A Framework for Developing and Evaluating Utility Substation Cyber Security

by Adam Gauci, P.Eng., Didier Giarratano, and Sandeep Pathania

Executive summary

The utility industry is under pressure to improve substation automation cyber security. Manufacturers of substation products use proprietary or product-specific methodologies for managing device security. As a result, standardization and ease of management of these devices is lacking. This paper reviews processes and procedures for securing a substation, offers advice for overcoming substation asset management challenges, and describes some of the tools available.

998-2095-07-21-14AR0

Schneider Electric

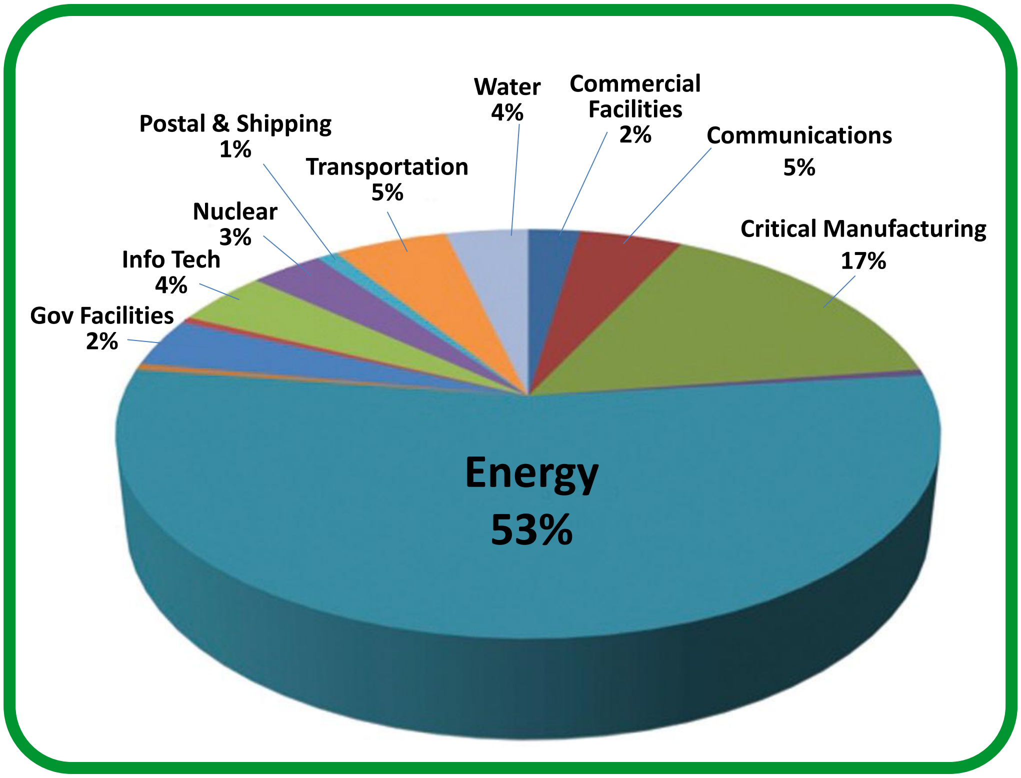
Introduction

Over the past decade, the demand for digitized, connected, and integrated operations has increased across all industries. Compared to the IT Industry, the Energy Industry is late to the connectivity game. The pressing need to improve critical power distribution infrastructure uptime is accelerating the rate of change in this domain. However, as the power networks merge and become "smarter", the benefits of improved connectivity also open the door to more cyber security risks. According to US Department of Homeland Security's Industrial Control Systems Computer Emergency Response Team (ICS-CERT), 53% of cyber security incidents reported and investigated by the agency in the first half of 2013 were related to the energy industry[1] (see **Figure 1**).

Now that cyber security is a top-of-mind concern, utility stakeholders are mimicking their IT peers and are scrambling to put their infrastructure security house in order. Within substations, proprietary devices once considered for specialized applications are now vulnerable. Sensitive information (such as online documentation that describes how these devices work) can be accessed via the internet by anyone, including those with malicious intent who wish to cause disruption.

