Modern Power System Automation for Transmission Substations

G. M. Asim Akhtar, Muhammad Sheraz, Ali Safwan, M. Akhil Fazil, and Firas El Yassine
Schweitzer Engineering Laboratories, Inc.

Presented at
Saudi Arabia Smart Grid 2018
Jeddah, Saudi Arabia
December 11–13, 2018

Modern Power System Automation for Transmission Substations

G. M. Asim Akhtar, Muhammad Sheraz, Ali Safwan, M. Akhil Fazil, and Firas El Yassine
Schweitzer Engineering Laboratories, Inc.

***Abstract*—Global utilities concentrate not only on implementing new technologies to integrate renewables, but also on enhancing and optimizing power system automation for traditional power grids based on new protocols and smart engineering practices.**

This paper discusses an automation system consisting of intelligent electronic devices (IEDs) programmed to exchange information using various protocols to control, protect, and monitor the entire substation. These operations are performed from a substation-specific control room, remote control centers via SCADA, and standardized human-machine interfaces (HMIs).

The paper describes best engineering practices for primary and ancillary communications protocols, including IEC 61850 Manufacturing Message Specification, IEC 61850 GOOSE, Simple Network Time Protocol (SNTP), IEC 60870-5-101/104, and Simple Network Management Protocol (SNMP). The implementation of an optimized, reliable Ethernet communications network that serves as a backbone in the automation system, enabling all respective devices, protocols, and software to play their roles effectively, is also described. Cybersecurity requirements and real-time implementation, a core requirement of smart grid infrastructure, are also discussed. This paper provides a basis for understanding the design, testing, and commissioning requirements of an optimized automation system to facilitate the concept of a smart grid.

I. Introduction

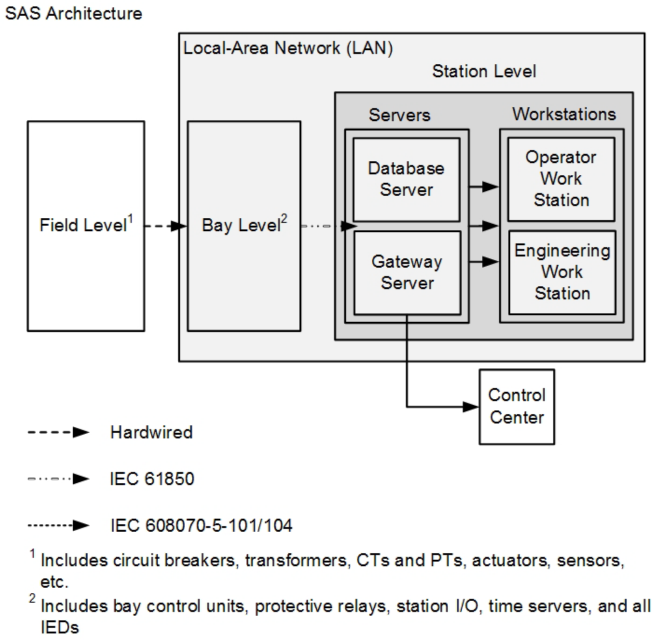
A transmission substation is the core component of an electrical power system designed to transmit power reliably and efficiently. Modern smart grid technology has led utilities and vendors to improve transmission substations by deploying substation automation systems based on new protocols and proven smart engineering practices.

In this paper, the authors present their knowledge of designing, testing, and commissioning an IEC 61850-based substation automation system (SAS). The paper is designed to present major aspects of modern SAS by covering basic information and best practices based on years of experience.

Section II presents a brief overview of an SAS. The SAS components are explained in Section III, followed by highlights of major and minor communications protocols in Section IV. Sections V and VI present a robust communications network and cybersecurity considerations, respectively. Sections VII and VIII explain substation automation philosophy and include HMI visualization, respectively.

II. Overview of a Substation Automation System

Automatic substation monitoring and control via intelligent electronic devices (IEDs) and a communications network constitutes an SAS. Through centrally located servers and workstations, an SAS uses the functional capability of IEDs to implement automation, protection, metering, control, and monitoring. It is designed to facilitate control locally from within the substation and remotely from utility load dispatch centers or load control centers. Fig. 1 shows a simplified block diagram for a transmission SAS.



¹ Includes circuit breakers, transformers, CTs and PTs, actuators, sensors, etc.
² Includes bay control units, protective relays, station I/O, time servers, and all IEDs

Fig. 1. Block Diagram of SAS

III. Substation Automation System Components

A. Servers

The hardened computers with the SCADA applications installed that communicate with IEDs to provide monitoring and control a power system.

