Field Device to Central Platform Applications

4

This section covers a very large number of utility applications ranging from power system Supervisory Control and Data Acquisition (SCADA) to all kinds of monitoring and surveillance applications collecting data from electrical substations or other field industrial process installations for processing at some central platform and providing "situational awareness" to grid operators, grid automation applications, asset managers or security surveillance staff. The central platform can react to the outcome through transmitting command signals to modify the situation (e.g., initiating circuit breaker operations, switch-over actions, etc.), through blocking actions (e.g., cyber security monitoring), or through initiating field interventions, depending on the nature of the application. Some common denominators of these data collecting, monitoring, and supervision applications in terms of communications are as follows:

- Preestablished peers—similar to substation-to-substation applications, the communication peers are predefined and invariable—from each substation to the corresponding platform.
- Communication can be initiated by the central platform (cyclic data collection or exceptional data request) or by "satellite" substations (event-driven exchanges).
- Continuous data flow—according to an application-dependent periodicity, data is collected from each substation on a continuous and permanent basis. The data traffic in the opposite direction is much smaller (i.e., highly unbalanced). This can be for example, sending commands or initiating data requests from a platform to a field installed device.
- Constant throughput—The required network throughput for these applications is almost constant depending on the volume of database to be cyclically refreshed.
- Time sensitivity—These applications are considered as real-time, but with no critical time constraints in the data collection (uplink). When data collection is performed through a request-response polling protocol, however, the transfer time may govern the data exchange efficiency. The down-link direction (e.g., command) however, is time sensitive and may need higher time control.

© Springer International Publishing Switzerland 2017

C. Samitier (ed.), *Utility Communication Networks and Services*,
CIGRE Green Books, DOI 10.1007/978-3-319-40283-3_4

Typical examples of substation-to-platform communications are given below:

- Power System SCADA
- Synchrophasor-Based Wide Area Monitoring Systems (WAMS)
- Video-surveillance
- Power asset monitoring
- Telecom network fault and performance monitoring
- Grid-level metering
- Environmental monitoring
- Asset cyber security monitoring
- Site access control.

4.1 Power System SCADA

The power grid's SCADA communications consist in the periodic exchange of short data messages between a central platform in the Control Center and Remote Terminal Units (RTU) in electrical substations, renewable energy storage and generation plants, or any other distributed component of the power system requiring supervision and control. The messages comprise status indications, measurements, commands, set-points, and synchronizing signals that must be transmitted in real-time and requiring data integrity, accuracy, and short transfer time.

Power transmission and distribution networks SCADA generally differ in their requirements, cost objectives, and hence suitable communication solutions. The number of outstations and their corresponding size, cost, volume of traffic, and geographical dispersion are very different in the national transmission grid and in regional distribution networks. The time constraints and the required level of availability, fault tolerance, and data integrity are also different. As a consequence, transmission grid SCADA communication is often implemented through a broadband private network (e.g., optical fiber), while in distribution networks (in particular for MV grids) low capacity UHF Multiple Address Radio systems (MARS), license-free or procured wireless services (GPRS, LTE, etc.) prevail.

Still today, the widest employed communication mode for the substation RTU remains the asynchronous serial link through an RS232 interface, polled by the central control platform. The communication protocol associated to this mode has been standardized as IEC 60870-5-101 (IEC101), although many other protocols are still in use in legacy systems. The major drawback to serial communication for SCADA is indeed its lack of flexibility (e.g., for back up control center connection) and cumbersome installation in particular at the control center. Packet switching, introduced in SCADA systems since the late 1980s for more efficient usage of leased aggregated bandwidth (X25, Frame Relay, ATM, etc.) have only gained worldwide popularity with the advent of IP communications. The TCP/IP protocol IEC 60870-5-104 (referred to as IEC104) is often the migration target for SCADA systems. The use of TCP/IP enhances considerably the flexibility of the SCADA

