Report

Deepti Mishra
Siv Hilde Houmb
Shukun Tokas

Power Grids - Cyber Security Requirements

for SCADA and Substations

Gjøvik 30.08.2021

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Computer Science (IDI)
Gjøvik
ISBN: 978-82-8340-119-6

Picture Credit: Statnett

NTNU
Norwegian University of
Science and Technology

NTNU
Norwegian University of
Science and Technology

Report

Power Grids – Cyber Security Requirements
for SCADA and Substations

VERSION
version number 1.0

AUTHORS
Deepti Mishra
Siv Hilde Houmb
Shukun Tokas

CLIENT(S)
Statnett

CLIENTS REF.
xxxxx xxxxxx xxxxxx xxxxxxxx

DATE
30.08.2021

PROJECT NUMBER
90547200

NUMBER OF PAGES AND ATTACHMENTS
45

CORRESPONDING AUTHOR
Deepti Mishra

CONTROLLED BY
Siv Hilde Houmb

APPROVED BY
Statnett

SIGNATURE
Deepti

SIGNATURE
Siv Hilde Houmb

SIGNATURE

REPORT NUMBER	**ISBN**	**CLASSIFICATION**
xxxxxxxxxx	978-82-8340-119-6	Statnett Public

Background

VERSION	DATE
1.0	30.08.2021

ABSTRACT

The 'Smart Grid' describes a next-generation electrical power system which brings multiple benefits from the increased use of information and communication technology but at the same time escalate security risks. Security experts recommend using standardized solutions to alleviate such security risks. This report aims to explore the cyber security requirements as prescribed in various standards from process, personnel, technical and operational perspectives for selected smart grid components, i.e., SCADA and substation. Another goal is to facilitate Statnett to identify potential gaps by considering cyber security requirements described in this report and the current state of practice. Since the set of requirements relevant for an organization depends on the context and their needs therefore this list should be taken as a recommendation.

Contents

Chapter 1 - Introduction

1.1 Background and motivation

The 'Smart Grid' describes a next-generation electrical power system that is characterized by the increased use of communications and information technology in the generation, delivery, and consumption of electrical energy worldwide (IEEE). Smart grid is composed of several distributed and heterogeneous applications such as advanced metering infrastructure (AMI), automation substation, supervisory control and data acquisition (SCADA), electrical vehicle (EV), and home energy management (HEM), etc.

Smart grid brings in multiple benefits stemming from wide application of information and communication technologies (ICT) that include improved power reliability and quality, self-healing and increased resilience to disruption, predictive and automated maintenance, and increased consumer choice (NIST-1108-R2, 2012). However, the dependence on ICT exposes smart grid to increased security risks. Further, the connection to the public networks adds new security threats. Hence, assuring cybersecurity of the smart grid is indispensable for the reliable operation of this new form of the electricity network (Leszczyna, 2018b).

1.2 Statnett

Statnett is the system operator in the Norwegian energy system and a state enterprise owned by the Norwegian state through the Ministry of Petroleum and Energy (Statnett). Its mission is securing power supply through operations, monitoring and preparedness, facilitating the realisation of Norway's climate objectives, and creation of value for their customers and the society in general. Ensuring cyber security in the Norwegian energy system is among its top business priorities as the modern digitized energy companies are faced with serious cyber risks and attacks.

1.3 Objective

The objective of this report is to explore the cyber security requirements as prescribed in various standards for selected smart grid components, i.e., SCADA and substation. The aim of the study is to facilitate Statnett to identify potential gaps by considering cyber security requirements described in this report and the current state of practice (Tokas, Houmb, & Hugo, 2021). Since security experts agree that standardized solutions and practices should be used in the first place (Leszczyna, 2018a, 2018b; Tipton & Nozaki, 2007; Von Solms, 1999), this study has focused on the available standards and best practices, particularly those that are directly relevant in this context. These standards are used as a basis to identify the cyber security requirements for SCADA and substations.