Figure 1

Number of cyber security incidents and percentage of total by industry in the US (courtesy of US Homeland Security Department)



Electrical substations today are characterized by different mixes of Information Technology (IT) and Operational Technology (OT). Operational Technology is defined as the automation and control systems and components that monitor, measure, and protect critical infrastructure. When bolstering the security of a substation network, IT infrastructure components such as PC hosts, network devices (e.g., switches, routers, and firewalls) are a logical first step for protection. Technologies / tools such as SNMP and SYSLOG can be used with security monitoring systems to easily monitor IT-based devices. Extending this same methodology to OT-based devices, however, can be more difficult to achieve.

[1] US Department of Homeland Security, *ICS-CERT Monitor*, "Incident Response Activity", April/May/June 2013, page 2

Most embedded devices and power systems applications were not designed with security monitoring in mind. To address this problem, many substation automation vendors have tried the bolt-on security approach, keeping cyber security functionally separate from non-secured OT devices and building a layer of security around them. This approach may allow for a layer of access control and monitoring, but once the initial layer is breached, devices remain vulnerable. While bolt-on solutions allow for a fast implementation to reduce the risk of a cyber-attack on OT devices, substation asset managers should consider upgrading their OT devices during their lifecycle to newer devices containing built-in cyber security functions. This paper details the level of security functionality required by OT devices in order to provide robust security monitoring. The processes and organization needed to support an OT security initiative are also described.

Device logging and monitoring

Unique human user names

Most devices found in today's substations contain multiple, fixed access accounts that are shared among several human users. This makes it difficult to determine which particular user has logged a security event. The solution to this problem is to provide a mechanism for eliminating generic and locally shared accounts and to enforce human user-based accounts where any action can be logged with a specific user's account name. Human users can access a multitude of devices inside a substation. Hence user account names should be synchronized across all devices. Rather than centralized authentication, local account synchronization is the preferred method because OT devices should always be accessible in case of emergency. In the event of network infrastructure failure, relying on a centralized server for access is a risky approach.

Unique human user names allows asset security managers to completely audit a user's actions, and to increase user accountability through non-repudiation, meaning that users cannot deny an action that they may or may not have taken. When possible, authentication should also protect front panel functions. This ensures that all critical device actions and configuration changes are recorded as events initiated by human users (see **Figure 2**).

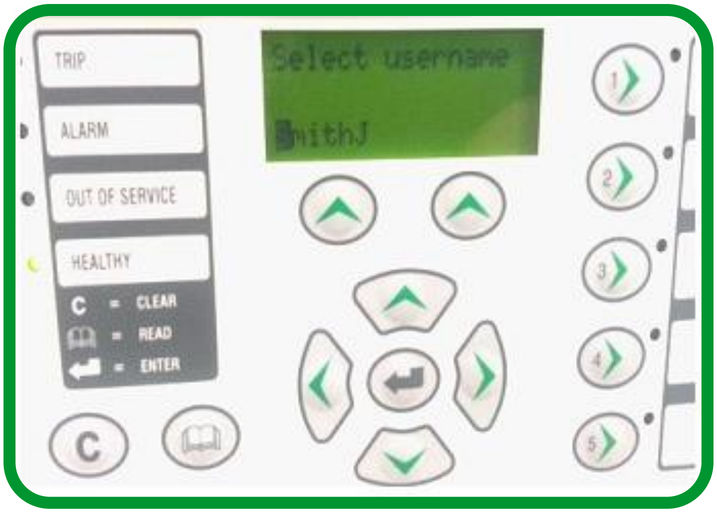


Figure 2
Example of unique user name logon scrolling for local IED device

Security logging

Devices must be able to identify the individuals who are authorized to take an action. Those particular security events that should be recorded must also be defined. In this case, many OT-related standards such as IEEE 1686 and IEC 62443-4-2 should provide guidance (see

Table 1). Internal mechanisms that record security events should be secure. It should not be possible to modify security events. A mechanism should be put into place that allows security administrators to forward security events to a centralized server.

