IEC 61850 Beyond Compliance: A Case Study of Modernizing Automation Systems in Transmission Power Substations in Emirate of Dubai Towards Smart Grid

Sultan Al Obaidli, Venkataraman Subramaniam, Hamood Alhuseini, and Ramesh Gupta
Dubai Electricity & Water Authority

David Dolezilek, Amandeep Kalra, and Prasanth Sankar
Schweitzer Engineering Laboratories, Inc.

Presented at
Saudi Arabia Smart Grid 2017
Jeddah, Saudi Arabia
December 12–14, 2017

Originally presented at the
Southern African Power System Protection & Automation Conference, November 2017

IEC 61850 Beyond Compliance: A Case Study of Modernizing Automation Systems in Transmission Power Substations in Emirate of Dubai Towards Smart Grid

Sultan Al Obaidli, Venkataraman Subramaniam, Hamood Alhuseini,
and Ramesh Gupta, *Dubai Electricity & Water Authority*
David Dolezilek, Amandeep Kalra, and Prasanth Sankar, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—A substation control and monitoring system (SCMS) is composed of digitally connected devices that exchange information using multiple communications protocols to protect, control, and monitor entire substation automation applications remotely from respective control centers. It is also essential to combine cybersecurity within the SCMS. In an effort to move towards smart grid, the Dubai Electricity & Water Authority (DEWA) initiated a long-term contract for the supply, installation, testing, and commissioning of 33 substations (132/11 kV) with modern automation systems for transmission power substations. DEWA has very strict requirements in terms of system availability, reliability, performance, cybersecurity, Ethernet network resiliency, and protection and communications redundancy. An HMI is included in the SCMS for local indication and control. Status, metering, and control data to the local HMI and remote utility enterprise system is provided by a redundant SCADA system. Reliable and secure communications to support mission-critical, high-speed protection schemes is achieved by an Ethernet network of utility-grade operational technology (OT) switches, not IT switches. The Ethernet network uses a modified ladder topology with IEC 62439 Part 1 Spanning Tree Algorithm (STA) via Rapid Spanning Tree Protocol (RSTP) for network resiliency and IEC 62439 Part 3 Parallel Redundancy Protocol (PRP) for message duplication. Data segregation and traffic control in the SCMS network is provided by IEEE 802.1 VLANs. The data acquisition and control along with engineering access and event report collection is accomplished using manufacturing message specification (MMS), whereas high-speed signal exchange for peer-to-peer protection schemes is accomplished using GOOSE communications protocols from the IEC 61850 communications standard. The DEWA technical SCMS specifications were built around the concept of future proofing and backward compatibility to support the evolution of smart grid capabilities by accepting smart technological advancements and future development of substation automation system features. It is strongly believed that the technical improvements made in DEWA specifications will lay a solid foundation for a sustainable automation system in DEWA over the years to come.**

Because DEWA is aware of the risks of digitizing substation communications networks and the recent increase in the number of cyberattacks against utilities that involve abusing vulnerabilities in the security of their communications networks, DEWA has strict cybersecurity requirements to prevent cyberinduced power outages that could potentially disrupt an electric power grid. The SCMS was designed with the holistic approach of a defense-in-depth philosophy, including supply chain security and physical security. The DEWA SCMS security design relies on a multilayer security zone approach to provide a scalable cybersecurity solution that automates tasks, streamlines operations, and improves performance.

This paper discusses DEWA system requirements developed to facilitate the safe, reliable, and economical delivery of power in Emirate of Dubai. This is followed by a discussion of various engineering decisions that resulted from lessons learned during the design stage of the DEWA transmission power substation automation system to ensure that the system is ready for future smart grid requirements. Various analysis tools and testing techniques are described in the paper that were used to quantify the performance attributes of the IEC 61850-based system design. This project proves that with the right engineering design and a properly configured Ethernet network that uses best engineering practices for OT, performance, interoperability, and compliance to standards can coexist.

I. Introduction

Dubai Electricity & Water Authority (DEWA) was established in 1992 by His Excellency Sheikh Maktoum bin Rashid Al Maktoum with an objective to provide the reliable and adequate delivery of power to residents of Emirate of Dubai. Since its inception, DEWA has continuously invested in maintaining and upgrading the power delivery infrastructure to meet the increasing demands of the growing Emirate of Dubai.

In 2015, DEWA awarded a North American engineering services firm a long-term contract to supply, install, test, and commission 33 substations (132/11 kV) with the goal of modernizing the automation system technology in transmission power substations.

II. Engineering Design for Aggressive Growth

The new technical specifications were built around the concept of future-proofing the substation control and monitoring system (SCMS) to cope with technological advancements and future developments in the field of substation protection and automation. The multiyear project consisted of installing and commissioning an IEC 61850 Edition 2-based SCMS. One major objective of the SCMS was to avoid the use of conventional operator control and metering panels, local alarm annunciator panels, conventional CTs and VTs (where possible), hardwired connections for inputs and outputs, and standalone digital fault recorders (DFRs) by

exploiting the latest state-of-the-art distributed control system technology. The SCMS design achieved this objective by using digital communications to assist in monitoring and controlling the substation's primary equipment in a secure, reliable, safe, and cost-effective manner.

The system engineering process is now fully compliant with IEC 61850, and there is emphasis on compliance with IEC 61850-6 Edition 2. Certification of product conformance to IEC 61850 is essential in providing confidence that the products will support interoperability and future additions. Some manufacturers have their own test lab capabilities to improve product development and test conformance as part of all the other associated product and type tests. Third-party, ISO-accredited, Class A test labs were also used to verify product conformance from each SCMS supplier.