1.4 Supervisory Control and Data Acquisition (SCADA)

SCADA systems are designed to collect field information, transfer it to a central computer facility, and display the information to the operator graphically or textually, thereby allowing the operator to monitor or control an entire system from a central location in near real time (NIST-SP-800-82, 2011). Based on the sophistication and setup of the individual system, control of any individual system, operation, or task can be automatic, or it can be performed by operator commands (NIST-SP-800-82, 2011). Process control and SCADA systems are making use of, and becoming progressively more reliant on standard ICT technologies and this transformation brings with it the following main concerns:

- These systems were traditionally only designed for the purpose of control and safety and now these once isolated systems are connected to larger open networks which exposes them to threats which these systems never expected to encounter such as worms, viruses and hackers (CPNI, 2008a).
- Previous proprietary process control systems are now replaced with commercial off the shelf software (COTS) and general-purpose hardware. Many of the standard IT security protection measures have not been adopted into the process control environment which keeps the environment insecure (CPNI, 2008a).
- Control systems are connected to other networks that are not secure (Finco, Lee, Miller, Tebbe, & Wells, 2007).
- Insecure connections exacerbate vulnerabilities (Finco et al., 2007).
- Manuals on how to use SCADA systems are publicly available to the actors with malicious intent as well as to legitimate users (Finco et al., 2007).

1.5 Substations

Cyber security in substation automation, protection, and control systems is widely recognized as a critical component in the overall reliability of electricity supply. Modern substation automation, protection, and control systems, while using technology advancements to achieve greater power-system reliability, can be vulnerable to a multitude of cyber security threats with the increasing dependency on communication technology and the growing pressure of a secure utility infrastructure which can lead to overall power-system integrity issues (IEEE-C37.240, 2015). The substation automation, protection, monitoring and control system components (actors) must include security measures such as access control, use control, data integrity and confidentiality, restricted data flow, timely response to events and network resource availability.

1.6 State of the art

Many standards and guidelines for cyber security of smart grids have been proposed in recent years which makes it difficult for smart grid stakeholders to find relevant documents related with their problems. Leszczyna (2018c) conducted a systematic review of existing literature with the aim to identify standards that address the subject of cyber security assessment of smart grids and were used in most of the recent studies.

Table 1: Most commonly used cyber security assessment standards in the scientific studies (Leszczyna, 2018c)

	No. of studies
IEC 62351 Standard	15
ISO/IEC 27000 Standards	11
NERC CIP Regulation	10
IEEE 1686 Standard	9
NISTIR 7628 Guideline	7
IEC 62443 (ISA 99) Standards	7

However, the review did not consider that applicability of available standards to specific components of a smart grid. In another systematic review, Leszczyna (2018b) identified standards that define cyber security requirements for smart grids. Since the scope of this study is to explore the cyber security gaps for selected smart grid components, i.e., SCADA and automation substation, available standards were explored for their applicability to these specific components of smart grids. Table 2 presents the available standards with the focus on SCADA and substation.

Table 2: Standards/guidelines with a focus on SCADA and substation

SCADA	**Substations**
IEC 62443 (2009) • **ISA/IEC 62443-2-1** • ISA/IEC 62443-3-1 • **ISA/IEC 62443-3-2** • **ISA/IEC 62443-3-3**	**IEEE C37.240 (2014)** IEC 62443 (2009) • **ISA/IEC 62443-2-1** • ISA/IEC 62443-3-1 • **ISA/IEC 62443-3-2** • **ISA/IEC 62443-3-3**
NIST SP 800-82 Guide (2015)	IEEE 1408 (2008)
NISTIR 7628 (2014)	**IEEE 1686 (2013)**
CPNI Good Practice Guide for Process and SCADA security (2008)	IEC TC57 (2012)
Cyber Security Procurement Language for Control Systems (2009)	IEC 61850
ISO/IEC 27019 (2017)	IEC 62531

Due to limited time and resources, some of the above-mentioned standards (in bold) are explored to identify cyber security requirements for SCADA and substations. Chapter 3 contains the list of cyber security requirements applicable for selected smart grid components however, this list is not exhaustive and should be looked upon as a recommendation. The set of requirements relevant for an organization depends on the context and their needs therefore the organization should choose these requirements accordingly.