1) Database Server

The database (DB) server has the main SCADA application software installed. It communicates with the IEDs in the field to gather data and send control commands. Data consist of real-time analog values, indications, alarms, controls, and set points.

The computer represents these data on the SCADA HMI. Due to the vital importance of the servers, the best configuration is to have them redundant within a master-standby (hot-cold) configuration. Furthermore, the number of redundant sets of database servers can be increased based on the number of voltage levels and IEDs.

2) Gateway Server

The gateway (GW) server is responsible for communicating outside of the substation (e.g., to a master station) to manage operation of all substations in a specific geographical area. The SCADA application database is also configured in the GW server. The main purpose of this machine is to perform as a protocol converter between IEC 61850 and various other protocols used in the substation to the protocols utilized in the master station (primarily IEC 60870-5-101 and IEC 60870-5-104). The GW server has a crucial role; it is vital that another redundant machine be provided as backup. However, both GW servers always communicate with the field. The master station performs the redundancy by choosing which GW server to communicate through. In other words, both GW servers are configured as master-master (hot-hot).

A typical arrangement of DA and GW servers in SAS is shown in Fig. 2.

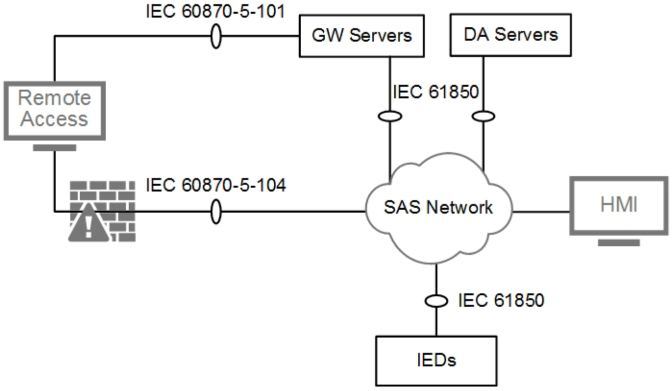


Fig. 2. DA and GW Servers in an SAS Network

B. Network Components

The two major network components of an SAS are industrial-grade managed Ethernet switches and a redundancy box.

1) Managed Ethernet Switches

These are configurable network-switching devices that connect all components of an SAS to a network and transmit/receive data per the defined and required functionality. These are multiport devices capable of configuring with each port level. The two distinctive features of a managed Ethernet switch are virtual local-area network (VLAN) awareness and Rapid Spanning Tree Protocol (RSTP) support.

2) Redundancy Box

This device is found in substations where a communications network is deployed based on IEC 62439-3 Parallel Redundancy Protocol (PRP). The IEDs and devices with only one network interface and that are not compliant to PRP are connected to a PRP-based network via a redundancy box that provides a redundant path of communication.

C. Intelligent Electronic Devices

In power system automation, an IED is a smart device that can perform both basic and advanced functions related to protection, automation, monitoring, and control. In an IEC 61850 environment, every IED can communicate independently with SCADA acting as an intelligent interface for field devices. In transmission substations, IEDs include bay control units, protection relays, transformer tap changer control modules, smart metering devices, and IEC 61850 compliant I/O modules to integrate legacy devices into the SAS.

D. Workstations

Two main workstations are provided for the grid operators to complete routine maintenance and perform operational activities.

1) Operator Workstation

This machine is provided with a graphical user interface (GUI) connected to the DB servers. The operator workstations (OWS) are not connected to field-level IEDs; rather, the IEDs completely rely on the integrity of the DB servers for accurate representation of the data. The OWS is configured to communicate only with the master DB server.

2) Engineering Workstation

The engineering workstation (EWS) communicates with all devices available in a substation. The EWS has a specific role, which is to configure or modify IED settings parameters and Substation Configuration Description (SCD) files of all IEDs present in the substation. It does not perform any SCADA duties. This computer must be highly secured as it can provide access to any IED present in the substation.

E. Satellite Clock for Time Synchronization

Time synchronization plays a crucial role in SCADA applications to precisely analyze data acquired over any distributed control system or network. Time synchronization is achieved by installing a dedicated Simple Network Time Protocol (SNTP) server that can acquire correct, precise time via Global Positioning System (GPS) and Global Navigation Satellite System (GLONASS) satellites. Installing an SNTP server has advantages. It reduces the cost for implementation of the physical layer and utilizes the same local-area network (LAN) on which IEDs communicate. Critical application requiring high-accuracy, Inter-Range Instrumentation Group (IRIG)-based protocol is also used.

F. Security Gateway

The SAS for modern substations is designed with the flexibility to communicate with each remote-control center via both serial-and Ethernet-based protocols. Security gateways that meet cybersecurity requirements are installed according to customer standards to secure the option of Ethernet-based communication.