During the detailed design phase of the project, the following aspects were reviewed and approved:

- An interoperability document of the IEC 61850 standard from the vendor (Protocol Implementation Conformance Statement [PICS]/Protocol Implementation eXtra Information for Testing [PIXIT]).
- Substation Configuration Description (SCD) and IED capability description files (ICD).
- Mapping of SCADA I/O signals to an IEC 61850 communications model to achieve interoperability across different IED vendors.
- Standard modelling of IEC 61850 to ensure full compliance with the standard. Standard logical nodes from IEC 61850 Edition 2 were used to avoid generic logical node usage.
- Assignment of an information object address (IOA) for gateway servers to connect to remote SCADA control centers in line with the standard guidelines issued by DEWA.
- Remote user access authentication through demilitarized zone (DMZ) using active directory services from the DEWA centralized Lightweight Directory Access Protocol (LDAP) server.

A station HMI is included in the SCMS for local indication and control in conjunction with front-panel HMIs on the IEDs. Status, metering, and control data to the local HMI and remote utility enterprise system is provided by a redundant SCADA system. Reliable and secure communications to support mission-critical, high-speed protection schemes is achieved by an Ethernet network of utility-grade operational technology (OT) switches, not IT switches. The system translates between various communications protocols and interfaces with the redundant servers in the DEWA transmission control center and distribution control center infrastructures. The SCMS system design provides various benefits such as maximizing the effectiveness of the system, improving complete system awareness, and increasing work efficiencies across multiple departments within the company because of new secure remote access capabilities. DEWA identified the following objectives that they wanted to achieve through implementing an SCMS:

- Increase system reliability.
- Increase LAN availability.
- Achieve better defense against cyberattacks.
- Improve system operation and understanding.

The Ethernet network uses a modified ladder topology that incorporates IEC 62439 Part 1 Spanning Tree Algorithm (STA) via Rapid Spanning Tree Protocol (RSTP) for network resiliency, IEC 62439 Part 3 Parallel Redundancy Protocol (PRP) for message duplication, and IEEE 802.1 VLANs to provide data segregation and traffic control. Data acquisition along with control, engineering access, and event report collection in the SCMS is accomplished using the manufacturing message specification (MMS) protocol, whereas high-speed, peer-to-peer signal exchange for the protection and automation schemes is accomplished using GOOSE communications protocols from the IEC 61850 communications standard. The DEWA technical SCMS specifications were built around the concept of future proofing and backward compatibility to support the evolution of smart grid capabilities by accepting smart technological advancements and future development of substation automation system features.

This paper describes how DEWA in collaboration with a North American engineering services firm implemented a cost-effective system that provides a very capable, reliable, dependable, and secure SCMS.

III. Specification of Communications Services via IEC 61850 and Companion Standards

IEC 61850 is one of several IEC and IEEE technical standards related to communications networks used to protect and control electric power systems. Several international standards, including IEC 61850, together define the expected behavior and performance of mission-critical communications, including the following:

- IED performance requirements (IEC 61850, IEC 60834, IEC 15802, IEEE 802.1, and IEEE 1613).
- Message latency specifications (IEC 61850, IEC 60834, IEC 15802, and IEEE 802.1).
- Message speed (IEC 61850).
- Signal exchange dependability and security requirements (IEC 61850 and IEC 60834).
- Signal exchange availability requirements (IEC 61850, IEC 60834, and IEEE 802.1).
- Signal exchange reliability metrics (IEC 61850, IEEE 1613, and IEC 60870).

Based on these standards, a service level specification can be created for each class of digital communications. Then using this SLS, design engineers work with network and IED providers to create a service level agreement (SLA) for each type of digital message in the data flow design. Each SLA defines the commitment between the service provider and the client. Specifically, the aspects of the service—quality, availability, and responsiveness—are designed and documented between the service provider and the service user.

As an example, those IEC and IEEE standards collectively define the SLS for exchange of protection and control signals as follows:

- The design must support signal exchange between IEDs in less than 3 ms, with Ethernet packet transit through a network in less than 1 ms, 99.99 percent of the time.
- The system can fail to meet the design requirements the remaining 0.01 percent of the time but must not exceed a 15 ms Ethernet packet transit time through the network. Therefore, the time to detect and isolate Ethernet faults and reconfigure and reestablish communications must be less than 15 ms for the entire network. When this is not possible, it is the responsibility of the system designer to explain why and how often this requirement will not be met by the chosen design.
- To satisfy dependability, GOOSE exchanges with a one-second heartbeat shall not drop a single GOOSE message during an entire year. To satisfy security, IEDs shall not receive more than nine unwanted or extra GOOSE messages every 24 hours.
- For each signal exchange, performance levels shall be supervised, monitored, and recorded. Adequate statistics shall be available via out-of-band event reports.
- For each signal exchange, failures to meet the SLA will be detected immediately by each IED and registered as bad integrity for the duration of the failure. IEDs use this integrity status to indicate a failed signal exchange within the protection and automation logic.
- For each signal exchange, failures to meet the SLA will be reported in real time via IED front-panel HMI alarm and indication and will be reported to control, engineering, and cybersecurity clients.