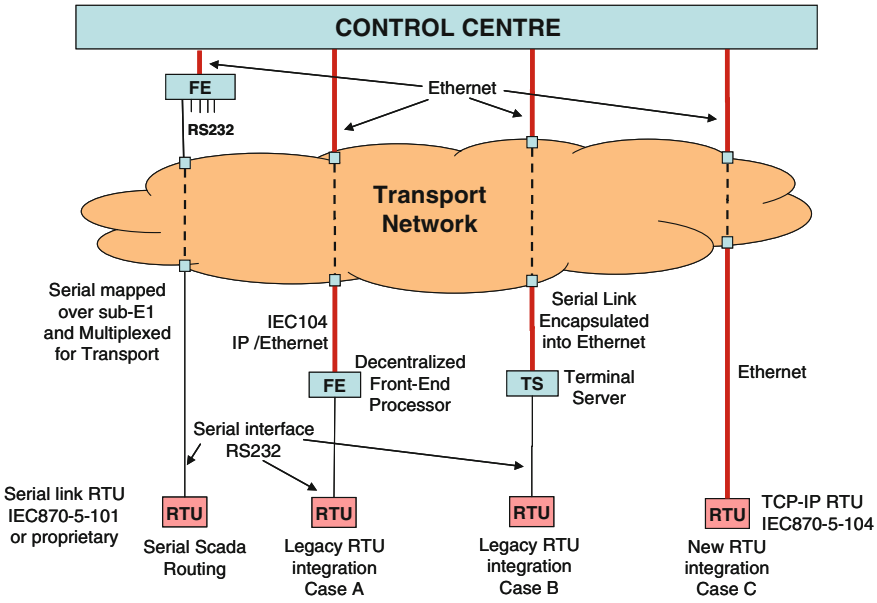

Fig. 4.1 SCADA RTU to control platform connection alternatives

communication system, facilitating the relocation of an RTU or the switch-over of RTU communications to a back up facility.

The RTU communicates through a Fast Ethernet LAN access interface, although the bandwidth allocated to each RTU communication remains often around 20 kbps. Legacy RTU may be connected through a Terminal Server or protocol gateway often integrated into the substation access device switch.

The migration process to TCP/IP in large SCADA networks may be extended over many years, with different timelines for the replacement of the RTUs, network interfaces and SCADA servers. During this long transition period, legacy and new RTUs have to coexist across the grid and the communications may be Ethernet/IP at the SCADA server but serial at the RTU end (Fig. 4.1).

4.2 Synchrophasor-Based Wide Area Monitoring System

WAMS refers to a group of power system applications which use a synchronized snap-shot of power system parameters to enable a better awareness of stability issues and power flows across a grid incorporating dispersed generation and multiple Utilities. These systems operate through phasor acquisition of parameters such as bus voltages, line currents, etc. in electrical substations The Phasor Measurement Unit (PMU) and the Phasor Data Concentrators (PDC) constitute the substation acquisition device and the concentrating gateway device respectively, as previously

described under system protection schemes. However, unlike system protection schemes where decision algorithms generally in a substation provide action at other substations (therefore a substation-to-substation application), here the phasor data is generally employed in a control center for operator situation-awareness, for modeling and analysis or for enhancing the state estimator in an EMS/SCADA. Different levels of wide area applications have very different requirements in terms of information exchange and consequently telecommunication service.

- **Post-Incident Analysis and Static Modeling** applications are offline systems where collected data is used to analyze the cause of an event or to adjust the behavior model for a system. Data can be collected continuously, daily, or only on request. The communication service can be a TCP/IP file transfer service with no real-time constraint.
- **Visualization and Situational Awareness** applications collect data from sites and display them for human operator observation. These applications which constitute the great majority of present day systems have time requirements which are those of a human operator and must additionally present a level of sample loss unperceivable by the human operator. In terms of communication service a non-acknowledge UDP/IP is an adequate solution in this case whether through a dedicated network or a public provider.
- **Monitoring and Decision Support Systems** use collected data to produce analytical information helping operators respond to grid events and to position the grid for improved security and resilience. Stability diagrams and corresponding voltage collapse margins, as well as different monitoring applications (voltage and frequency stability, power oscillations, line temperature, etc.) are among these applications. Monitoring and decision support applications have time constraints which are similar to power system SCADA. This is achievable through UDP over a private IP network or a service provider VPN through a carefully specified SLA.
- **Closed-Loop Applications** are those which incorporate collecting of data from the grid, processing, automatic recognition of a pattern, and remedial action upon the grid. The systems are used for emergency situation control and special protection applications as described earlier in Sect. 3.2. Closed-loop synchrophasor applications are not yet widely implemented and their critical real-time nature necessitates particular attention on time control. Furthermore the decision to act automatically upon the network in real-time means that the data set (from different locations and sample stack from each point) must be complete, that is to say almost lossless.