IV. Communications Protocols

A. IEC 61850-Based Manufacturing Message Specification and Generic Object-Oriented Substation Event Protocol

IEC 61850 is known for fast and reliable system-wide distribution of I/O values. This data transfer is based on a publisher-subscriber and/or client-server mechanism depending on the selected protocol, which could be either Manufacturing Message Specification (MMS) or Generic Object-Oriented Substation Event (GOOSE). IEC 61850 defines the structure for an event while GOOSE and MMS protocols define the specific transport mechanism for information transfer between devices. Fig. 3 provides a model for IEC 61850 and Fig. 4 shows the data mode hierarchy for an IEC 61850-compliant IED.

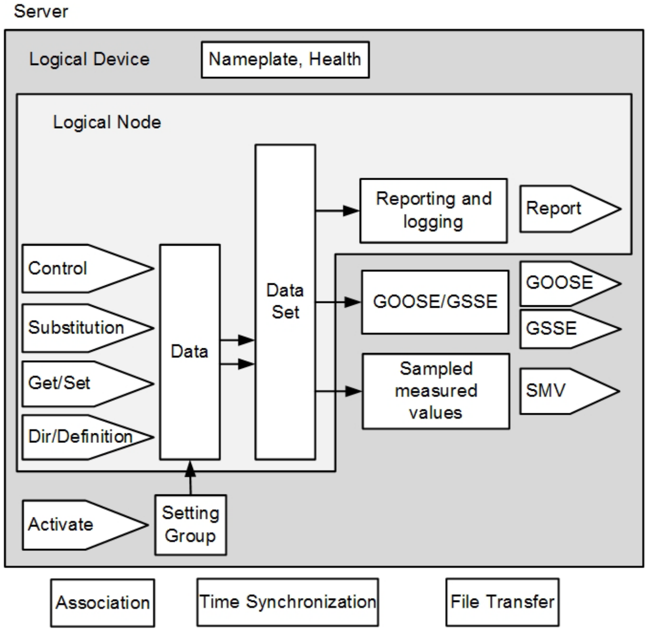


Fig. 3. ASCII Model for IEC 61850

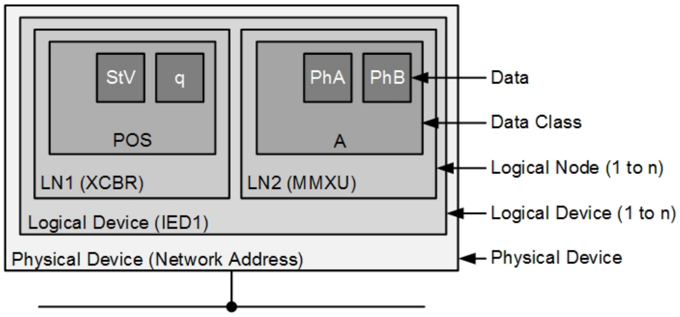


Fig. 4. Sample Data Model Hierarchy for a IEC 61850-Compliant IED

GOOSE protocol is used for time-critical high-speed and high-priority application-based data acquisition. It enables the IED to send unsolicited messages that can be received by single or multiple IEDs in peer-to-peer or one-to-many fashion. Generally, it is used for protection and bay control interlocking where information sharing is critical between IED(s).

MMS is usually preferred for SCADA or non-time-critical data acquisition. It is implemented for communication of IEDs with central servers and gateways. The distinctive feature of this protocol is report-based data transmission activation, which can be based on either event change or time interval. The report can be either buffered or unbuffered. As a best practice, status values and commands are part of buffered reports so that upon failure/switching over of server computers the data are not lost; rather, they are stored in a buffer and are available inside the IED. Analog measurements are made a part of unbuffered reports because losing such information during DB server failure or switching over is not critical.

B. Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is an application layer protocol usually utilized to monitor network devices (i.e., Ethernet switches). It is also used to monitor server and GW computers, satellite clocks, and security GW. It is deployed in three versions: V1, V2C, and V3. V3 is preferred in modern substations as it features improved performance, flexibility, and security.

C. IEC 60870-5-101/-104 Protocol

IEC 60870-5-101 is transmission protocol used for communications between load dispatch center (LDC) and local SAS via serial interface. IEC 60870-5-104 is an extension of IEC 60870-5-101 based on Ethernet network.

D. Parallel Redundancy Protocol

The ability to reconfigure in case of a failure is an important parameter to determine the robustness and availability of a communications network. Compared to other well-known reconfiguration protocols, PRP follows an entirely different approach. It operates on two completely independent networks. The data are transmitted on both networks. The receiving end, which must be a PRP compliant entity, accepts the message arriving first and discards the other. Deploying this protocol without explicit reconfiguration of network topology does not cause an interval of unavailability.