IV. Editions of IEC 61850

IEC 61850 is actually a series of parts that documents important information as technical reports (TR), technical standards (TS), and international standards (IS). There are now 45 parts in the series and growing as the standard is called upon to document more standardized capabilities. The first vote on the standard resulted in all parts in the series being in Edition 1 simultaneously. Since that time, each part in the series has experienced slow and constant development to make improvements and add functionality via the technical issue (tissue) process. Many parts of the series are still in Edition 1, some are in Edition 2, and others are progressing towards Edition 3, as illustrated in the partial development history shown in Fig. 1.

IEC 61850 and associated TRs document many potential communications functionalities for numerous devices and software applications within various types of systems. Product developers implement an appropriate subset of the IEC 61850 functionality in conjunction with the other product features and applications.

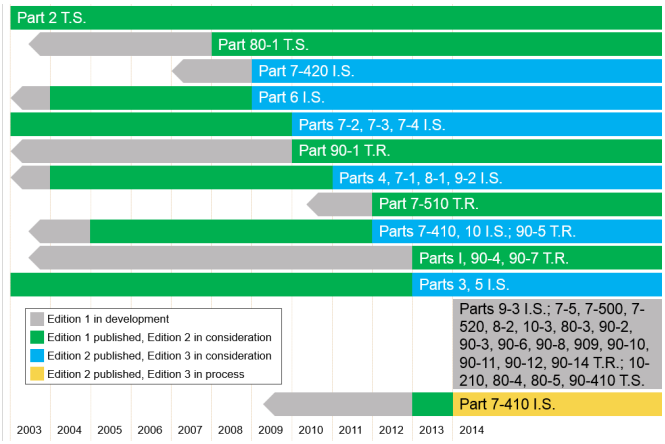

Fig. 1. Illustration of the Different Concurrent Editions of Parts of IEC 61850

UCA® International Users Group (UCAiug) acts to monitor and improve the state of IEC 61850 by collecting and addressing tissues. When accepted, most tissues are resolved by a group of technical experts and result in recommended changes to the applicable parts of the standard. Errors usually result in recommended modifications, ambiguities usually result in recommended clarifications, and new ideas usually result in recommended additions. These new changes are aggregated for a period of time until a group of them are proposed as a new edition to the applicable part in the series and put up for a vote. When new recommendations are accepted, the part is updated to a new edition. The intent of this process is that newer additions to the existing editions and new editions remain backward compatible. In some cases, these new additions reflect capabilities that already exist in some devices while others require new product development.

As documented at www.UCAiug.org, UCAiug also acts to monitor and improve the state of UCAiug test procedure versions. Test procedures are used to confirm product conformance to a specific subset of the functionality documented in IEC 61850 and associated TRs. The test procedures contain numerous test blocks that have mandatory and conditional requirements. These tests to not address all IEC 61850 functionality but rather a subset that is useful to improve interoperability among products. When required, the test procedures are updated to a new version to include additional tests. In some cases, these new additions reflect capabilities that already exist in some devices while others test new product features.

Product developers select test procedures and associated test blocks to be applied to their product. The testing service documents the product, test procedure version, and test blocks successfully applied to the product. Certificates of successful testing are given a Level A status when provided by an independent testing company that is not associated with product development or system development. A Level B status is given to certificates provided by an organization that may not be isolated from product or system development, such as a device manufacturer. Also, testing of features not specified in the UCAiug test procedures need to be tested by a Level B test facility that is familiar with the product and features.

Interoperability testing is the responsibility of each product developer and system developer. UCAiug hosts interoperability meetings annually for collaboration among manufacturers. Each manufacturer and system developer is expected to build and maintain an interoperability network made up of multiple versions of products from numerous manufacturers to confirm interoperability. Interoperability certificates are provided by Level B facilities that have experience in system development.

V. What Is New in Edition 2

Users informally consider the present edition of the standard to be that of Part 10 – Conformance Testing, which is in Edition 2 at the time this paper was written. As mentioned, the many parts of the IEC 61850 series exist as various editions based on their maturity and evolution. However, because Part 10 addresses the verifying conformance of some device capabilities within system specifications, end users often consider the Part 10 edition to represent the entire series. Therefore, the existing state of all documents at the time Part 10 became Edition 2 is collectively known as IEC 61850 Edition 2. Therefore, even though Part 90-4 is only in its first edition, it is equally or more important because it more fully explains system engineering guidelines. As a fundamental part of the Edition 2 system design, Part 90-4 provides advice and guidelines on device security, management of communications, engineering access, and testing for IEC 61850-based substation automation. At the same time, IEC 62439 Industrial Communication Networks – High Availability Automation Networks was referenced as a TR. Part 1 of this standard explains the resilient method of using STAs in unmanned systems to automatically detect and isolate Ethernet faults and then quickly recover by reconfiguring and reestablishing communications. Part 3 explains that if recovery technology is not available, repairable technology, such as PRP, can be used to duplicate messages in manned stations relying on people to detect and repair the Ethernet failure. Most PRP systems also include STA within the Ethernet design.

Therefore, IEC 61850 Edition 2 system capabilities are described by the many parts of the standard in general and the following references in specific:

- IEC 61850 Part 10: Conformance Testing – Edition 2.
- IEC 61850 Part 90-4: Network Engineering Guidelines for Substations – Edition 1.
- UCAiug Test Procedure Version 2.
- IEC 62439 Industrial Communication Networks – High Availability Automation Networks.

Many IEC 61850 system features have been present in numerous devices for over a decade. Many of these features were available but not considered or tested by the UCAiug Revision 1 test procedures. In addition, many features remain outside the scope of Version 2 test procedures. As an example, contemporary IEC 61850 system specifications referring to Part 10 and Part 90-4 identify 53 IEC 61850 Edition 2 features in the following five categories:

- IED function and Substation Configuration Language (SCL) file.
- IED cybersecurity.
- IED and network communications management.
- IED engineering access.
- IED communications and SLA testing.