PMU operation is specified by IEEE C37.118 which defines phasor construction using the GPS-satellite timing signal, as well as the phasor's data format. The exact data volume associated with the transmission of a data packet from a PMU varies depending on the incorporated parameters and the way each of them is coded (i.e., floating point or not, etc.) but can be assumed to be around 80–100 octets. This data volume is to be transferred across the network at a rate which is governed by the

	Wide Area Monitoring Applications	Latency	Resolution (sample/sec)	Comments
Situational Awareness	Situational Awareness Dashboard	1-5 sec	1	Assess system state (Normal, Alert, Alarm)
	Real-time Compliance Monitoring	1-5 sec	1	Angle of Separation, Display Voltage, Phase, Power swing, Line loading MW / MVAR flows
	Frequency Instability Detection /Islanding	1-5 sec	25-30	
Monitoring & Decision Support	Real-time Monitoring and Trending	1-5 sec	1	Decision support and security assessment Help operator to respond to grid events Provide time series information Stability diagrams & Collapse margins Reposition the grid for improved security Monitoring of voltage & frequency stability Display of line temperatures
	Real-time Alerts and Alarms	1-5 sec	25-30	
	State Estimation	1-2 min	25-30	
	Small-signal Stability Monitoring	Few sec	10-60	
	Voltage Stability Monitoring/Assessment	Few sec	25-30	
	Line Thermal Monitoring (Overload)	Few sec	25-30	
Analysis & Static Modeling	Pattern Recognition/ Correlation Analysis	N/A	1	Post-incident Analysis Identify system security metrics System-level and grid asset models
	Disturbance Analysis Compliance	N/A	25-30	
	Frequency Response Analysis	N/A	10	
	Model Validation	N/A	25-30	
Protection & Control	Adaptive Relaying	100ms	25-30	Emergency situation control and protection Closed loop SPS applications
	Out-of-step Protection	100ms	25-30	
	Small-signal stability Prot. & Control	100ms	25-30	
	Short-term stability control (e.g. transient stability)	100ms	25-30	
	Long-term stability control (e.g. Wide Area frequency/ voltage stability)	1-5 sec	25-30	

Fig. 4.2 Wide area applications communication service requirements [extracted from NASPI]

sampling frequency of the PMU. The sampling frequency is expressed as a number of (or a fraction of) AC cycles. It varies generally between 25 and 30 samples per second (one sample every two cycles) to 100–120 samples per second (2 samples every cycle). The required communication throughput is then somewhere in the range of 16–100 kbps although PDC links may require 100 kbps–1 Mbps or more.

Figure 4.2 provides some communication requirements for typical synchrophasor applications including some closed loop ones already discussed under System Protection Schemes.

4.3 Other IP-Based Monitoring Applications in the Substation

A long list of other field device to platform applications allow to monitor remotely the health of installed assets, the access security and environmental hazards in field process sites, cyber security of intelligent substation device, or the state of telecommunication devices and services in the electrical substation. These applications require access to an IP-based network connecting substations to central platforms. The exchanged data volume and hence the required communication channel throughput varies according to the quantity of information and the frequency of cyclic collection of measurements, threshold crossing events and device alarms. End-to-end latency is generally not a design or dimensioning issue for these monitoring applications although operator usage comfort still requires the systems to transmit transactional data (e.g., request/reply or command/react) in reasonable time. A number of these monitoring applications are briefly described.

Video Surveillance
Video monitoring of substations and other operational assets is a growing application in the grid due to concerns and regulatory obligations over the integrity and security of national critical infrastructures. Remote video monitoring of installations can be a source of substantial data traffic across the power network if used extensively and can drive telecom network upgrades in particular for distribution grids where communication capacity has often been very low.