V. Communications Architecture

A modern SAS requires comprehensive integration of protection, control, and automation devices. These devices include logic controllers, protective relays, I/O modules, embedded computers and communications devices.

The competence and reliability of SAS depend on the Ethernet communications networks. Ethernet ring topology along with PRP is most reliable as it improves system determinism by combining the self-healing feature of an RSTP ring and the seamless redundancy of PRP.

Ethernet ring topology is famous for its flexibility, low overhead, and easy installation. It can be established using Rapid Spanning Tree Protocol (RSTP). RSTP works by blocking one of the paths in normal operation and serves it as a backup during contingencies by re-enabling it.

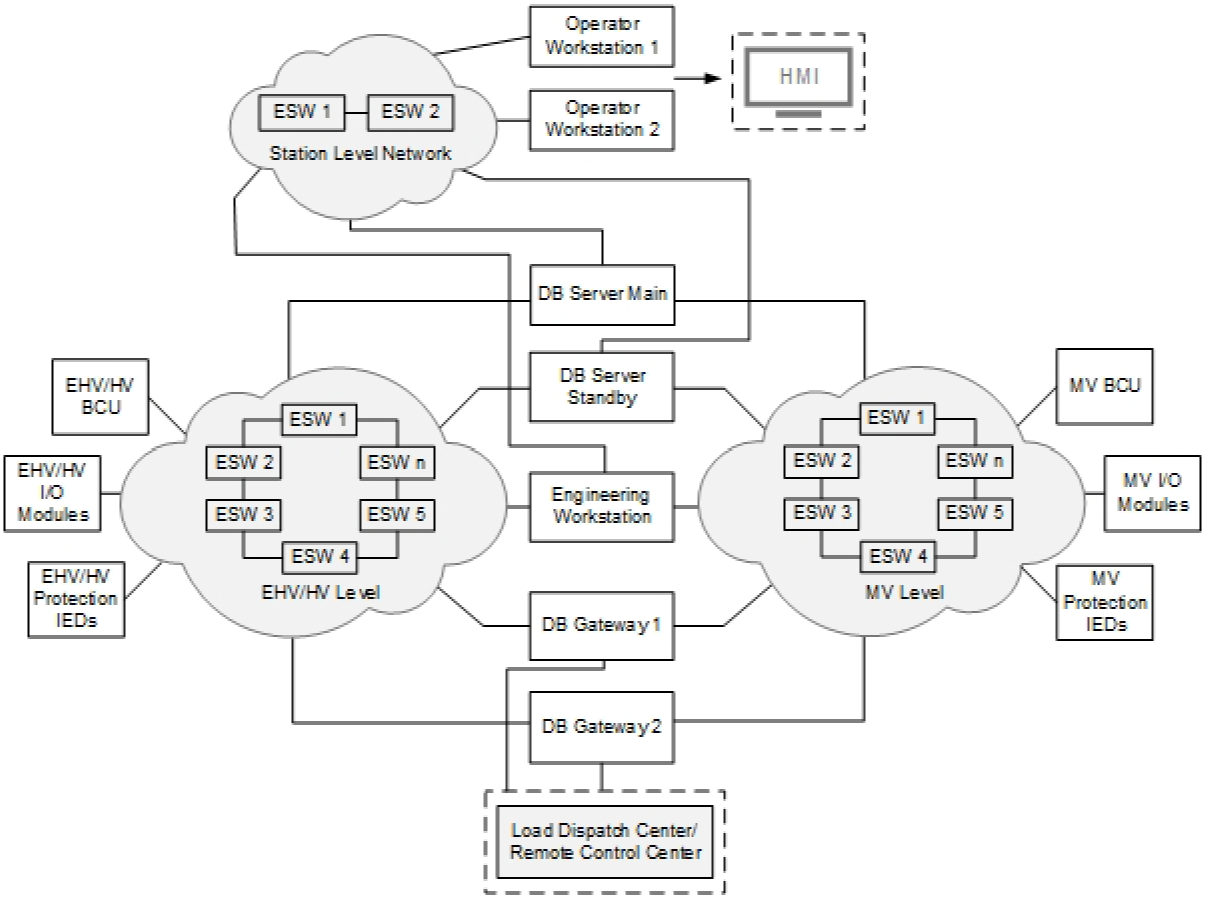


Fig. 5 Network Architecture for SAS

Various independent ring topology networks can be implemented; Fig. 5 is an example that shows a network with three rings named Station Level, extra high voltage (EHV)/high voltage (HV) Level, and medium voltage (MV) Level. This segregation is recommended to separate the station devices from the field devices and reduce the number of Ethernet switches in each ring to improve the RSTP network recovery time. Station Level serves as a communications path between DB servers and OWS where HMI is installed. HV and MV Levels provide a communications path between field IEDs and DB servers, Gateways, and the EWS.