Only 15 of these 53 unique features are addressed by the UCAiug Version 2 test procedures. Success often relies on manufacturers providing Level B testing for all of the necessary system features within and outside the scope of UCAiug Version 2 test procedures. By design, IEC 61850 describes communications and does not address cybersecurity. Instead, UCAiug recommends that device and system cybersecurity be accomplished using methods and standards created by security experts. For example, IEC 62351 Power Systems Management and Associated Information Exchange – Data and Communications Security is limited to the authentication of data transfer. Cybersecurity methods include data encryption and user authentication. However, comprehensive system security is left to the National Institute of Standards and Technology (NIST) Special Publication 800-37 risk management framework.

VI. System Specifications

DEWA was very clear with the requirements for the SCMS from the beginning of the planning and design phases. They not only wanted the SCMS to be compliant to the IEC 61850 standard, but they also wanted to achieve real-world interoperability without sacrificing the maximum performance and flexibility to satisfy present and future power system applications.

A. Hardware Requirements

Because of the geographical location and rugged environmental conditions of the installations, it was very important to write system specification requirements that demanded the system perform for decades in extreme temperature conditions. To meet the requirements of high availability and low maintenance cost, it was essential that the devices survive for decades in a harsh environment, fail very infrequently, and can be replaced quickly in the event of the failure. To keep maintenance activity to a minimum, the IEDs, Ethernet switches, computers, and firewalls within the SCMS must have low failure rates, as indicated by their mean time between failures (MTBF), and the ability to withstand a temperature range from –40 to +85°C.

B. Interoperability

To achieve the interoperability that DEWA was looking for, they selected devices from multiple manufacturers that had a proven record of interoperability, had participated in UCAiug interoperability testing, and had devices tested for IEC 61850 conformance certification.

C. Cybersecurity

DEWA was very well aware of global events and was looking for a holistic cybersecurity solution carefully integrated into the SCMS as part of a more comprehensive company-wide security framework. DEWA's primary focuses in this design requirement were availability and accessibility, including

remote access, and a strong focus on cybersecurity via multiple layers of defense against attackers.

D. Performance

IEC 61850-based substation designs are heavily dependent on connectivity between various devices to provide enhanced system capabilities. Therefore, it was very important to correctly engineer the communications network to achieve the desired system performance. DEWA had very stringent Ethernet network performance requirements, including the following:

- IEC 62439 Part 1 STA resiliency.
  - Immediate detection and isolation of Ethernet faults associated with port, cable, or device failures.
  - STA reconfiguration and reestablished GOOSE packet delivery in less than 8 ms within a single switch and less than 15 ms for virtually every fault in the network. In very rare instances, reconfiguration of a root bridge failure exceeds 15 ms.
  - Automatic, consistent, and rapid fault recovery and minimum message latency, even in the presence of additional Ethernet faults.
- Delivery of every protection and automation signal change of state within the SLA specification.
- Immediate detection and alarming of delayed and undelivered GOOSE packets.
- Scalability of system size without affecting performance.

E. Network Duplication

Network duplication was selected to provide two independent paths for each protection signal via IEC 62439 Part 3 PRP-based network methods. In PRP-based network designs, each IED is dually connected to two identical independent networks and each publishing IED duplicates each individual packet just as the packet egresses the device. Each subscriber accepts the first version of each packet and discards the received duplicated packet. This design increases the Ethernet network availability for the first Ethernet failure by duplicating message delivery. However, PRP does not detect this failure and cannot recover, and the result is a single-point-of-failure system. Thus, because PRP-based networks mask the first fault in the network and a second network failure could deny the exchange of duplicated packets, STA was also added to each network.

VII. System Cybersecurity Design

Defense-in-depth cybersecurity was applied from the very beginning of the planning and design phases of the project, which resulted in a robust and secure system that provides a reliable platform for future applications and improves the cybersecurity of existing implementations [1] [2].

A. Defense in Depth

DEWA, like all other utilities, has a comprehensive system design for cybersecurity, which includes corporate, control center, and grid communications. Control systems within the grid represent a subset of the overall company defenses. For the substation environment, defense-in-depth cybersecurity design provides a complete and robust OT security solution that connects to both the OT control center and corporate IT system. The multilayer security approach segregates different substation equipment to different layers, as shown in Fig. 2. Each layer has different sets of vulnerabilities with different strengths and weaknesses. A multilayer security approach provides an opportunity to evaluate each layer separately as part of the whole system to select separate defense mechanisms, resulting in a holistic cybersecurity system. For example, at Layer 1 physical access to the IEDs is a vulnerability. Therefore, the controls surrounding the protection of the ingress/egress point of the substation electronic security perimeter are provided by Layer 1. The security controls for communication and data concentrators are located at Layer 2. At the device level, host-based cybersecurity control is provided at Layer 3 [1][3].