Asset Condition Monitoring
Primary assets of the power system (circuit breaker, power transformer, etc.) generate condition monitoring data through their sensors and associated electronics. This data can be collected for maintenance requirements, and for determining duty cycle, device capability and loading ability. Asset condition monitoring enables the safe and efficient use of network components to their real end of life, at full efficiency, without disruption of service due to asset failure, environmental risks, or unnecessary preventive replacement.

Secondary assets of the electrical substation related to the measurement, protection, and control as well as the related power supplies can also be monitored over remote platforms. Moreover, these "Intelligent Electronic Devices" (IED) are configured, patched, upgraded, and in general, managed remotely implying not only network connectivity and bandwidth but also harsh cyber security constraints. These latter aspects are treated under Chap. 6 on "Office to field" applications.

Telecom Fault and Performance Monitoring
Telecommunication devices constitute a particular group of assets in the power system, often not directly part of power system but impacting its operational capability. Fault monitoring of telecom equipment, links and services, as well as the performance monitoring of the delivered communication services represent a nonnegligible communication load (e.g., SNMP exchanges over IP). This particular type of asset monitoring is further developed in Part 5.

Grid-Level Energy Metering and Monitoring
Energy metering information at the power delivery point of the transmission grid is required by the different actors of the open deregulated electricity market. This enables the settlement and reconciliation processes as well as invoicing of grid access services towards energy distributors. In addition to metering data, electrical power parameters are often monitored at the power delivery point to ensure the contractual quality of the delivered power.

Environmental Monitoring (Sites and Assets)
Power system process sites are increasingly equipped with environmental sensors for detecting abnormal temperature, fire, smoke, floods, gas, and chemicals and provide alarm information to remote monitoring platforms. The purpose of such monitoring is not only to protect substation assets and premises but also to protect the environment from industrial risks and hazards related to the substation assets (e.g., chemical pollution). Growing environmental concern and regulatory obligations in this field lead to steadily increasing deployments of such remote monitoring and early warning systems to avoid environmental impacts.

Asset Cyber Security Monitoring
The growing deployment of electronic intelligence in the electrical substation and the subsequent exchange of information between networked devices across the power grid have made it essential to implement numerous security barriers and intrusion detection/prevention systems. In particular, intelligent devices are made accessible from remote locations for data reporting (e.g., asset monitoring) and for remote diagnostics, parameter setting, and configuration change.

Remote access to substation device is increasingly authenticated and authorized at a remote server (e.g., RADIUS server) hence requiring particularly reliable and secure communications.

In addition to security protection at device level, remote access to the substation and to its critical information zone is further protected through white-list filtering determining the network users entitled to cross the barrier. Appropriate firewalls are integrated into the telecom access and aggregation devices and into substation switches. These security filtering components, although local, need to be remotely updated, patched and configured through reliable and secure communications. Moreover, as the number of security-related devices and systems increases, it becomes necessary to reinforce them through coordinated administration, supervision, and efficient logs processing. Security Operational Centers (SOC) are set up to collect security-related events across the network, to produce security reports and to enable the operator to take appropriate preventive measures in reaction to threat situations (e.g., blocking access ports). Security logs and reports may be used for investigations and for understanding of incidents or trends especially through dashboards.

Site Access Control

Electronic site access control systems are increasingly used to control, register, and monitor the physical access to operational sites. Smart electronic identity cards and biometric authentication are becoming part of the security and safety policy. Electronic access control allows differentiated accessibility in time and across locations for different classes of staff (operational, service contractors, maintenance, etc.).

Protecting sites like power plants or substations from intruders has always been a main concern for Utilities, not only for the site protection itself but also for human and animal safety. Fences and guards were in the past the only solutions, but with increasingly unmanned installations, intrusion detection systems are being introduced.

The classical intrusion detection system is composed of sensors (radio, laser, dry contacts, …) connected to a local collector unit that monitors the sensor states and, in case of a detection, sends online notifications to the SOC of the utility and local security forces. More recent developments use video-surveillance cameras and image analysis software that alerts SOC operators in case of image pattern changes.

Site access and intrusion detection applications require fast and reliable data communications for authentication and access registration.