PRP provides the redundancy for FO connections between IEDs and Ethernet switches. IEDs connected to two independent Ethernet rings transmit and receive the same data simultaneously and achieve bumpless redundancy with zero-millisecond failover time. PRP implementation is shown in Fig. 6. Redundancy (Red) Boxes are used to connect devices that do not support the PRP feature.

It important to note that the communications network is not only for IEC 61850-based data communication but is also used for other services like time synchronization using SNTP, engineering access to IEDs from EWS via Telnet and File Transfer Protocol (FTP), network Ethernet switch monitoring, and server monitoring using SNMP.

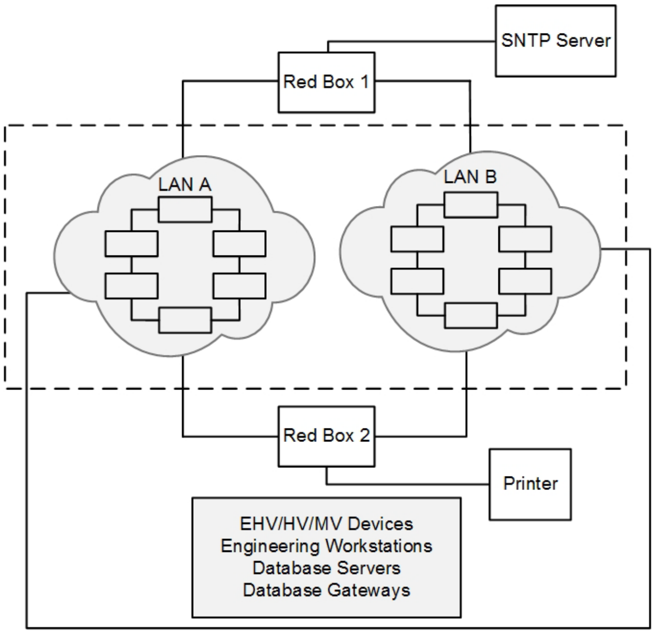


Fig. 6 Connection of Redundancy Boxes in PRP Network

VI. Cybersecurity

Cybersecurity is no longer an additional cost that can be eliminated to meet budget requirements. This is especially important as businesses are more digitized, meaning they are exposed to an increasing number of threats if security risks are not managed properly. Cyber attacks in which attackers try to access and control a private system, disrupt the system functionality, or even obtain financial gain are targeting private businesses and governments. Those attacks do not have to originate outside the organization; they can be initiated from within. Consequently, cybersecurity should be planned from the beginning and cover the entire organization. Cybersecurity is becoming a necessity for each system in IT, as well as in operational technology (OT) to protect the network, data control, and daily business operations.

A. Define and Document Organization Policies

Confirm that the company has its own policies by identifying valuable assets and how they are protected. Identify the most critical threats, their effect on the organization, and risk mitigation. A checklist helps apply those company policies to daily activities and allow easy tracking.

B. Monitor the Network

In OT networks, visibility is the most powerful cyber defense. Risks can only be prevented if you know what is running on the network. The best way to achieve visibility is a network management system that monitors network device performance.

C. Firewalls

Firewalls between data levels within an organization's network securely segregates the network by creating a security perimeter. This ensures a securely segregated network by creating perimeter networks (also known as DMZ, demilitarized zone, and screened subnet). If any level of security, the intruder faces a lock that blocks the attack. Centralizing storage of important process data for business analysis is required and allows communication between IT and OT networks. Industrial firewalls with a predefined database of industrial control system (ICS) and SCADA protocols are used as a first line of defense in OT networks.

D. Update Software

Malware attack old and known vulnerabilities. It is paramount to anticipate the attackers before they learn the system weaknesses and exploit them. System administrators should update operating systems, antivirus software, and applications. Some organizations do not perform these updates as it is cumbersome, and can disrupt the ongoing operations. Updates should be included in company policy with a clear implementation procedure.

E. Install Antivirus Software

Phishing emails, suspicious USBs, guest computers, and malicious code attached to legitimate software are always a threat, especially when employees are not following rules and policies. Keeping a continuous-monitoring software to oversee their activities helps stop and prevent any illegal execution. Most importantly, update the software on a regular basis or even daily, if possible.