Chapter 2 - Research Methods

This study is comprised of two study actions: (1) determine the current state of practice at Statnett, and (2) determine cyber security requirements for SCADA and substations.

2.1 Current "state of practice"

To determine the current state of practice, the project developed a questionnaire that was distributed and used as the basis for structured interviews with relevant personnel from Statnett. Further details on this study activity is provided in report 2 (Tokas et al., 2021).

2.2 Cyber security requirements for SCADA and substations

Organizations are dealing with the crucial issue of cyber security of various inter-connected systems in a smart grid. An important step towards ensuring this is to have a well-established cyber security management system (CSMS) (IEC62443-2-1, 2010). People, processes and technology are 3 key pillars of Information Security Management System (ISMS) (ISO/IEC27001, 2013) and the core basis of a layered approach to cyber security. In this report, we use the term operational rather than processes to cover aspects that are not necessary strictly process. Hence a well-established CSMS includes cyber security requirements from process, personnel, technical and operational perspectives. Considering these perspectives, standards and guidelines (given in Table 2) are explored to identify cyber security requirements with respect to SCADA and substations. Some of the requirements listed may be relevant to more than one category. In these cases, we only list the requirement once, and in the category considered as the most relevant.

The summary of these requirements is given in the next chapter.

Chapter 3 - An overview of security requirements for SCADA and Substations

3.1 Organizational and Process requirements

Cyber Security Management and Governance

An organization shall establish a Cyber Security Management System (CSMS) that covers the following three elements: (1) Risk analysis, (2) Addressing risk with the CSMS, and (3) Monitoring and improving the CSMS (IEC62443-2-1, 2010).

- The organization shall develop a formal written scope for the cyber security program (IEC62443-2-1, 2010).
- The scope should explain the strategic goals, process, and timing for the CSMS (IEC62443-2-1, 2010).
- The organization shall obtain senior management support for a cyber security program (IEC62443-2-1, 2010).
- Organizational responsibilities shall be clearly defined for cyber security and related physical security activities (IEC62443-2-1, 2010). There shall be an organization, structure or network of stakeholders established (or chosen) under management leadership, with the responsibility to provide clear direction and oversight for the cyber aspects of the IACS (IEC62443-2-1, 2010). The core team of stakeholders should be cross-functional in nature to bring together the skills necessary to address security in all parts of the IACS (IEC62443-2-1, 2010). Their responsibilities and tasks include:
    - Understanding the business risks by considering technologies involved, threats, critical assets, existing exposure, regulations and legislations (CPNI, 2008e).
    - Developing & updating policies and standards (CPNI, 2008e).
    - Ensuring compliance with policies and standards (CPNI, 2008e).
    - Implementing secure architecture by ensuring practical application of policies and standards (CPNI, 2008e).
    - Establishing Process Control Security Response Team (PCSRT) either as a coordination centre or local site that run entities or a combination of both (CPNI, 2008e).
    - Improving awareness and skills by organizing awareness and training (CPNI, 2008e).
    - Managing third party risks by ensuring education and auditing of 3rd parties (CPNI, 2008e).
    - Ensuring criticality classification and prioritization (CPNI, 2008e).
- The organization establishes and maintains contact with security groups and associations to stay up to date with the latest recommended security practices, techniques, and technologies and to share current security-related information including threats, vulnerabilities, and incidents (NISTIR-7628-Vol1, 2014).

Risk Management and Assessment

- The organization should develop a high-level business rationale, as a basis for its effort to manage IACS cyber security, which addresses the unique dependence of the organization on IACS (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- The organization develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, and other organizations associated with the operation and use of information systems and implements that strategy consistently across the organization (NISTIR-7628-Vol1, 2014).

