# AN INVESTIGATION ON DATA GATEWAY FUNCTIONALITIES FOR ENTERPRISE ANCILLARY SERVICES IN DIGITAL SUBSTATIONS

Yiming WU
Vattenfall Services Nordic – Sweden
yiming.wu@vattenfall.com

Florin STELEA
SWECO Energy – Sweden
florin.stelea@sweco.se

Anders JOHNSSON
Vattenfall Eldistribution - Sweden
anders.johnsson@vattenfall.com

## *ABSTRACT*

*Network control center Supervisory Control And Data Acquisition (SCADA) associated with Distribution Management System (DMS) use often Remote Terminal Units (RTU) as protocol gateways deployed in substations to send and receive data for operation related applications. The heterogeneous requirements from power system operation related applications together with less critical enterprise DMS services impose different functionalities on the substation data gateways. This paper presents an investigation about the imposed duties associated with these services, revealing the necessary data gateway functionalities for a Nordic Distribution System Operator (DSO). The outcome of this study is considered for substation data gateway specification to be deployed in a digital substation pilot project for the DSO.*

## INTRODUCTION

Substations are crucial parts in electrical power systems. Their protection, automation and control systems (PACS) and monitoring functionalities ensure safe and reliable operation of distribution systems. Aside with development of information and communication technologies, full digitalization of the substation is a trend. The concept of fully digital substation is proposed to digitalize not only signals at bay level but also on process level [1]. The introduction of the IEC61850 standard helps solving the interoperability issue among devices from different vendors by use of a standard data structure for information modelling and standard communication protocols for data exchange [2][3][4]. The data contained in the IEC61850 compliant devices can also be shared flexibly not only for operation related services (e.g. protection functions, remote monitoring and control functions) but also for enterprise data analytics and monitoring services (e.g. power quality monitoring, equipment maintenance, fault localization, isolation and restoration, planning, etc.), hereby named as enterprise ancillary services. However, providing data from substations towards enterprise central services is facing the following challenges:

- *Various communication protocols*
- *Time synchronization among different substations*
- *Cyber-security*
- *Various requirements on Quality of Service (QoS) and other non-functional aspects*

In order to solve these challenges, a substation data gateway is suggested to be deployed. Based on the identified data flows for different enterprise central services and their demands on communication protocols, time synchronization, cyber-security, QoS and other non-functional aspects, the functionalities of the gateway can be outlined, as presented in this paper.

## RELATED WORK

In this section, the functionalities of the typical existing substation gateway, also known as Remote Terminal Unit (RTU), are presented. Then different types of substation data gateways available on the market are presented. Thereafter, the work related to time synchronization and cyber security functionalities on gateway are reviewed.

### Functionalities of the RTU

The RTU is used mainly for the operation related service, remote monitoring and control. Conventionally, the functionalities of the RTU include Analogue to Digital (A/D) conversion, binary I/O signal conversion, command authorization control and output, protocol conversion, logical control, disturbance record file collection and so on. The A/D conversion is used to digitize the analogue measurement signals (e.g. current, voltage, active and reactive power, and step of tap changer). The binary I/O is used to convert the discrete signals following status of primary apparatuses, automation functions and alarms into digital images to be used by SCADA system. Remote commands issued from control center are forwarded by RTU with authorization control to the apparatuses using binary contacts or local communication with control terminals. The information exchange within the substation local area network follows one standard (e.g. Modbus, SPACOM or IEC61850) and the communication to the control center normally follows another standard (e.g. IEC60870-5-101/104 or DNP3). Therefore, a protocol conversion is performed in the RTU. In addition, some local control functions and collection of disturbance record functions could also be implemented in the RTU.

### Different types of substation data gateway

After a market scanning for substation data gateways, different products from various vendors can be roughly classified into following types:

- *Protocol convert gateway*: Mainly used to translate data flows from one communication protocol to another. RTU, as a typical example, converts the status and measurement information from IEC61850 MMS format to IEC60870-5-104 types to the control center.
- *Security gateway:* Used to provide a secure channel to

manage substation devices such as IEDs, RTUs, energy meters, etc. from a central point. It normally provides access privilege to different remote users, security monitoring and control on data flows.

- *Analytics gateway:* Used to provide monitoring and analytics on the data flows with additional status information. This information can be used for trouble-shooting of communication systems and other functions that relies on the communication systems.
- *Hybrid gateway:* A gateway that integrates two or more of the above functionalities in the same device.