Table 1
Security events as defined in IEEE 1686

Event name	Description
Log In	Successful log in (locally or remotely) of a user to the device.
Manual Log Out	User-initiated log out.
Timed Log Out	Log out of user after a predefined period of inactivity elapses.
Value Forcing	Action of a logged-in user that overrides real data with manual entry and/or causes a control operation.
Configuration Access	Downloading of a configuration file from the IED to an external device or memory location (e.g., computer, memory stick, compact disk).
Configuration Change	The uploading of a new configuration file to the IED or keystroke entry of new configuration parameters that causes a change in IED configuration.
Firmware Change	Writing to memory of new IED operating firmware.
ID/Password Creation or Modification	Creation of new ID/password or modification of ID/password or RBAC levels of authorization.
ID/Password Deletion	Deletion of a user ID/password.
Audit Log Access	User access of audit log for viewing or audit log download to an external device or memory location (e.g., computer, memory stick, compact disk).
Time/Date Change	User request to change time and date.
Unsuccessful Login Attempt	Three incorrect password entries in succession during a single log-in attempt. Successive failed log-in attempts after three will generate a single entry into the audit log trail listed listing the time of the last attempt and total number of log-in attempts that have occurred in succession.
Reboot	The rebooting or restarting of the IED by means of removing power or through the use of a device-resident rebooting mechanism such as a reset button, power-up sequence, or access software feature.
Attempted Use of Unauthorized Configuration Software:	The detection by the IED of an attempted use of configuration software, accessing computer, or a combination thereof which is not registered as legitimately able to be used for configuration of the IED.
Invalid Configuration or Firmware Download	The detection by the IED of a configuration or firmware download to the IED that does not contain the proper credentials that identify the configuration or firmware as valid.
Unauthorized Configuration or Firmware File	The detection by the IED of a configuration or firmware download to the IED that does not contain the proper credentials that identify the configuration or firmware as authorized.
Unexpected Time Signal Out of Tolerance	The IED shall validate time-synchronization messages received through protocol or dedicated time-synchronization channels and alarm if the time-synchronization message is not within the tolerances of the IED's internal/local clock.
Invalid Field Hardware Changes	The IED shall validate user-performable (as identified by the vendor) field hardware changes and alarm if the field hardware change is performed improperly (i.e., wrong I/O board inserted in a designated I/O slot).

SYSLOG is a long-time IT industry standard used with telecommunications and network infrastructure devices. This standard defines a client / server protocol for transmitting logs to a centralized server. In most cases, the perimeter of a substation contains many different types of devices. To provide the most complete audit of a substation perimeter, it is necessary to collect the security logs from as many different devices as possible. SYSLOG makes it possible to collect data from a multitude of OT devices and from any IT device that supports the protocol. Once the data is aggregated and normalized into one complete substation security log, it is much easier to correlate security events generated by multiple devices and to detect potential malicious behavior.

Collected logs can also be transferred to an enterprise-level Security Information and Event Management (SIEM) system. Such a system identifies root causes of security incidents through analytics, provides alerts based on potential malicious activity signatures/patterns, and generates data and statistics that can be used for compliance reporting.

Security Monitoring

Security monitoring can be accomplished using the common IT administrative Simple Network Management Protocol (SNMP). SNMP is used to manage IP-based devices such as switches, routers workstations, and printers via a Network Management System (NMS). Alerts notify a security administrator in real time of any abnormal or failing system components. These alerts can be sent directly as alarms or via e-mail or SMS.

The SNMP approach can also be applied to OT devices. Monitoring data that is available via SNMP can also be used for cyber security monitoring. The data objects that OT devices can provide are based on the Management Information Base (MIB) defined in the IEC 62351-7 standard.

Monitoring data from OT devices can be leveraged at the NMS level in the following ways:

1. **Monitoring of device status:** The NMS can alert the security administrator of any device failures or changes.
2. **Monitoring of device performance and communications:** Monitoring of the device CPU and communications interface can help to alert the security administrator to any potential overload conditions that may help detect many types of attacks, e.g., Denial of Service (DoS) attacks.
3. **Intrusion detection:** Data regarding device status and performance can be correlated inside an Intrusion Detection System (IDS) to help detect changes in condition that could signal a potential system intrusion.
4. **Configuration management:** Portions of the device configuration can be monitored and recorded for unapproved changes. This can make it easier to ensure the configuration is restored after a failure. This gives the administrator the ability to make configuration changes in real time in order to respond to a security event. An example of this is to force the switch of standard redundant communication channels to a backup channel if the main channel has been compromised.

Cyber security compliance

Secure system deployment in secondary control systems should be supported by the organizational and operational processes that manage the critical infrastructures. This is to ensure that all stakeholders (e.g., utility site teams, suppliers, site maintenance and commissioning teams) are well trained and sensitized to those security measures that are in place. In addition, these stakeholders must be made to use and maintain the secured system baseline while performing daily operations.