F. Practice the Principle of Least Privilege

When granting access to user, administrators tend to default to minimum privileges. If access to sensitive data is required, a higher privilege is granted if approved by management. Access should be documented, timed, and revoked when it is no longer needed.

G. Require Secure Password Practices

Administrators generally require users to create passwords not less than eight characters, having alpha numeric upper and lower case in addition to a special symbol. This creates a defense mechanism against brute force, dictionary, and rainbow table attacks. According to some cybersecurity reports, over sixty percent of breaches happened because of a lost or stolen password. Supervisors should require users to change their password frequently, meaning every four to six months or two to three times per year. This is not applicable to users only; system administrators should also practice this on network devices such as switches, routers, firewalls, servers, computers, and IEDs.

H. Use Multifactor Authenticator

If a user account is compromised via a security mistake or social engineering, which are very likely, using a second factor of authentication is essential as it adds another layer of protection. In addition to a password, each user should have a certificate, biometric scan, or PIN number sent to their mobile device as a Short Message Service (SMS) or through an external application to access the account.

I. Back Up Data and Prepare a Plan

No matter how prepared an organization is, the possibility of a breach should be considered. The organization should back up their systems regularly and store backup files in a safe place in a different location. This measure is helpful not only for cyber attacks, but also hardware malfunctions, fires, natural disasters, etc. The organization should also have a clear strategy for reacting to and performing in such situations, as well as the expected online return time.

J. Employee Awareness

All employees should be trained for network security as well as physical security without exception. It is widely known that users are the weakest factor in the cybersecurity defense mechanism. Disobeying the rules or bypassing security protocols to achieve a more comfortable way creates cracks in the system that exposes the organization to attacks. Employees should be updated regularly on new policies and protocols to educate them and enforce accountability.

K. Mobile Devices

Regardless of whether an organization is IT or OT, guests and maintenance engineers often bring personal laptops and connect to the organization network. Personal computers may have malwares or viruses that could be planted into organization network devices. To avoid this, it is better to keep extra laptops ready for guests to use. The laptops should be equipped with limited access and the correct applications and software to facilitate a secure workspace, as well as protect the organization from any sources of data bleeding.

VII. SAS Visualization

As mentioned, SAS provides overall monitoring and control of substation from the local HMI. The HMI is a graphical representation of the complete substation that collects real-time information from the DB server, which takes data from field devices and transforms them into dynamic graphics, alarm, and event texts. The following are notable features that are served by the SAS HMI.

A. Overall Single-Line Diagram

The main screen of the HMI shows the single-line diagram of each voltage level (380 kV/110 kV/33 kV/13.8 kV). The diagram presents the open/close status of all the equipment, i.e., circuit breakers (CBs), isolators (ISOs), earth switches (ESWs), and line/bus potential transformers (PTs). It also shows the voltages and frequencies of the available buses and names and number of transformer, incomer, bus section, and bus coupler bays. The screen contains other useful information such as voltage levels of transformer bays, remote substation/circuit names of incoming bays, etc. This screen only monitors equipment for control purposes; the user must navigate to the associated bay view of the equipment. Fig. 7 shows a portion of a sample single-line overview screen.

B. Individual Bay Views

This type of screen provides detailed information about the individual bays. The number of screens equals the number of bays available in all substation voltage levels. This view provides the following information about the bays:

- Measurement of phase-to-phase voltages, phase current, active/reactive power, frequency, and power factor.
- Position of the bay selector switch, i.e., Off, Emergency, Local/BCU, Remote.
- Position of synchronism selector switch and state of synchronization; this information is available only if there is a bay-supporting synchronism check feature.
- Names of associated bay control units (BCU)s, protection relays, and I/O modules, as well as their fail/normal status.
- Open/close status of available switching equipment.
- Interlocking condition (satisfied or not) for each controllable equipment.

Individual bay views also allow the authorized user to initiate commands for the controllable equipment, e.g., CBs, ISOs, on-load tap changer (OLTC), etc.

C. Interlocking Screen(s)

This screen is responsible for giving in-depth information regarding the interlocking logic of controllable equipment. It also depicts the real-time information about the interlocks in a logic gate (AND/OR) circuits that facilitates easy identification and marking of the unsatisfied interlocking condition blocking the equipment from operating. This type of screen is helpful for the operators during maintenance and switching activities during which they must satisfy certain interlocks before any operation.

D. Communications Screen(s)

Ethernet switches are integrated with DA servers to provide port up/down statuses. This screen shows information related to the network.

E. Miscellaneous Screen(s)

Other screens include the alarm list that shows all points configured as alarms with defined priority and color; the event list that provides record of all operator actions, switching between servers to share master/standby roles, user login information etc.; and the legend screen that provides a description of each symbol and color used for developing all screens.