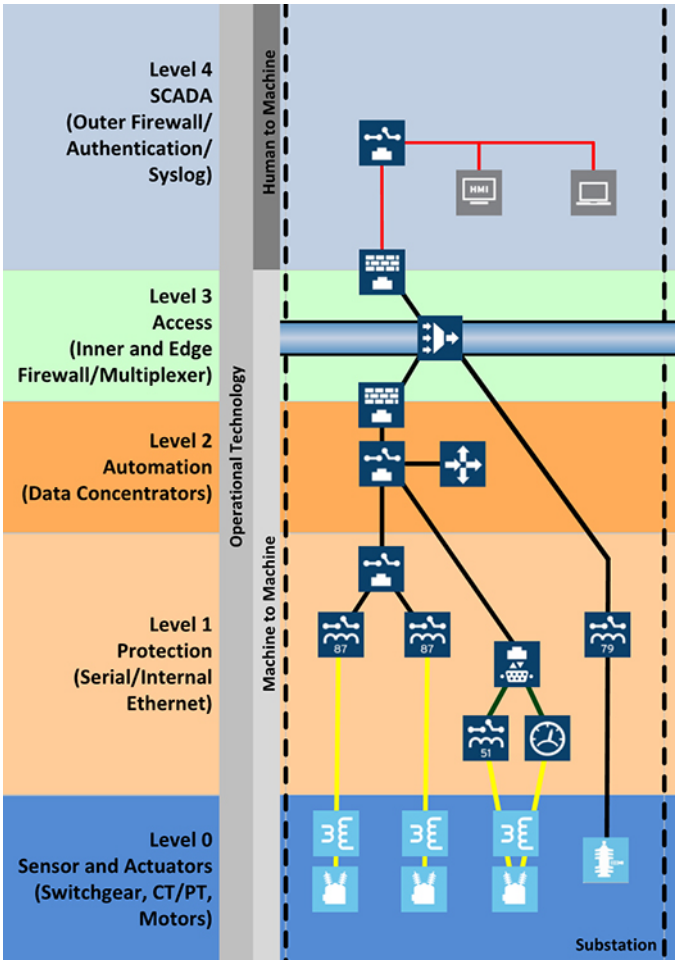

Fig. 2. Multilayer Defense-in-Depth Model

1) Centralized User and Password Management

The SCMS includes various innovative features like automatic management of IED passwords. The centralized password management device (CPMD) keeps clear distinction between the different steps of generating new IED passwords and applying IED passwords. It can generate and apply new complex passwords to the IED or revert the IED passwords back to a default state in the case of extenuating circumstances (e.g., a natural disaster). A user with administrative privileges in the CPMD can automatically generate and apply passwords for all connected IEDs based on a regular time period (e.g., every 90 days).

2) Proxy Password Services

The proxy services function helps in creating a user audit trail through strong and centralized user-based authentication and authorization support for modern and legacy IEDs. The CPMD manages protected IED passwords, ensuring that passwords are changed regularly and that they conform to complexity rules for stronger security. Therefore, robust password requirements can be satisfied by enforcing strong passwords on IEDs, configuring the CPMD to automatically change the password on a configurable schedule, and ensuring that no weak or default passwords are in use [4].

3) Allowed Clients and Whitelisting

Allowed clients are hosts or networks that have authorization to access Ethernet-based services running on the device. Administrative users can configure allowed clients to access the web management, VPN, port switch, device time, and Simple Network Management Protocol (SNMP) services or combinations of the five services. The device logs all configuration changes to allowed clients. Allowed clients are considered to be an IP whitelisting of incoming connections to services running on the device. Once an administrator has defined an allowed client for a service, then only that allowed client can use the service unless the administrator adds more allowed clients for that service.

4) Exe-GUARD®

Exe-GUARD antivirus technology provides host intrusion prevention protection against past, present, and future malware threats via a strong whitelist defensive architecture [5]. The biggest advantage of this technology is that the need for signature updates is eliminated without adding any additional settings to the device. Exe-GUARD provides protection against rootkits, contains kernel-level whitelisting with secured memory privileges, and implements mandatory access controls (MACs). With executable whitelisting, powerful resistance to code injection is provided by the Exe-GUARD.

VIII. System Communications Network Design

A. Best Engineering Practices for Network Topology

Ethernet communication in the SCMS is a switched network with several physical cable paths or loops, like cables in a looped electrical distribution system, where one is active and the others may act as hot standby. Ethernet packets are prevented from traveling in a loop back towards their IED of origin by an Ethernet switch mechanism that virtually opens and stops the packet flow.

Physical loops in the Ethernet network are prevented using Rapid Spanning Tree Algorithm (RSTA) and RSTP by algorithmically enabling and disabling links in a topology within the physical wiring of the network. For a reliable and dependable Ethernet packet distribution network, periods of network darkness should be as short and infrequent as possible. An extended ladder topology, as illustrated in Fig. 3, was deployed to increase the size and availability of the DEWA Ethernet network and the SCMS. To duplicate each Ethernet message, IEC 62439 PRP-enabled devices were connected to two redundant extended ladder Ethernet networks. IEC 62439-3 Clause 4 standardized the PRP as a data communications network protocol. The IEDs supporting PRP are connected to two independent Ethernet networks, which may also support RSTA and RSTP. In this way, when one network is dark, the other will likely not be dark and the signal transmission will be more reliable. A PRP network without a reconfiguration method like RSTA and RSTP only works for one failure and then becomes permanently failed. Each independent PRP network requires transmission, transfer, and transit time tests.