### Time synchronization

Time synchronization is a typical substation ancillary service used in the substation to provide a common clock signal for substation's Intelligent Electronic Devices (IED). For example, synchronized time stamps in disturbance recorders can simplify analytics after fault. In digital substations, protection functions require high accuracy time synchronization (e.g. ~100ns) between IEDs and Merging Units (MU). The conventional Simple Network Time Protocol (SNTP) based time synchronization solution cannot fulfil the need on accuracy. Instead the IEEE 1588 Precision Time Protocol (PTP) is suggested to be used as an Ethernet based solution. In [5], a solution that uses a time gateway is proposed to use SNTP to synchronize the legacy devices which only support SNTP, while the gateway itself can be synchronized using PTP. However, there is still a challenge even if the PTP is selected, as it does exist several different communication profiles. The telecom profile follows ITU-T PTP Telecom Profile (designated as PTP telecom profile) [6] and the power profile follows IEEE C37.238 (designated as PTP power profile) [7]. In this paper, the time synchronization is within the scope of the functions that a substation data gateway shall provide.

### Cyber-security

Current cyber-attacks on communication systems of power systems reveal the vulnerabilities and rises the need for cyber security within power systems [8]. International organizations such as CIGRÉ and IEC have put great efforts to improve the cyber security of power systems. The IEC62351 series of standards is released as a guideline that helps power utility companies to implement cyber-security countermeasures against potential cyber-attacks [9]. However, the recommended cyber-security countermeasures might violate the end-to-end latency requirements of the protection applications. Considering the restricted computational resources in IEDs, the security framework that protects all substation communications is considered [8]. A generic solution is to provide good enough cyber-security countermeasures on the entry points of the substation communication network. In this paper, the gateways are recognized as the entry points of the substation communication network. Therefore, the cyber-security is within the scope of functionalities of the substation data gateway.

## ENTERPRISE ANCILLARY SERVICES

The enterprise ancillary services of a Nordic Distribution System Operator (DSO) have been listed and described as the followings:

- Communication network operation: Focuses on supervision and control of power system auxiliary communication system. The communication networks inside the digital substations shall also be monitored.
- Asset management: Includes the management of both primary equipment (e.g. circuit breaker and transformer) and PACS equipment (e.g. IEDs, RTUs and MUs of the control system). The maintenance on primary equipment is changing from corrective to preventive manner that requires more information from the substation to improve the failure prediction model [10][11]. Related to PACS equipment, asset management shall cover not only the physical device itself but also the software and firmware running on top of it.
- Substation physical security: Inclusion of information from substation ancillary systems such as intrusion detection, access control, fire detection and protection, and CCTV surveillance monitoring.
- Substation auxiliary power supplies: Inclusion of information from substation's AC and DC auxiliary supplies.
- Power quality and energy metering: Includes power quality monitoring, billing metering, and metering data concentration from secondary substations.

### Data flow identification

In this section, the data flows for different enterprise ancillary services are identified, including the data content and communication protocols. Requirements on availability and latency have been determined by interviewing experts from the Nordic DSO.

The data flows for communication network operation brings the status information and event logs from the communication nodes to the communication Network Operation Center (NOC) using Simple Network Monitoring Protocol (SNMP), syslog, etc. IEC61850 part 90-4 is used to map the information from Management Information Base (MIB) to IEC61850 based data structure. The communication status of the nodes (e.g. IEDs, MUs and switches) can use MMS as status information carrier. Since the existing NOC does not support MMS, communication status from substation communication nodes shall be converted to SNMP. The availability for the data flow should be greater than 99.9% and the latency for the data less than 1s.

The data flow for asset management brings both disturbance records and real-time measurements to the centralized application, condition based primary asset management, where the decision on maintenance action for primary devices is made. The disturbance records can be retrieved from IEDs using MMS file transfer service and the real-time measurements can be retrieved from the IEDs using MMS reporting. As the centralized application for asset management only supports File Transfer Protocol

(FTP), a conversion shall be done from MMS to FTP. The disturbance analyse is also classified in the category of asset management in the Nordic DSO. The latency requirements on disturbance records can be higher than 60s. And the availability requirement for disturbance records transfer is at least 99.9% since it is not only used by the asset management service but also the disturbance analysis service. The real-time measurements for the asset management service require latency of data flow to be less than 10s with availability of at least 99%.

The data flows for substation physical security related services normally have their own proprietary communication protocols. But the central level security management systems normally use the same communication protocols. These data flows require the same level of availability, above 99.9%, and less than 10s for latency, except for the CCTV surveillance streams which require the latency to be less than 1s.