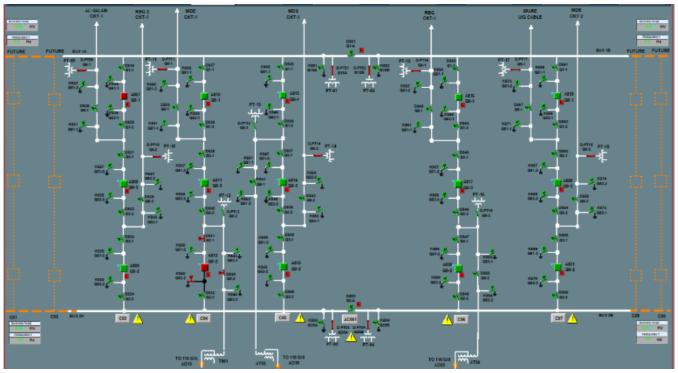


Fig. 7 Sample Single-Line Overview Screen

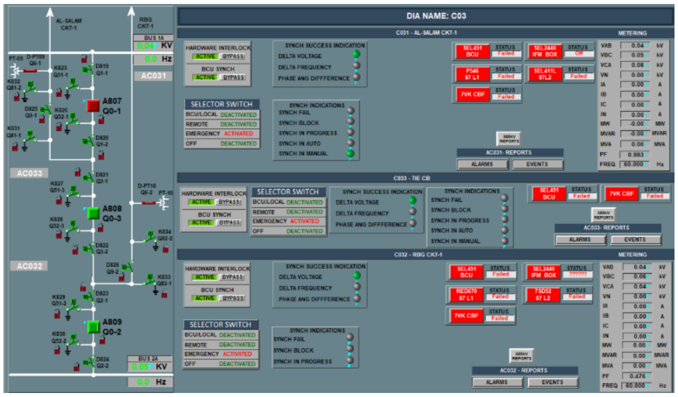


Fig. 8 Sample 380 kV Bay View

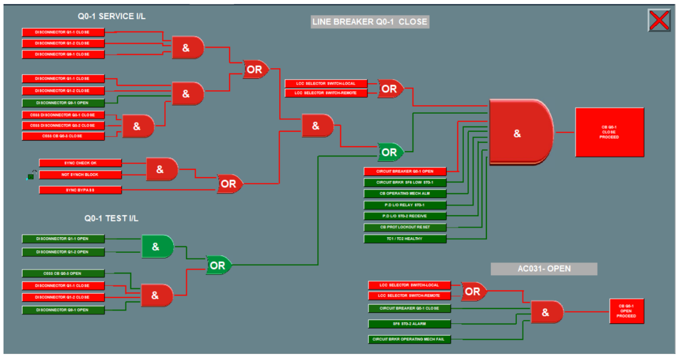


Fig. 9 Sample Interlocking Screen

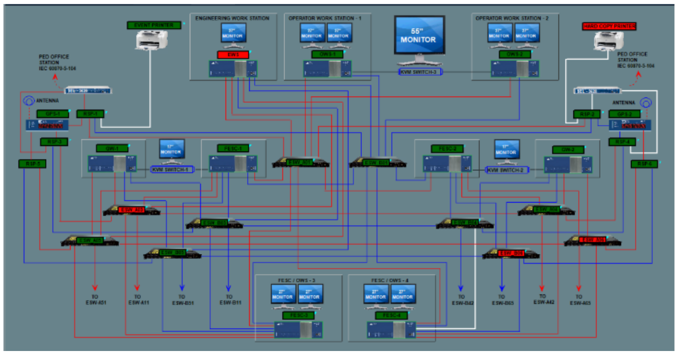


Fig. 10 SAS Communications Network Overview

VIII. SAS Operation Philosophy

The SAS is designed and deployed based on the information from Sections III through VII. However, an understanding of integrated operation is also important to describe. This operation is dependent on the reference, which can be either the local substation where SAS is deployed or the remote-control center.

A. With Reference to Local Substation

Firstly, handling database servers is important because they are the brain of an SAS. The local substation has the privilege to enable/disable and switch between master/standby for database servers. These servers should be synchronized so that if the master fails, the standby takes over with updated system information. Secondly, there is complete control and monitoring provision available for each substation section, i.e., diameter, bay, and feeder. The operator can control each equipment (i.e., breaker, disconnect switch, and ESW) based on satisfied interlockings programmed in the control IED of respective bays as well as satisfying synchronization check conditions (if required). The interlocking and synchronization features can be bypassed via control buttons on the HMI. Lastly, the operator has an option to switch the control mode of the control IED to either HMI or local. In the case of local, the control functions can only be performed through the IED front panel; however, complete monitoring is still available on the HMI screen. In the case of HMI control, the IED can only be controlled via the HMI.