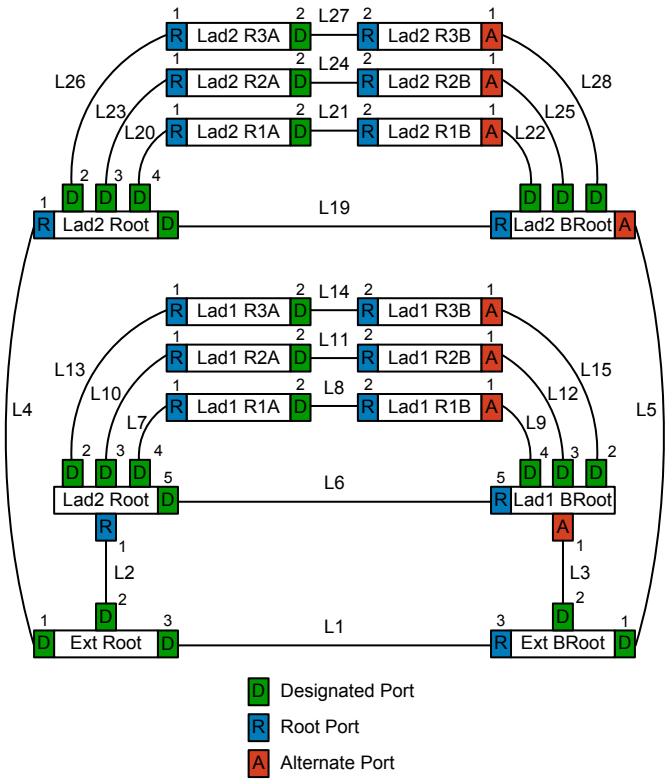

Fig. 3. Extended Ladder Topology

B. Best Engineering Practices for Digital Communications

The best-known methods for precise GOOSE performance are described in multiple international standards. These best-known methods and the associated standards are documented in the paper titled “Case Study of Time-Domain Automation and Communications: Field-Proven Benefits to Automation,

Control, Monitoring, and Special Protection Schemes" [6] and are repeated here as the following:

- Create message segregation via a unique VLAN ID per GOOSE message (IEC 61850 and IEEE 802.1).
- Create message segregation via unique multicast MAC addresses per GOOSE message. (IEC 61850 and IEC 15802).
- Assign a unique application identifier (APP ID) per GOOSE message (IEC 61850).
- Match the last octet of the MAC address, VLAN ID, and APP ID.
- Use message priority tags based on the mission-critical nature of the communications-assisted application (IEC 61850 and IEEE 802.1).
- Assign a descriptive GOOSE ID rather than generic GOOSE ID (IEC 61850).
- Use a descriptive textual name and VLAN ID.
- Carefully design data set contents and message retransmission properties (IEC 61850 and IEC 60834).
- Choose IEDs and switches that immediately publish, transmit, and react to GOOSE messages (IEC 61850 and IEC 60834).
- Select root bridge Ethernet switches and IED ports based on actual network performance in primary and reconfigured states (IEC 61850 and IEEE 802.1).
- Test and verify Ethernet switches to satisfy 7 ms reconfiguration times within one switch and 15 ms reconfiguration time across the network. These methods must be based on standardized STAs and RSTP rather than proprietary solutions (IEC 61850, IEC 60834, and IEEE 802.1).
- Provide high availability to mission-critical applications using redundant devices as well as redundant communications (IEC 61850).
- Ensure that all network multicast messages have a unique VLAN ID and MAC address. All untagged traffic must be tagged with port-based VLAN (PVLAN) 1001 at ingress to the Ethernet network (IEC 61850 and IEC 60834).
- Disable all unused IED and switch communications ports. All network engineering ports must have static MAC address filters to prevent all but known engineering laptops (NERC CIP and NERC PRC-005).
- Ensure that all IEDs monitor the multicast message sequence number and state number to supervise data exchange via digital messaging (IEC 61850 and IEC 60834).
- Ensure that all IEDs create GOOSE diagnostic reports, including performance and reliability statistics and real-time operational information for each published and subscribed GOOSE message (IEC 61850 and IEC 60834).
- Ensure that each IED supervises all GOOSE attributes to detect and alarm abnormal behavior via the front-panel display, SCADA alarms, and email to technicians (IEC 61850 and IEC 60834).
- Ensure that each IED time-stamps and creates a sequential events record for each GOOSE message failure and then reacts to the failure by modifying logic as well as local and remote applications to reflect that communications-assisted data acquisition has failed (IEC 61850 and IEC 60834).

IX. Performance Validation

As mentioned, the IEC 61850 Part 90-4 Technical Report provides advice on network engineering and commissioning [7]. Section 5.3.17 describes testing and specifically recommends the following: "Once the network has been designed, its compliance to the requirements needs to be tested, first as a design verification, then during factory acceptance tests and finally at site acceptance." This TR also requires that an appropriate subset of the tests should continue to monitor the network during operation and detect and mitigate failures and conformance to SLAs. Point-to-point client-server exchanges are monitored by traditional feedback mechanisms. However, because data producers are unaware of multicast message delivery, signal exchange between data producers and data consumers must be monitored by each consumer.