- The organization develops, implements, reviews, and updates on an organization-defined frequency (NISTIR-7628-Vol1, 2014):
  - A documented risk assessment security policy that addresses the objectives, roles, and responsibilities for the risk assessment security program as it relates to protecting the organization's personnel and assets; and the scope of the risk assessment security program as it applies to all of the organizational staff, contractors, and third parties; and
  - Procedures to address the implementation of the risk assessment security policy and associated risk assessment protection requirements.
- Management commitment ensures compliance with the organization's security policy and other regulatory requirements (NISTIR-7628-Vol1, 2014).
- The organization ensures that the risk assessment policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations (NISTIR-7628-Vol1, 2014).
- The organization conducts assessments of risk from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and smart grid information systems and updates risk assessments on an organization-defined frequency or whenever significant changes occur to the smart grid information system or environment of operation, or other conditions that may impact the security of the smart grid information system (NISTIR-7628-Vol1, 2014).
- The organization develops a risk management plan which should be reviewed and approved by a management authority, risk-reduction mitigation measures are planned and implemented and the results monitored to ensure effectiveness of the organization's risk management plan (NISTIR-7628-Vol1, 2014).
- The organization (NISTIR-7628-Vol1, 2014):
  - Monitors and evaluates the smart grid information system according to the risk management plan on an organization-defined frequency to identify vulnerabilities that might affect the security of a smart grid information system;
  - Analyzes vulnerability scan reports and remediates vulnerabilities within an organization-defined time frame based on an assessment of risk;
  - Shares information obtained from the vulnerability scanning process with designated personnel throughout the organization to help eliminate similar vulnerabilities in other smart grid information systems;
  - Updates the smart grid information system to address any identified vulnerabilities in accordance with organization's smart grid information system maintenance policy; and
  - Updates the list of smart grid information system vulnerabilities on an organization-defined frequency or when new vulnerabilities are identified and reported.
- The organization shall select a particular risk assessment and analysis approach and methodology that identifies and prioritizes risks based upon security threats, vulnerabilities and consequences related to their IACS assets (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- The organization should provide participants in the risk assessment activity with appropriate information including methodology training, before beginning to identify the risks (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- A high-level system risk assessment shall be performed to understand the financial and HSE consequences in the event that availability, integrity or confidentiality of the IACS is compromised (IEC62443-2-1, 2010; IEC62443-3-2, 2020). Create organization level inventory. Assess each asset at enterprise level to determine priority order of sites security gap mitigation (site risk table) (CPNI, 2008a).

- The organization's risk assessment methodology shall include methods for prioritizing detailed vulnerabilities identified in the detailed vulnerability assessment (IEC62443-2-1, 2010; IEC62443-3-2, 2020). The organization shall develop the criteria and assign a priority rating for mitigating the risk of each logical control system (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- The organization shall identify the various Industrial Automation and Control Systems (IACS), gather data about the devices to characterize the nature of the security risk and group the devices into logical systems (IEC62443-2-1, 2010; IEC62443-3-2, 2020). For an ICS, a very important aspect of the risk assessment is to determine the value of the data that is flowing from the control network to the corporate network. In instances where pricing decisions are determined from this data, the data could have a very high value. The fiscal justification for mitigation has to be derived by comparing the mitigation cost to the effects of the consequence (NIST-SP-800-82-R2, 2015) (NIST-SP-800-82-R2, 2015) . Review all system elements e.g. servers, workstations, network infrastructure etc. to determine vulnerabilities such as connections to other systems, remote access, access control, third party code, system resilience and continuity etc. (CPNI, 2008a)**.** A well-thought-out security implementation is a balance of risk versus cost. In some situations, the risk may be safety, health, or environment-related rather than purely economic. The risk may result in an unrecoverable consequence rather than a temporary financial setback (NIST-SP-800-82-R2, 2015) .
- The results of physical, HSE and cyber security risk assessments shall be integrated to understand the assets' overall risk (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- The risk assessment methodology and the results of the risk assessment shall be documented (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- The organization shall conduct a detailed risk assessment incorporating the vulnerabilities identified in the detailed vulnerability assessment (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- The organization shall identify the risk and vulnerability reassessment frequency as well as any reassessment triggering criteria based on technology, organization, or industrial operation changes (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- The organization shall perform a cyber security risk assessment of the SUC (System Under Consideration) or confirm a previous initial cyber security risk assessment is still applicable in order to identify the worst case unmitigated cyber security risk that could result from the interference with, breach or disruption of, or disablement of mission critical IACS operations (IEC62443-2-1, 2010; IEC62443-3-2, 2020). Create site level inventory. Assess each site assets to determine priority order of assets security mitigation (CPNI, 2008a).
- For each project with implications on process control systems, appoint security architect as a single point of accountability for security risk management for the full life cycle of the project (CPNI, 2008f).

