwich University (2019) IT vs. OT: comparing two vital information security concepts. Norwich University. Online. Available at: https://online.norwich.edu/academic-programs/resources/it-vs-ot. Accessed: 2 Sept 2022
2. Kuppusamy E, Mariappan K (2021) Integration of operation technology (OT) and information technology (IT) through intelligent automation in manufacturing industries. In: Advances in manufacturing technology XXXIV: proceedings of the 18th international conference on manufacturing research, incorporating the 35th national conference on manufacturing research, 7–10 Sept 2021. University of Derby, Derby, UK. IOS Press
3. Alber B, Prince A (2021) The structure of OT typologies. Chapter 1: introduction to property theory
4. Green B, Derbyshire R, Knowles W, Boorman J, Ciholas P, Prince D, Hutchison D (2020) {ICS} testbed tetris: practical building blocks towards a cyber security resource. In: 13th USENIX workshop on cyber security experimentation and test (CSET 20)
5. US Homeland Security (2022) Cybersecurity, cybersecurity | Homeland security. Available at: https://www.dhs.gov/topics/cybersecurity. Accessed: 8 Sept 2022
6. Ani UPD, Watson JM, Green B, Craggs B, Nurse JR (2021) Design considerations for building credible security testbeds: perspectives from industrial control system use cases. J Cyber Secur Technol 5(2):71–119
7. Anwar RW, Abdullah T, Pastore F (2021) Firewall best practices for securing smart healthcare environment: a review. Appl Sci 11(19):9183
8. IECEE Publication (2022) Rules of procedure—CB scheme of the IECEE for mutual recognition of test certificates for electrotechnical equipment and components (CB scheme) and its related services: statement of test results—Energy Efficiency Testing Service (E3) Global Motor Energy Efficiency (GMEE) Program Industrial Cyber Security Program. IECEE documents | Rules, operational documents and guides. Available at: IECEE 02—rules of procedure. Accessed: 13 Sept 2022
9. Knapp ED, Langill J (2014) Industrial network security: securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems. Syngress
10. Stouffer K et al (2015) Guide to industrial control systems (ICS) security. CSRC. Available at: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final. Accessed: 13 Nov 2022
11. Hayden E (2019) 4 steps to critical infrastructure protection readiness: TechTarget, security. TechTarget. Available at: http://www.techtarget.com/searchsecurity/tip/252465638/4-steps-to-critical-infrastructure-protection-readiness. Accessed: 26 Sept 2022
12. Boyer SA (2010) SCADA: supervisory control and data acquisition, 4th edn. ISA—International Society of Automation, Research Triangle Park
13. Franceschett AL, de Souza PR, de Barros FLP, de Carvalho VR (2019) A holistic approach—how to achieve the state-of-art in cybersecurity for a secondary distribution automation energy system applying the IEC 62443 standard. In: 2019 IEEE PES innovative smart grid technologies conference-Latin America (ISGT Latin America). IEEE
14. Ehrlich M et al (2019) Secure and flexible deployment of industrial applications inside cloud-based environments: semantic scholar. In: 2019 24th IEEE international conference on emerging technologies and factory automation (ETFA). Available at: https://www.semanticscholar.org/paper/Secure-and-Flexible-Deployment-of-Industrial-inside-Ehrlich-Trsek/e73f3d815cbf1c3f1ae437908cc39dbb37befb00. Accessed: 24 Dec 2022
15. Conklin WA (2016) IT vs. OT security: a time to consider a change in CIA to include resilienc. In: 2016 49th Hawaii international conference on system sciences (HICSS). IEEE
16. Joint Task Force Transformation Initiative (2011) Managing information security risk: organization, mission, and information system view. CSRC. Available at: https://csrc.nist.gov/publications/detail/sp/800-39/final. Accessed: 22 Sept 2022
17. Team E (2021) Understanding IEC 62443. IEC. Available at: https://www.iec.ch/blog/understanding-iec-62443. Accessed: 12 Sept 2022

18. ITL NIST (2018) About the RMF–NIST risk management framework: CSRC. CSRC. Available at: https://csrc.nist.gov/projects/risk-management/about-rmf. Accessed: 12 Nov 2022
19. Boehm A (2018) Take security to the next level with the top 5 CIS critical security controls, Ivanti. Ivanti. Available at: https://www.ivanti.com/blog/take-security-to-the-next-level-with-cis-critical-security-controls. Accessed: 21 Oct 2022
20. Cooper D (2021) NIST test personal identity verification (PIV) cards version 2
21. Abdelghani T (2019) Implementation of defense in depth strategy to secure industrial control system in critical infrastructures. Am J Artif Intell 3(2):17–22
22. Dutta N, Tanchak K, Delvadia K (2020) Modern methods for analyzing malware targeting control systems. In: Recent developments on industrial control systems resilience. Springer, Cham, pp 135–150
23. Culot G et al (2019) Addressing industry 4.0 cybersecurity challenges: semantic scholar. IEEE Eng Manag Rev. Available at: https://www.semanticscholar.org/paper/Addressing-Industry-4.0-Cybersecurity-Challenges-Culot-Fattori/ddefa2b96bdf6e9dc66ffc373ef5fd216b662574. Accessed 30 Sept 2022