Each subscriber must uniquely monitor and validate the SLA for each multicast exchange. In the case of GOOSE messages, each message exchange is supervised in real time to confirm its integrity before signal contents are used for communications-assisted protection and logic. This supervision includes the following:

- Consumer devices detect and document delayed GOOSE message events for each subscription.
- Consumer devices detect and document undelivered, lost GOOSE message events for each subscription.
- Consumer devices detect and document the maximum quantity of packets lost in a single event, total aggregate quantity of packets lost, and maximum outage time as the duration of time the GOOSE messages are not received for each GOOSE subscription.
- Consumer devices create and store a GOOSE message receipt report containing message configuration information as well as the message status, including priority tag, VLAN, state number, sequence number, time-to-live (TTL) value, and error code for each subscription. In this case. the TTL value is recalculated in real time and represents the expected time duration before receipt of the next GOOSE message.
- Consumer devices create and store a GOOSE message receipt event report containing statistics of the GOOSE receipt performance, including:
  - Out-of-sequence count. This is the count messages lost because of both sequence number and state number out-of-sequence errors. It is not recorded

for the first message after the device is turned on or reconfigured.
- TTL count. This is the count of the number of times a message is not received within the expected time interval.
- Decode error count. This is the count of the number of messages where enough information is decoded to associate them with a subscription but fails further decoding because of corruption or errors, such as a mismatched data set.
- Buffer overflow count. This is the count of the number of messages that are discarded because the message receive queue was full. This may occur as a result of time compression in the network that causes two packets from the same subscription to be received within one publication period. The receiving IED should discard the older packets for this subscription and process only the newest one.
- Message lost count. This is the aggregate count of the estimated number of messages lost because of out-of-sequence errors. For each out-of-sequence error, the number of messages lost is estimated by subtracting the expected state number from the received state number and the expected sequence number from the received sequence number and summing them. This estimate is only made if the state number or sequence number in the received message is greater than expected.
- Maximum message lost count. This is the maximum estimated number of messages lost for an out-of-sequence error.
- Total downtime. This is the total time (in seconds) the subscription was in an error state.
- Maximum downtime. This is the maximum time (in seconds) the subscription was continuously in an error state.
- Message status history. The GOOSE report maintains statistics for several of the most recent error events, including date of event, time of event, duration of event, and event error code.

X. Future Enhancements

DEWA believes in the continuous improvement of their system and is always on the forefront of adopting new technologies to modernize their system and set an example for utilities around the world. Utilizing and maintaining various SCMSs over the period of several years, DEWA recognized the various limitations in different technologies and is collaborating with various vendors to solve the real-world challenges faced by various utilities. Some of the future enhancements that DEWA is looking at are discussed in the following subsections.

A. Software-Defined Networking (SDN)

While working on different stages (specifying, designing, building, testing, and commissioning) of the SCMS project, DEWA learned that networking is a central, often essential, function in the critical infrastructure of today. They also learned that traditional Ethernet-technology based on STA in IT switches is unsuitable for real-time power protection communications because of various limitations like slow failover times, lack of cybersecurity, less or no network visibility, and topology limitations. Therefore, DEWA is looking at SDN, which is revolutionizing the data communications networking world by introducing the concept of programmable networking to enable system managers to react and keep up with the ever-changing demands of today's fully connected world. In addition, this technology brings great advantages to the engineered industrial control system world. SDN is fast finding popularity for the complex systems involved in managing critical infrastructure operations, such as the electric power grid and industrial plant systems. The three distinct advantages that SDN brings to Ethernet-based control systems include dramatically improved packet delivery performance under both normal and fault event conditions, greater cybersecurity without added complexity, and centralized situational awareness with no disruption in change control, enabling seamless scalability. The gap between interoperability and highly reliable communication, a vital requirement for power system applications, is bridged by SDN [8] [9].

B. Color Touchscreen Displays

With the rapid advancement in technology that allows man-to-machine interaction, the future of reliable large color display touchscreens with configurable HMI screens on each device seems very convincing. DEWA is looking at devices that allow smart touch capabilities and provide the user an option to have intuitive and interactive displays for local control.

XI. Conclusion

Building a modern, rugged, and secure SCMS requires diligent attention to all steps of the engineering process as well as rugged hardware with high MTBF to increase the overall system availability. The steps of the engineering process include specifying, designing, building, testing, and consistently verifying integrity. In the present-world scenario, thorough system design for digital substations requires data flow design and service level specifications for each digital message exchange. It also requires as systemic focus on a cybersecurity strategy that incorporates security features in the devices and substation network devices as elements of a more comprehensive security framework. The defense-in-depth security model provides multiple layers of security to protect mission-critical assets and disrupts unwanted actions. Effective and appropriate security requires continuous system monitoring and frequent updates to security policies and procedures. In fact, the security framework is as important, and needs to be as comprehensive, as the SCMS itself. Best-in-class cybersecurity is designed into the protection and control communications networks and not just added at the perimeter. Communications networks are the backbone of the modern day SCMS, and high-performance systems require technical capabilities and not a mere compliance to standards. DEWA has developed a modern

and comprehensive IEC 61850 Edition 2 SCMS design based on proven best engineering practices and well-researched new technologies to achieve interoperability without sacrificing performance.

The DEWA SCMS satisfies each SLA as a commitment between the service provider and the client to satisfy quality, availability, and responsiveness but also continually monitor, report, and react to the integrity of signal exchange processes.

In the end, DEWA has carefully selected from numerous available technologies and designs to create a SCSM system specification proven to accomplish the following:

- Increased system reliability.
- Increased LAN availability.
- Better defense against cyberattacks.
- Improved system operation and understanding.

Although the DEWA SCMS design based on IEC 61850 Edition 2 is sufficient and complete, DEWA is looking forward to adding SDN and large touchscreen device displays.

XII. References

[1] C. Ewing, "Engineering Defense-in-Depth Cybersecurity for the Modern Substation," proceedings of the 12th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2010.

[2] J. Smith, J. Pereyda, and D. Gammel, "Cybersecurity Best Practices for Creating Resilient Control Systems," presented at Resilience Week 2016, Chicago, IL, August 2016.