To the energy metering category, billing meters normally are IEC62056 compliant devices [12] using DLMS/COSEM as communication protocol. The data flow should have the availability of at least 99.9% and the latency should be less than 60s. The power quality data is normally collected and stored in standalone meters or IEDs (with power quality monitoring function) as a file in PQDIF format as specified in IEEE 1159.3 [13]. The PQDIF file can be retrieved by MMS (if supported by the power quality meter) or FTP. The availability of the data flow should be at least 99% and the latency less than 60s.

Figure 1 illustrates the overall data flows for different services from end nodes (e.g. IEDs, MUs, meters, switches, etc.) to central level services. The figure includes not only the data flows for substation ancillary services but also the data flows for operation related services, which have more restrict requirements on availability and latency.

## Criticality classification for data flows

In the previous section, data flows of different services have been identified. Their availability and latency requirements are determined. The availability of different services can be divided in the following levels:

- >99.999% extremely high
- >99.99% high
- >99.9% medium
- >99% low

The latency requirements for different services can also be divided in the following levels:

- <4, <10 ms low
- <100 ms relatively low
- <1000, <10000 ms medium
- <60000, >60000 ms high

Based on these classifications, in this paper, the criticality of data flows can be obtained and listed in Table 1.

Data flows belonging to criticality level 1 and 2 are considered as extremely critical as they are used by the protection related services. The high accuracy time

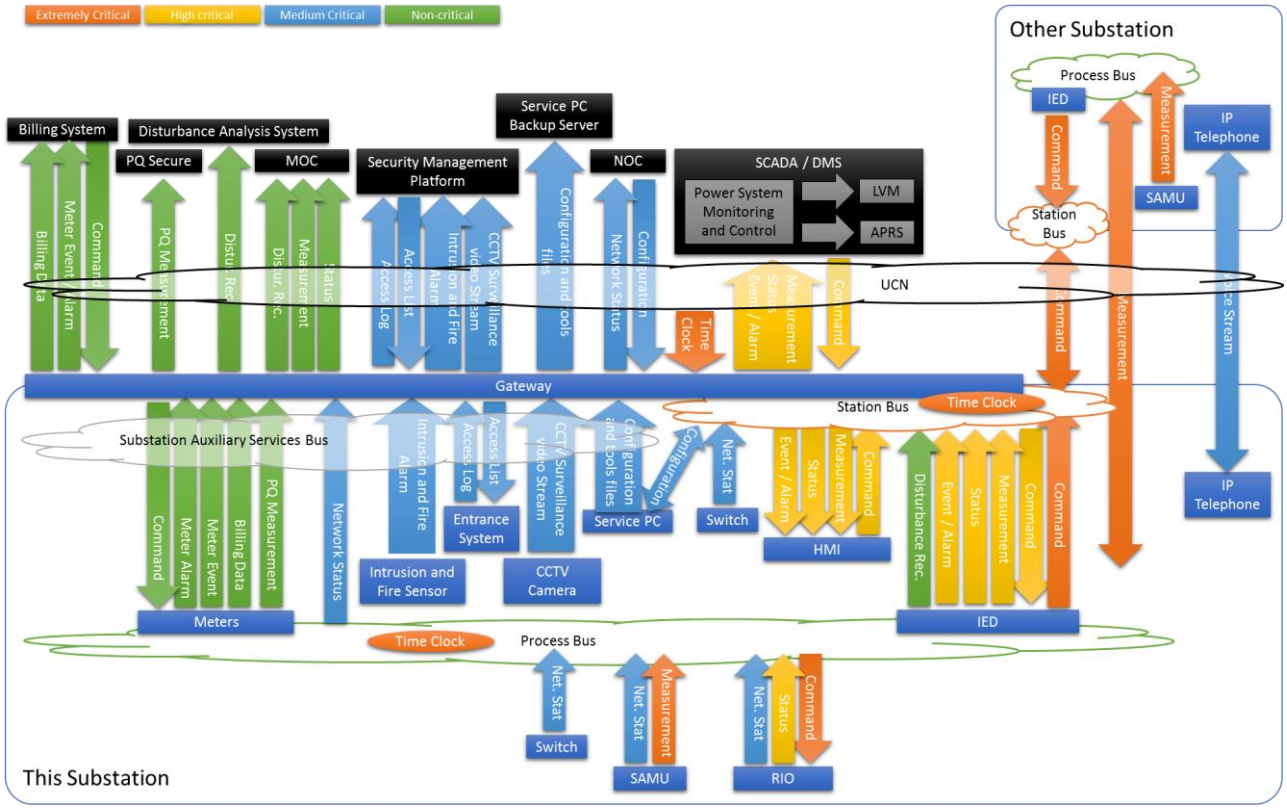


**Figure 1.** Summary of data flows

synchronization service is also considered as extremely critical since operation of protection services rely on them. Data flows belonging to criticality level 3 and 4 are regarded as highly critical as they are used for SCADA applications. Data flows belonging to criticality level 5, 6, and 8 are regarded as medium critical. And data flows belonging to criticality level 7 and 9 are regarded as non-critical. It can be found that data flows for enterprise ancillary services are either medium critical or non-critical.