The security policy model illustrated in **Figure 3** provides a step-by-step approach to implementing basic security concepts such as Availability, Integrity, and Confidentiality (AIC), or Authorization, Authentication and Audit-ability (AAA).

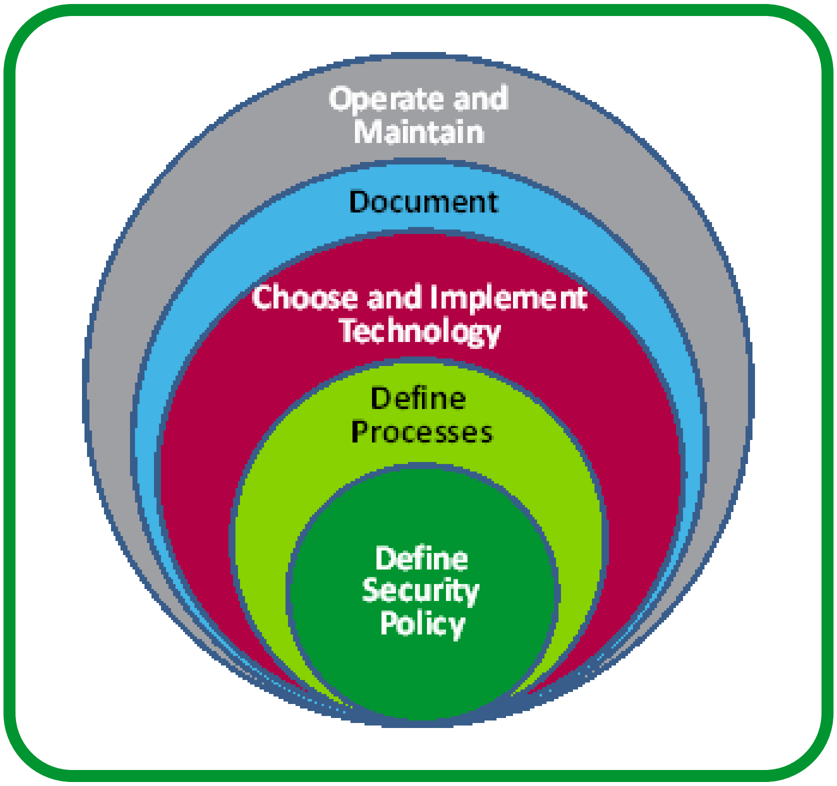


Figure 3
Example of a security policy model

Step 1: Define security policy

The cyber security policy provides a formal set of rules to be followed. The purpose of the policy is to inform employees, contractors, and other authorized users of their obligations regarding protection of technology and information assets. It describes the list of assets that must be protected, identifies threats to those assets, describes authorized users' responsibilities and associated access privileges, and describes unauthorized actions and resulting accountability for the violation of the security policy. The policy should also include the following:

- A list of control system hardware, embedded device CPUs, hard drives, USB, CD drives, front end data and historian servers, associated device drivers, operating systems, historians, backup and restore solutions, anti-malware solutions, emails, and web-server applications.
- A list of control system software: HMI, gateway applications, configuration and maintenance tools, setting and disturbance analysis applications, and engineering software.
- Classification and protection of information.
- Rules to protect sensitive information: For example, lists defining the sensitive information (hard copy or soft copy) being used, and classifying information into distinct categories such as confidential, non-confidential, internal use, and public.
- Classification and protection of control system components, networks, and servers (e.g., whether the device handles sensitive or protected data, handles mission critical services, can be connected to other networks, or can be connected to the internet).

- A risk assessment based on internal and external threats (e.g., hackers, terrorists, disgruntled employees or contractors, unintentional usage).
- Escalation procedure for cyber incidents with the responsible individual identified (i.e., whom to notify during a cyber-incident). This is generally addressed using an incident response plan.
- Incident Response Plan: This defines how an organization prioritizes, acts, responds, and communicates in the event of a cyber security incident. Both internal and external incidents are covered. Examples of incidents include:
    - Breach by gaining unauthorized access, taking unauthorized control, extracting confidential information, or manipulating system data.
    - Unintentional misuse that causes a disruption of the expected system behavior and impacts essential services.
    - Public disclosure of a new vulnerability by vendors or cyber security experts which could impact products or software application components of the system in question.
- CERT (Computer Emergency Response Team): This group of individuals is responsible for organizing, leading, communicating, and resolving cyber security incidents within an organization in a timely manner. This team should include participation from senior management, technical, and quality departments. The major responsibilities of this team include:
    - Assess the incident.
    - Determine validity and root cause.
    - Correct the problem and support the operations teams.
    - Determine how to avoid similar exploitation or vulnerabilities in the future.
    - Communicate effectively with operations teams.
    - Communicate effectively with vendors and corporate or federal CERT bodies.