B. With Reference to Remote Control Center

Every utility system has a load dispatch center or load control center that monitors multiple transmission substations simultaneously. It means the control and automation systems installed in remote centers are communicating with multiple SASs. For this communication, every SAS has GW servers; these are like database servers in terms of communicating with all SAS components, but differ in that they are not provided with an HMI. They also convert all information gathered over IEC 61850 MMS/GOOSE to IEC 60870-5-101/104 and transmit per the customer-specific I/O list. Usually, the data transmitted between the local substation and remote center are limited and grouped to optimize transmission. The SAS control is usually with the remote center unless the control is disabled from the local substation HMI or GW servers are stopped/disabled.

IX. Conclusion

Deploying a robust, secure, and reliable SAS requires understanding and following various aspects of engineering and design identified and explained in this paper. The SAS built on IEC 61850-based protocols with a diligently engineered, secure, highly-available PRP-based network is the key to implementing the smart grid concept. Handling the various properties of different protocols with proper knowledge and best-known methods ensure an optimized SAS capable of providing an efficient platform for automation control and monitoring.

X. References

[1] N. Moreno, M. Flores, L. Torres, J. Juárez, and D. González, “Case Study: IEC 61850 as Automation Standard for New Substations at CFE, Practical Experiences,” proceedings of the 12th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2010.

[2] C. E. Anderson, S. Zniber, Y. Botza, D. Dolezilek, and J. McDevitt, “Case Study: IEC 61850 Application for a Transmission Substation in Ghana,” proceedings of the Power and Energy Automation Conference, Spokane, WA, March 2013.

[3] S. A. Obaidli, V. Subramaniam, H. Alhuseini, R. Gupta, D. Dolezilek, A. Kalra, and P. Sankar, “IEC 61850 Beyond Compliance: A Case Study of Modernizing Automation Systems in Transmission Power Substations in Emirate of Dubai Towards Smart Grid,” proceedings of the Southern African Power System Protection and Automation Conference, Johannesburg, South Africa. November 2017.

XI. Biographies

G. M. Asim Akhtar is a special protection systems engineer. He joined Schweitzer Engineering Laboratories, Inc. in 2015. He earned his B.Sc. degree from NED University of Engineering and Technology in Karachi, Pakistan, and his M.Sc. degree from King Fahd University of Petroleum and Minerals in Dhahran, Saudi Arabia. Before joining SEL, he was employed by Pakistan Petroleum Limited as a senior engineer responsible for electric power operations and maintenance. His research interests include power management systems, substation automation, electric vehicles, and the integration of renewables into power grids. In addition to his technical papers in the field of electricity market and electric vehicles, he holds one U.S. patent.

Muhammad Sheraz is special protection systems engineer. He joined Schweitzer Engineering Laboratories, Inc. in 2014. He earned his B.Sc. degree from the University and Engineering Technology (UET) in Lahore, Pakistan, and his M.Sc. degree from King Fahd University of Petroleum and Minerals in Dhahran, Saudi Arabia. He received Best Poster Award, International Conference on Renewable Energies and Power Quality, Bilbao, Spain, March 2013. His research interests include power management systems, substation automation, and the integration of renewables into power grids.

Ali Safwan is a regional services manager for the Middle East and North Africa regions. He has been with Schweitzer Engineering Laboratories, Inc. since 2010. Before joining SEL, he was associated with the oil and gas industries for almost 25 years. His areas of expertise include design engineering and services of electrical power systems along with networking and cybersecurity.

M. Akhil Fazil is a regional engineering services and proposals manager for the Middle East and North Africa regions with Schweitzer Engineering Laboratories. Inc. He earned his B.S. degree in electronics and communication in 1999 from Osmania University in Hyderabad, India. He started his career in 2001as an automation engineer with Schneider Electric, Saudi Arabia, where he was responsible for providing solutions for substation and industrial automation applications through system design, integration, and commissioning activities. Mohammed was hired by Schweitzer Engineering Laboratories, Inc., in March 2008 as an integration application engineer. He was involved in the design, development, implementation, commissioning, and execution of substation automation-based projects.

Firas El Yassine is network engineer. He joined Schweitzer Engineering Laboratories, Inc. in 2016. He earned his B.Sc. and M.Sc. degrees in 2002 in computer engineering from University of Balamand (UoB), El-Koura, Lebanon. He worked in different companies in the IT industry. He holds certifications from Cisco: CCNP R&S, CCNP Security and from Microsoft: MCITP.

20180626 • TP6875-01