**Table 1.** Criticality category for different data flows

| Criticality | Availability | Latency | Data flows for Different Services |
|---|---|---|---|
| 1 | Extremely High (>99.999%) | Low (<4, <10) | High Accuracy Time Synchronization, Line Differential Protection, Remote Trip |
| 2 | High (>99.99%) | Low (<4, <10) | Inter-substation relay communication |
| 3 | High (>99.99%) | Medium (<1000, <10000) | SCADA Primary distribution substations, Automatic Power Restoration |
| 4 | Medium (>99.9%) | Low (<4, <10) | Time Synchronization |
| 5 | Medium (>99.9%) | Relatively low (<100) | IP Telephony |
| 6 | Medium (>99.9%) | Medium (<1000, <10000) | Remote Backup Alarm Annunciation, Network Monitoring, Mobile System, System Operation and Backup, Physical Intrusion Detection System, Fire Detection/Protection System, Access Control System, CCTV Surveillance Camera Monitoring |
| 7 | Low (>99%) | Medium (<1000, <10000) | Remote Disconnector, Condition Monitoring, Remote Access |
| 8 | Medium (>99.9%) | High (<60000, >60000) | Low Voltage Monitoring, Disturbance File Collection |
| 9 | Low (>99%) | High (<60000, >60000) | Power Quality Monitoring, Billing Metering, Metering Operation, Event and Alarm |

***Note: Criticality class 1 and 2 are extremely critical; class 3 and 4 are high critical; class 5, 6, and 7 are medium; class 8 and 9 are non-critical.***

## FUNCTIONALITIES OF SUBSTATION DATA GATEWAY

In the previous sections, the functionalities of the substation data gateway for the Nordic DSO can be identified as the followings: *protocol conversion*, *time synchronization*, *cyber security*, *proxy*, *and other local processing capabilities*. The demands from enterprise ancillary services onto these functionalities of the substation data gateway are described in detail in the following subsections. In addition, other functionality which is required by some specific services is described as well.

### Protocol conversion

The requirements on the protocol conversion can be pointed out from identified data flows. If a data flow from the process level devices (e.g. MUs, IEDs, and etc.) follows one standard protocol and the data receiver (e.g. centralized application) requires another communication protocol then the data gateway need to provide protocol conversion for this data flow. See communication network monitoring as an example described above. The required conversion of different protocols is identified and concluded in the following table.

**Table 2.** Protocol conversion for ancillary services

| Data from/to substation | Procotol towards substation | Protocl towards central service |
|---|---|---|
| Communication node status | MMS report | SNMP |
| Disturbance recorder | MMS file transfer | FTP/SFTP |
| PQDIF file | MMS file transfer | FTP/SFTP |
| Status, measurement, and command | MMS report | IEC60870-5-104 |
| Time synchronization data | PTP telecom profile | PTP power profile |

***Note: The status indication, measurement and command are regarded as redundant service for remote monitoring and control service (SCADA) which can also be sent via additional gateway.***

### Time synchronization

For the Nordic DSO, substations are connected to a Utility Communication Network (UCN) infrastructure (representing a Wide Area Network, WAN) where the PTP is supported. However, WAN equipment only supports PTP telecom profile. In the substations, some MUs and IEDs support only the PTP power profile. Therefore, to have an overall time synchronization solution, a PTP profile conversion is needed as illustrated in Figure 2. The gateway acts as transparent clock towards WAN using PTP telecom profile to synchronize its internal clock to the grandmaster in the WAN. It also acts as grandmaster towards the substation using PTP power profile which uses its internal clock as the time reference. The gateway must have high accuracy on its internal clock in order to provide high accuracy time synchronization in case its synchronization to the WAN grandmaster is lost.