Supply Chain Risk assessment

- There is a need to develop policies and procedures for acquisition of resources required to adequately protect an information system. These acquisitions are based on security requirements and security specifications (NIST-SP-800-82-R2, 2015; NISTIR-7628-Vol1, 2014).
- Ensure external suppliers and contractors that have an impact on the security of smart grid information systems meet the organization's policy and procedures to maintain the overall level of ICS security. Security policies and procedures of second and third-tier suppliers should also be in compliance with corporate cyber security policies and procedures in the case that they impact ICS security (NIST-SP-800-82-R2, 2015) (NISTIR-7628-Vol1, 2014).

- The security requirements of an organization outsourcing the management and control of all or some of its information systems, networks, and desktop environments should be addressed in a contract agreed between the parties (NIST-SP-800-82-R2, 2015; NISTIR-7628-Vol1, 2014).
- Establish procedures to remove external supplier and contractor access to smart grid information systems at the conclusion/termination of the contract (NISTIR-7628-Vol1, 2014).
- Build process control security requirements into preferred vendor selection and accreditation (CPNI, 2008e).
- For each item in the inventory, determine associated third parties and perform review (CPNI, 2008e).
- Manage risks from vendors, sub-contractors, support organizations and in the supply chain by (CPNI, 2008e):
    - Ensuring security clauses are included in the contract.
    - Continuously engage with vendors so that any vulnerabilities will be notified promptly within the supplied systems.
    - Requesting vendors to provide security guidance for their control systems.
    - Establishing an effective software patching process with vendors.
    - Engage vendors to provide guidance on hardening the systems.
    - Manage risk of remote support by vendors.
    - Establishing their response capabilities.
    - Undertake regular security reviews and audits of all vendors.
- There is a need for critical operational/security updates from vendors to update firmware and/or software, retrieve maintenance information and retrieve event logs (NISTIR-7628-Vol1, 2014).

Security and Authorization Policy and Procedures

- The organization develops, implements, reviews, and updates on an organization-defined frequency (NISTIR-7628-Vol1, 2014):
    - A documented security and authorization policy that addresses the objectives, roles, and responsibilities for the security and authorization security program as it relates to protecting the organization's personnel and assets, and the scope of the security and authorization security program as it applies to all of the organizational staff and third-party contractors; and
    - Procedures to address the implementation of the security and authorization policy and associated security and authorization protection requirements.
- The organization shall develop high-level cyber security policies for the IACS environment which are approved by management (IEC62443-2-1, 2010). Management commitment ensures compliance with the organization's security and authorization security policy and other regulatory requirements (NISTIR-7628-Vol1, 2014) and applicable federal, state, local, tribal, and territorial laws and regulations (NISTIR-7628-Vol1, 2014).
- The organization shall develop and approve cyber security procedures, based on the cyber security policies and provide guidance in how to meet the policies (IEC62443-2-1, 2010).
- Cyber security policies and procedures that deal with IACS risks should be consistent with or extensions of policies created by other risk management systems (IEC62443-2-1, 2010).
- Cyber security policies and procedures, for the IACS environment, shall include compliance requirements (IEC62443-2-1, 2010).
- The organization shall determine and document its risk tolerance as a basis for creation of policy and risk management activities (IEC62443-2-1, 2010).