[3] J. Smith, N. Kipp, D. Gammel, and T. Watkins, "Defense-in-Depth Security for Industrial Control Systems," presented at the EEA Conference, Wellington, New Zealand, June 2016.

[4] M. R. Duff, P. Gupta, D. Prajapati, and A. Langseth, "Utility Implements Communications-Assisted Special Protection and Control Schemes for Distribution Substations," proceedings of the 70th Annual Conference for Protective Relay Engineers, College Station, TX, April 2017.

[5] SEL-3610 Port Server, SEL-3620 Ethernet Security Gateway, and SEL-3622 Security Gateway Instruction Manual. Available: https://selinc.com.

[6] J. M. Herrera, M. S. Mingarro, S. L. Barba, D. Dolezilek, F. Calero, A. Kalra, and B. Waldron, "Case Study of Time-Domain Automation and Communications: Field-Proven Benefits to Automation, Control, Monitoring, and Special Protection Schemes," proceedings of the International Conference and Exhibition – Relay Protection and Automation for Electric Power Systems, Saint Petersburg, Russia, April 2017.

[7] IEC TR 61850-90-4:2013, Communication Networks and Systems for Power Utility Automation – Part 90-4: Network Engineering Guidelines, Technical Report, August 2013. Available: http://webstore.iec.ch/.

[8] M. Hadley, D. Nicol, and R. Smith, "Software-Defined Networking Redefines Performance for Ethernet Control Systems," presented at the Power and Energy Automation Conference, Spokane, WA, March 2017

[9] D. Dolezilek, J. Dearien, A. Kalra, and J. Needs, "Appropriate Testing Reveals New Best-in-Class Topology for Ethernet Networks," presented at the 13th International Conference on Developments in Power System Protection, Edinburgh, United Kingdom, March 2016.

XIII. Further Reading

S. Chelluri, D. Dolezilek, J. Dearien, and A. Kalra, "Understanding and Validating Ethernet Networks for Mission-Critical Protection, Automation, and Control Applications," March 2014. Available: http://selinc.com.

XIV. Biographies

Sultan Al Obaidli is the head of OT Projects & Engineering Management in Dubai Electricity & Water Authority. He has 12 years of experience in electric power automation, communication, control, SCADA, SCMS, SDH network, PABX Telephony, and project management, where both Telecontrol Engineering & Telecommunication Engineering Units are under his supervision and responsibility. He was fully involved in the DEWA SCMS long-term contract from the very beginning of the planning and design phases.

Venkataraman Subramaniam is an OT Specialist in SCADA Engineering at Dubai Electricity & Water Authority. He has more than 20 years of experience in electric power automation, control, SCADA, and SCMS.

Hamood Alhuseini is the head of the OT Telecontrol Engineering Unit at Dubai Electricity & Water Authority. He has 8 years of experience in electric power automation, control, SCADA, and SCMS.

Ramesh Gupta is a Senior Design Engineer within the OT Telecontrol Engineering Unit at Dubai Electricity & Water Authority (DEWA). He has experience in electric power automation, control, SCADA, and SCMS. He was the DEWA design engineer for the SCMS long-term contract.

David Dolezilek is the international technical director at Schweitzer Engineering Laboratories, Inc. and has three decades of experience in electric power protection, automation, communication, and control. He leads a team that develops and implements innovative solutions to intricate power system challenges and teaches numerous topics as adjunct faculty. David is a patented inventor, has authored dozens of technical papers, and continues to research first principles of mission-critical technologies. Through his work, he has created methods to specify, design, and measure service level specifications for digital communication of signals, including class, source, destination, bandwidth, speed, latency, jitter, and acceptable loss. As a result, he helped coin the term operational technology (OT) to explain the difference in performance and security requirements of Ethernet for mission-critical applications versus IT applications. David is a founding member of the DNP3 Technical Committee (IEEE 1815), a founding member of UCA2, and a founding member of both IEC 61850 Technical Committee 57 and IEC 62351 for security. He is a member of the IEEE, the IEEE Reliability Society, and several CIGRE working groups.

Amandeep Kalra is an application engineer II with Schweitzer Engineering Laboratories, Inc. (SEL) in Lynnwood, Washington, with several years of experience in designing automation systems and secure communications networks. He has authored numerous technical papers focusing on IEC 61131-based automation controllers, secure Ethernet networks, cybersecurity, and Ethernet-based communications protocols as well as IEC 61850 communications standards. He is a patented inventor and has represented SEL at various international conferences and IEC 61850 interoperability demonstrations organized by UCA and frequently teaches engineering design and application of IEC 61850 solutions. He has a bachelor of technology degree in instrumentation and control engineering from the National Institute of Technology, India, and a master's degree in electrical engineering from California State University, Northridge.

Prasanth Sankar received his B.Tech degree in Electronics And Instrumentation from the University of Calicut, India, in 2001, and the M.Tech with specialization in Micro-Electro-Mechanical Systems (MEMS) and Biomedical Engineering from the Indian Institute of Technology (IIT), Bombay, India, in 2007. In 2016, he received the Project Management Professional (PMP) certification from the Project Management Institute (PMI), in the United States. He has more than 14 years of experience in substation automation, design, and execution. In 2012, Prasanth joined Schweitzer Engineering Laboratories, Inc. (SEL) Middle East, UAE, as a senior automation engineer. He has been a design manager at SEL in the Middle East, UAE, since 2015. His main areas of interest include substation automation and project management. He holds one patent, Indian Patent No. 263931, for an electronic explosive detector.

20170714 • TP6827-01