"The key to maintaining an effective security baseline is to conduct a review once or twice a year".

Step 2: Define processes

As system security baselines keep changing in order to address emerging vulnerabilities, cyber security system processes and procedures need to be reviewed and updated regularly to follow this evolution. The key to maintaining an effective security baseline is to conduct a review once or twice a year. Another important step is to maintain a strong patch management system. The deployment of a patch management system in support of secondary control systems involves the following steps:

- System inventory baseline: Generate a target system inventory list using an automated or manual process to determine which hardware equipment, operating systems, and software applications are used.
- Periodic risk analysis: Monitor security sources for vulnerability announcements and patch and non-patch remediation. Analyze the applicability of the same to targeted system architecture.
- Remediation of risks: Find, download, or acquire remediation from vendors. Prioritize risks and store fixes in a configuration management system for testing and application on system components.
- Testing of patches: Test the patches / fixes in a non-production environment or acquire patches from suppliers that were tested in the intended system configuration to determine whether there is regression in the system functions.
- Schedule a patch implementation cycle depending on the compliance needs or planned system maintenance cycles. Inform the stakeholders of the patch cycle results.
- Secure delivery and deployment of patches to the target system.

- Revise the asset inventory baseline to ensure that no change from the last revision is carried over to the beginning of the next cycle.

Step 3: Choose and implement technology

Choose technology based on international standards to implement security policy and proposed risk mitigation actions. A “Secure by design” approach which is based on international standards like IEC 62351 and IEEE 1686 (as opposed to a “Bolt-on security” approach) can help to further reduce risk when securing control system components. Determine which standards are best suited to implement the cyber security requirements in the operational technology environment and help to enforce and maintain security policy needs in an efficient manner.

Step 4: Document

Cyber security documentation should include detailed procedures, processes, network diagrams, security architectures, and the product and system technical and user documentation supplied by vendors. As-built documentation of deployed system and approved cyber security templates for periodic security audits, security risk assessments, engineering, servicing, commissioning, and patch management should also be included as part of the essential documentation.

Asset management challenges

Cross Functional Expertise

Two options exist for addressing the issue of cyber security implementation in substations. The first option is to train cyber security specialists capable of working in the field. The second option is to manage cyber security from a central location where a pool of experts can handle complex and cross-disciplinary events.

The system complexity is driven by the need for more cross-domain activity where protection engineers, IT managers, security managers, and application engineers are required to share their expertise to identify the potential issues and attacks affecting their systems.

Cyber security constraints are creating a new approach in substation design, commissioning, and operation. The nature of information exchange is evolving and driving the trend toward more robust cyber security. A settings file, for instance, is a potential threat if some of the information can be compromised or changed.

These new constraints are now part of everyday life for utility operations and maintenance teams. The integration of cyber security is also driving dramatic changes in operational and maintenance processes.

Vulnerability Management

When cyber threats were less of an issue, the relationship between a utility and a vendor was based on discussions around bugs that could be found in products or systems. Very often, the utility qualified hardware reliability and tested the software and the algorithms embedded in the product. The qualification of a product characterized, in detail, the behavior of the system / product. The qualified hardware / software were managed cautiously to guarantee the behavior of the overall product.

This strategy is now becoming almost impossible to maintain as far as cyber security is concerned because of a new factor that has entered the picture: vulnerability. A recent example is the “heartbleed” vulnerability discovered recently on a communication stack called OPENSSL. Several releases of this stack were impacted by this vulnerability, leading several companies to release new firmware for their products / systems. As a result, regulators are imposing a requirement to update, within a defined and limited period of time, devices affected by the latest secure instance of firmware, especially when a crypto library is at stake. In this case, it is almost impossible to redo the full qualification processes of the device. The system is sometimes even more complex because direct business relationships exist between the utility and the relay manufacturer. For instance, in some complex ecosystems, contractors, integrators, panel builders, and manufacturers are involved. The problem of asset management is becoming more complex and, in many cases, the utility is left with the challenge of how to address these constraints.