- Cyber security policies and procedures, for the IACS environment, shall be communicated to all appropriate personnel (IEC62443-2-1, 2010).
- The cyber security policies and procedures shall be reviewed regularly, validated to confirm that they are up-to-date and being followed and updated as required to ensure that they remain appropriate (IEC62443-2-1, 2010).
- Management commitment ensures compliance with the organization's security policy and other regulatory requirements (NISTIR-7628-Vol1, 2014). Senior leadership shall demonstrate commitment to cyber security by endorsing the cyber security policies (IEC62443-2-1, 2010).

Security Awareness and Training Policy and Procedures

- The organization develops, implements, reviews, and updates on an organization-defined frequency (NIST-SP-800-82-R2, 2015; NISTIR-7628-Vol1, 2014):
    - A documented awareness and training security policy that addresses the objectives, roles, and responsibilities for the awareness and training security program as it relates to protecting the organization's personnel and assets, and the scope of the awareness and training security program as it applies to all of the organizational staff, contractors, and third parties.
    - Procedures to address the implementation of the awareness and training security policy and associated awareness and training protection requirements.
- Management commitment ensures compliance with the organization's security policy and other regulatory requirements (NIST-SP-800-82-R2, 2015; NISTIR-7628-Vol1, 2014) .
- The organization ensures that the awareness and training security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations (NIST-SP-800-82-R2, 2015; NISTIR-7628-Vol1, 2014).

Access Control Policy and Procedures

- The organization develops, implements, reviews, and updates on an organization-defined frequency:
    - A documented access control security policy that addresses the objectives, roles, and responsibilities for the access control security program as it relates to protecting the organization's personnel and assets and the scope of the access control security program as it applies to all of the organizational staff, contractors, and third parties (NISTIR-7628-Vol1, 2014). Rules that define the privileges authorized under access account for personnel in various job roles shall be defined in an authorization security policy that is clearly documented and applies to all personnel upon authentication (IEC62443-2-1, 2010).
    - Procedures to address the implementation of the access control security policy and associated access control protection requirements (NISTIR-7628-Vol1, 2014).
- Management commitment ensures compliance with the organization's security policy and other regulatory requirements (NISTIR-7628-Vol1, 2014); and
- The organization ensures that the access control security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations (NISTIR-7628-Vol1, 2014).
- The security controls within Access Control (AC) family provide policies and procedures for managing information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. Controls cover access and flow enforcement issues such as separation of duties, least privilege, unsuccessful login attempts, system use notification, previous logon notification, concurrent session control, session lock, and session termination (NIST-SP-800-82-R2, 2015).

Remote Access Policy and Procedures

- Access control policy and procedures includes controls to address the use of portable and remote devices and personally owned information systems to access the information system as well as the use of remote access capabilities and the implementation of wireless technologies (NIST-SP-800-82-R2, 2015). The organization documents allowed methods of remote access to the smart grid information system and establishes usage restrictions and implementation guidance for each allowed remote access method. It authorizes remote access prior to connection and enforces requirements for remote connections to the smart grid information system (NISTIR-7628-Vol1, 2014).
- The organization establishes terms and conditions for authorized individuals to access the smart grid information system from an external information system and process, store, and transmit organization-controlled information using an external information system (NISTIR-7628-Vol1, 2014).
- The organization documents allowed methods of remote access to the smart grid information system and establishes usage restrictions and implementation guidance for each allowed remote access method. It authorizes remote access prior to connection and enforces requirements for remote connections to the smart grid information system (NISTIR-7628-Vol1, 2014).
- The organization establishes use restrictions and implementation guidance for wireless technologies and authorizes, monitors, and manages wireless access to the smart grid information system (NISTIR-7628-Vol1, 2014).
- Supplemental guidance on: remote electronic authentication, wireless network security with particular emphasis on the IEEE 802.11b and Bluetooth standards 0, IEEE 802.11i wireless network security, requirements for the personal identity verification of federal employees and contractors (found in FIPS 201), PIV card to reader interoperability, interfaces for personal identity verification, biometrics for personal identity verification, and cryptographic algorithms and key sizes for personal identity verification, can be found in specific NIST-SP 800-XX documents (NIST-SP-800-82-R2, 2015).