24. Ehrlich M et al (2019) Figure 1 from automated processing of security requirements and controls for a common Industrie 4.0 use case: semantic scholar. In: 2019 international conference on networked systems (NetSys). Available at: https://www.semanticscholar.org/paper/Automated-Processing-of-Security-Requirements-and-a-Ehrlich-Gergeleit/51d9b30acce66178804333c960d20ee638887988/figure/0. Accessed 5 Oct 2022
25. Hahm O, Baccelli E, Petersen H, Tsiftes N (2015) Operating systems for low-end devices in the internet of things: a survey. IEEE Internet Things J 3(5):720–734
26. Raymundo Belleza R, de Freitas Pignaton E (2018) Performance study of real-time operating systems for internet of things devices. IET Softw 12(3):176–182
27. Zakaria HM (2022) Security of IoT: sine logistic map, S-box, and Tan-Bessel function
28. Steinert LF (2022) Safety critical, high-performance systems based on COTS multicore processors for industrial and aerospace applications. Doctoral dissertation, Technische Universität München
29. IEC (2010) What is IEC 61508? 61508 Association. Available at: https://www.61508.org/knowledge/what-is-iec-61508.php. Accessed: 26 Dec 2022
30. DRAGOS (2022) 10 ways asset visibility builds the foundation for OT cybersecurity. Available at: https://cdn.cyberscoop.com/asset-visibility-builds-OT-cybersecurity-foundation.pdf. Accessed 21 Oct 2022
31. Lopes IM et al (2019) How ISO 27001 can help achieve GDPR compliance. In: 2019 14th Iberian conference on information systems and technologies (CISTI). IEEE
32. Singgrit P, Pamuji GC (2020) The use of ISO 27001 framework for government's online E-monitoring system implementation. Int J Educ Inf Technol Others 3(3):556–563
33. Murray G, Johnstone MN, Valli C (2017) The convergence of IT and OT in critical infrastructure
34. Hohenegger A (2019) Die common criteria und IEC-62443. Deutscher IT-Sicherheitskongress
35. Fachot M (2020) IEC 62443 standards—a cornerstone of industrial cyber security. Etech. Available at: https://etech.iec.ch/issue/2020-04/iec-62443-standards-a-cornerstone-of-industrial-cyber-security#:~:text=The%20IEC%2062443%20series%20of%20Standards%20is%20organized,4%20Components%20%28IEC%2062443-4.%2A%20%E2%80%93%20both%20parts%20published%29. Accessed: 27 Oct 2022
36. ISA (2020) Security lifecycles in the ISA/IEC 62443 series. ISA.org. Available at: https://21577316.fs1.hubspotusercontent-na1.net/hubfs/21577316/2022%20ISA%20Website%20Redesigns/ISA%20Secure/Files%20Repository%20For%20Learning%20Center/Articles%20Page/ISAGCA-Security-Lifecycles-whitepaper.pdf. Accessed: 27 Oct 2022
37. Gupta S (2020) Assuring compliance with government certification and accreditation regulations. In: Cloud computing security
38. Brandao Filho SB, Cesar CDAC (2022) A secure method for industrial IoT development. SN Comput Sci 3(2):173
39. Stouffer K, Pease M, Tang C, Zimmerman T, Pillitteri V, Lightman S (2022) Guide to operational technology (OT) security (No. NIST Special Publication (SP) 800-82 Rev. 3 (Draft)). National Institute of Standards and Technology

40. Syafrizal M, Selamat SR, Zakaria NA (2020) Analysis of cybersecurity standard and framework components. Int J Commun Netw Inf Secur 12(3):417–432
41. Hohenegger A, Krummeck G, Baños J, Ortega A, Hager M, Sterba J, Kertis T, Novobilsky P, Prochazka J, Caracuel B, Sanz AL (2021) Security certification experience for industrial cyberphysical systems using common criteria and IEC 62443 certifications in certMILS. In: 2021 4th IEEE international conference on industrial cyber-physical systems (ICPS). IEEE
42. Téglásy BZ, Katsikas S, Lundteigen MA (2022) Standardized cyber security risk assessment for unmanned offshore facilities. In: Proceedings of the 3rd international workshop on engineering and cybersecurity of critical systems
43. Grove C (2021) Surprising findings in the SANS 2021 OT/ICS cybersecurity survey. Nozomi Networks. Available at: https://www.nozominetworks.com/blog/surprising-findings-in-the-sans-2021-ot-ics-cybersecurity-survey/. Accessed: 2 Nov 2022
44. Jones N (2019) International policy: pitfalls and possibilities. In: Cyber security: threats and responses for government and business
45. Stouffer K et al (2022) Guide to operational technology (OT) security. CSRC. Available at: https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/draft. Accessed: 4 Nov 2022
46. Irny S, Rose A (2005) Designing a strategic information systems planning. Issues Inf Syst VI(1)
47. BouSaba C (2019) Implementing a DeMilitarized zone using holistic open source solution. In: 2019 ASEE annual conference and exposition
48. Tanveer A et al (2022) Tracing security requirements in industrial control systems using graph databases—software and systems modeling. Springer, Berlin. Available at: https://doi.org/10.1007/s10270-022-01019-8?code=4e726f40-5d33-456d-abf4-ffac84231bc8&error=cookies_not_supported. Accessed: 14 Dec 2022
49. Lal M (2015) Neo4j graph data modeling. Packt Publishing Ltd., UK
50. Tanveer A, Sinha R, Kuo MM (2020) Secure links: secure-by-design communications in IEC 61499 industrial control applications. IEEE Trans Ind Inf 17(6):3992–4002
51. Sinha R, Dowdeswell B, Zhabelova G, Vyatkin V (2018) Torus: scalable requirements traceability for large-scale cyber-physical systems. ACM Trans Cyber Phys Syst 3(2):1–25