The issue is becoming more critical for utilities because some insurance companies are now refusing to compensate damage caused to a system by a cyber attack if all the known patches have not been properly applied. It has become clear that all equipment, including OT devices, must follow the same rules, and that all the components—including internal device software libraries—must be identified and documented.

Configuration Management

Multiple types of configurations exist. The first type of configuration is specific to a device (such as the number of boards and the configuration of each board). The second type of configuration is related to the functionality of the device. In this second configuration, the settings, the thresholds, and the different logics are all accounted for. While the first type of configuration is generally static and defined during commissioning, the second is more dynamic and can change based on operational conditions or on system changes over time.

"Configuration is dynamic and therefore has a great impact on the security of systems".

Access to the configuration can also be performed in several different ways:

- Via the settings tool of the device, which can be accessed locally or remotely
- Via the front panel of the device, where some parameters can be adjusted
- Via the local Human Machine Interface (HMIs)

These options are well defined when the system aligns to the IEC 61850 standard.

Configuration is dynamic and therefore has a great impact on the security of systems. It is a key tool for restoring the system to a normal operating state after a system component failure. Most of the standards and regulations (like NERC CIP) require the management of configuration data. The management task is quite complex because in each instance the information is different from one device to another and from one manufacturer to another, even if the function is the same. Regardless of which configuration method is used to manage OT equipment, the means to manage device configuration on a regular basis is a key issue and mandatory from the cyber security perspective.

No standard has yet been developed to address the configuration management issue. The primary functions of most OT substation security systems in place today are to store the information in order to retrieve it in case of a security incident, and to provide an alert if a configuration is different and has been changed on the device. While the comparison between two different configurations coming from the same device is quite simple, the comparison of the same function coming from different vendor devices remains almost impossible. This is why standardization efforts are still needed in this area. A common set of ground rules must be established in order to define objects that can be compared so that these objects can be better managed. For example, security log event definitions are not yet defined as a configuration parameter. Therefore a powerful tool is needed to correlate the information coming from the different assets, which, in turn, have been produced by different manufacturers.

Conclusion

Utility vendors should apply standardized cyber security techniques and technologies to substation devices in order to protect critical infrastructure from cyber threats. Logging and monitoring is one area where principles such as unique users and IT protocols like SYSLOG and SNMP are being deployed directly into OT embedded devices (e.g., IEDs, bay controllers, RTUs, etc.).

Cyber security technology only partially addresses the issue of cyber threats. Utilities also need to deploy the proper organization and processes in order to supplement the impact of cyber security protection technologies. As cyber security is an ongoing process, new technologies and security layers need to be developed in order to address gaps exploited by hackers. In the realm of Asset Management, for example, the lack of a standardized approach must be overcome. One potential answer is for utilities and vendors to develop standardized processes together so that concepts such as device configuration can be utilized in a heterogeneous vendor environment.

About the authors

Adam F. Gauci is the Cyber Security Marketing Manager, responsible for product management and critical infrastructure solutions within Schneider Electric's Energy Division. Mr. Gauci is currently a member of the IEEE Power and Energy Society and a registered professional engineer in the province of Ontario, Canada. He holds a Bachelor of Science degree in Computer Engineering from Queen's University at Kingston, Ontario. His previous work experience includes working for Hydro One Networks as a Protection and Control Engineer and Cooper Power Systems as a Field Application Engineer.

Didier Giarratano is the Director of Cyber Security Platforms at Schneider Electric. In this role, he oversees and manages the research and development of cyber security solutions for critical infrastructure. Mr. Giarratano is currently a member of the IEEE Power and Energy Society and a full participating member of the Power Systems Relaying Committee.

Sandeep Kumar Pathania is the Offer Creation Manager within Schneider Electric's Energy Division and is responsible for leading cyber security and IEC61850 projects. He holds a Bachelor in Electronics & Communication Engineering degree from Punjab Technical University, and a Polytechnic Diploma in Electronics Engineering with specialization in microprocessor programming. Mr. Pathania has over 12 years of work experience in energy automation and control systems. His previous work experience includes digital control system project engineering at Alstom T&D India and substation automation at AREVA T&D India. He is a member of the IEEE Power and Energy Society.