Continuity of Operations Policy, Procedures and Plan

Contingency plans are designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster (NIST-SP-800-82-R2, 2015).

- The organization develops, implements, reviews, and updates on an organization-defined frequency (NISTIR-7628-Vol1, 2014):
    - A documented continuity of operations security policy that addresses the objectives, roles, and responsibilities for the continuity of operations security program as it relates to protecting the organization’s personnel and assets and the scope of the continuity of operations security program as it applies to all of the organizational staff, contractors, and third parties; and
    - Procedures to address the implementation of the continuity of operations security policy and associated continuity of operations protection requirements.
- Management commitment ensures compliance with the organization’s security policy and other regulatory requirements (NISTIR-7628-Vol1, 2014).
- The organization ensures that the continuity of operations security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations (NISTIR-7628-Vol1, 2014).
- Prior to creating a business continuity plan, the organization shall specify recovery objectives for the systems involved based on business needs. Continuity plans shall be

developed and implemented to ensure that business processes can be restored in accordance with recovery objectives (IEC62443-2-1, 2010).

- The organization develops and implements a continuity of operations plan dealing with the overall issue of maintaining or reestablishing operations in case of an undesirable interruption for a smart grid information system (NISTIR-7628-Vol1, 2014). It includes:
    - Business continuity plan to addresses the overall issue of maintaining or reestablishing production in the case of an interruption due to natural disaster, equipment failure, intentional/unintentional man-made events (NIST-SP-800-82-R2, 2015).
    - A disaster recovery plan (DRP) to recover and protect an IT infrastructure in the event of a disaster. It should include components, such as (NIST-SP-800-82-R2, 2015):
        - Required response to events or conditions of varying duration and severity that would activate the recovery plan.
        - Procedures for operating the ICS in manual mode with all external electronic connections severed until secure conditions can be restored.
        - Roles and responsibilities of responders.
        - Processes and procedures for the backup and secure storage of information.
        - Personnel list for authorized physical and cyber access to the ICS.
- The security controls that fall within the (NIST SP 800-53) Contingency Planning family provide policies and procedures to implement a contingency plan by specifying roles and responsibilities, and assigning personnel and activities associated with restoring the information system after a disruption or failure. Along with planning, controls also exist for contingency training, testing, and plan update, and for backup information processing and storage sites (NIST-SP-800-82-R2, 2015) .
- A business continuity team should be formed including IACS and other process owners. In the event of a significant disruption, this team should determine the priority of critical business and IACS systems to re-establish operations (IEC62443-2-1, 2010).
- The organization should determine the impact to each system due to a significant disruption and the consequences associated with loss of one or more of the systems (IEC62443-2-1, 2010).
- It should cover the full range of failures or problems that could be caused by cyber incidents (NIST-SP-800-82-R2, 2015) .
- It should also include procedures for restoring systems from known valid backups, isolating systems from all non-essential interferences and connections that could permit cyber security intrusions, and alternatives to achieve necessary interfaces and coordination (NIST-SP-800-82-R2, 2015) .
- The organization provides the capability to recover and reconstitute the smart grid information system to a known secure state after a disruption, compromise, or failure (NISTIR-7628-Vol1, 2014). The organization shall create backup and restore procedures that support the business continuity plan (IEC62443-2-1, 2010).
- The organization identifies an **alternate control center**, necessary telecommunications, and initiates any necessary agreements to permit the resumption of smart grid information system operations for critical functions within an organization-prescribed time period when the primary control center is unavailable (NISTIR-7628-Vol1, 2014).
- The organization identifies **alternate telecommunication services** for the smart grid information system and initiates necessary agreements to permit the resumption of operations for the safe operation of the smart grid information system within an organization-defined time period when the primary smart grid information system capabilities are unavailable (NISTIR-7628-Vol1, 2014).