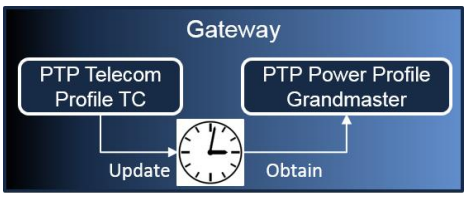


**Figure 2.** Time synchronization function provided by substation data gateway

### Cyber-security

As mentioned in previous section, the cyber-security is also an important functionality that shall be provided by the substation data gateway as it is recognized as an entry point to the substation communication network. The gateway shall provide cyber-security countermeasures such as firewall, authentication and encryption functions. The firewall can provide access control based on the IP

address, port address, and communication protocols specified by different data flows. The authentication mechanisms such as Remote Authentication Dial-In User Service (RADIUS) can be provided by the gateway. Since the gateway also acts as protocol converter or proxy server, the corresponding encryption mechanisms suggested in different parts of the IEC62351 series is considered to be implemented in the gateway. The DSO has its own cyber-security policy on network separation based on the security zone division. The gateway must be equipped with multiple communication ports in order to meet the physical separation requirement.

### Proxy server

Several proxy servers are identified to be implemented in the gateway for different enterprise ancillary services:

- MMS proxy: MMS proxy, as introduced in IEC 61850-90-2 [14], can be used to represent data from different IEDs to avoid direct access to the IEDs from clients outside of the substation.
- SNMP proxy: Used for the substation communication network supervision to represent communication node status to the NOC.
- SFTP server: Used to transfer disturbance records or PQDIF files from the substation to a central application. Additional file handling can be implemented in the gateway at the substation level.

### Other Functionalities

Other service specific functionalities can also be integrated in the substation data gateway. For example, for an asset management application, the real-time measurement shall be calculated as accumulated value for the decision making. For disturbance recorder file transfer, as the naming convention can be different for different vendors, the gateway is then able to help correcting the name of files and file storage structures at the substation level. These additional functionalities deployed in the substation gateway can enhance the scalability of the centralized enterprise ancillary services.

## CONCLUSION AND FUTURE WORK

This paper has presented results of an investigation of enterprise ancillary services that was performed based on the needs of a Nordic DSO. The data flows for these services have been identified with their communication protocols and requirements on end-to-end latency and availability. Based on the characteristics of the identified data flows, the functionalities of the substation data gateway can be determined as protocol conversion, time synchronization, cyber-security, and proxy server. The outcome of this study is considered for substation data gateway specification for a digital substation pilot project for the DSO. The gateway is to be implemented in parallel to the traditional RTU. Different functionalities can be gradually deployed for different ancillary services.

- Stage 1: Support for IEC61850 proxy and FTP proxy server to collect non-time critical data and files from IED's.
- Stage 2: Support for SNMP proxy and IEC61850 based power quality monitoring file collection plus functionality to support substation physical security.
- Stage 3: Capability to support all ancillary services. Full flexibility and scalability.

The deployment of a substation data gateway is the enabler of data sharing from digital substations to enterprise ancillary applications targeting to achieve higher efficiency and lower cost operation of substations.

## REFERENCES

[1] S. Meier, "Enabling Digital Substations", ABB Technical Report, [Online]. Available: https://library.e.abb.com. Accessed November, 2018.

[2] IEC, 2010, IEC61850 - Part 7-4: Basic communication structure - Compatible logical node classes and data object classes.

[3] IEC, 2011, IEC61850 - Part 8-1: Specific communication service mapping (SCSM) - Mappings to ISO MMS and to ISO/IEC 8802-3.

[4] IEC, 2011, EC61850 - Part 9-2: Specific communication service mapping (SCSM) - Sampled values over ISO/IEC 8802-3.

[5] P. Ferrari and et al., 2012, "Evaluation of Time Gateways for Synchronization of Substation Automation Systems", IEEE Trans. on Instrumentation and Measurement, vol. 61, no. 10, 2612-2621.

[6] ITU-T, 2016, G.8275.2/Y.1369.2: Precision time protocol telecom profile for phase/time synchronization with partial timing support from the network.

[7] IEEE, 2017, IEEE C37.238: Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications.

[8] N. Moreira and et al., 2016, "Cyber-security in substation automation systems", Renewable and Sustainable Energy Reviews, Vol. 54, 1552-1562.

[9] IEC, 2016, IEC62351: Power systems management and associated information exchange - Data and communications security.

[10] J.J. Meeuwsen and W.L. Kling, 1997, "Effects of preventive maintenance on circuit breakers and protection systems upon substation reliability", Electric Power Systems Research, Vol. 40, no. 3, 181-188.

[11] Z. Liang and et al., 2018, "A Markovian model for power transformer maintenance", IJEPES, Vol. 99, 175-182.

[12] IEC 62056, 2017, Electricity metering data exchange - The DLMS/COSEM suite.

[13] IEEE 1159.3, 2003, IEEE recommended practice for power quality data interchange format (PQDIF).

[14] IEC, 2016, IEC61850 - Part 90-2: Using IEC 61850 for communication between substations and control centres.