- The business continuity plan shall define and communicate the specific roles and responsibilities for each part of the plan, (IEC62443-2-1, 2010) assigned individuals with contact information, and activities associated with restoring smart grid information system operations after a disruption or failure (NISTIR-7628-Vol1, 2014). Employees should be trained and familiarized with contingency plans (NIST-SP-800-82-R2, 2015) .
- Continuity and response plan to monitor, analyse and response to alerts and incidents must be regularly maintained, rehearsed and tested (CPNI, 2008c).
- A management authority reviews and approves the continuity of operations plan (NISTIR-7628-Vol1, 2014). Contingency plans should be periodically reviewed with employees responsible for restoration of the ICS, and tested to ensure continuity (NIST-SP-800-82-R2, 2015) . The business continuity plan shall be tested on a regular basis and updated as necessary (IEC62443-2-1, 2010). Plans should be reviewed at least annually, more frequently for critical or high-risk systems and modified following any changes to the security requirements (CPNI, 2008c).
- The organization tests and reviews the continuity of operations plan to determine its effectiveness for the smart grid information system on an organization-defined frequency using defined tests and results are documented. A management authority reviews the documented test results and initiates corrective actions, if necessary (NISTIR-7628-Vol1, 2014).

Incident Response Policy and Procedures

It is a documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of incidents against the information systems (NIST-SP-800-82-R2, 2015) .

- The organization develops, implements, reviews, and updates on an organization-defined frequency (NISTIR-7628-Vol1, 2014):
  - A documented incident response security policy that addresses:
    - The objectives, roles, and responsibilities for the incident response security program as it relates to protecting the organization's personnel and assets.
    - The scope of the incident response security program as it applies to all of the organizational staff, contractors, and third parties.
  - Procedures to address the implementation of the incident response security policy and associated incident response protection requirements (NISTIR-7628-Vol1, 2014).
- Management commitment ensures compliance with the organization's security policy and other regulatory requirements (NISTIR-7628-Vol1, 2014).
- The organization ensures that the incident response security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations (NISTIR-7628-Vol1, 2014).
- First a response should be measured against the "service being provided," not just the system that was compromised. A quick risk assessment should be performed, in case if an incident is discovered, to evaluate the effect of both the attack and the options to respond (NIST-SP-800-82-R2, 2015) .
- It is always possible that an ICS is compromised by an intentional or unintentional incident. Symptoms of an incident could include: unusually heavy network traffic or high CPU usage, locked out accounts, cleared log files, unexpected changes in configuration settings, etc. (NIST-SP-800-82-R2, 2015).
- To minimize the effects of these intrusions, it is necessary to plan a response, which might include the following:

    - Incident classification. Identification and classification of ICS incidents (to potential impact) so that a proper response can be formulated for each potential incident (NIST-SP-800-82-R2, 2015). The organization identifies potential interruptions and classifies them as to "cause," "effects," and "likelihood" (NISTIR-7628-Vol1, 2014).
    - Response actions. Depending on the type of incident and its effect on the ICS system and the physical process being controlled, response is taken. A written plan documenting the types of incidents and the response to each type should be prepared. This will provide guidance during times when there might be confusion or stress due to the incident. For reporting requirements, it should be noted where the report should be made and phone numbers to reduce reporting confusion (NIST-SP-800-82-R2, 2015).
    - Recovery actions. Risk analysis should be conducted to determine the sensitivity of the physical system being controlled to failure modes in the ICS. Step-by-step recovery actions should be documented, in each case, so that the system can be returned to normal operations as quickly and safely as possible. Recovery actions for an intrusion that affects operation of the ICS will closely align with the system's Disaster Recovery Plan, and should take into account the planning and coordination already established (NIST-SP-800-82-R2, 2015).

Information and Document Management Policy and Procedures

- The organization develops, implements, reviews, and updates on an organization-defined frequency (NISTIR-7628-Vol1, 2014):
    - A smart grid information and document management policy that addresses:
        - The objectives, roles and responsibilities for the information and document management security program as it relates to protecting the organization's personnel and assets.
        - The scope of the information and document management security program as it applies to all the organizational staff, contractors, and third parties.
        - The retrieval of written and electronic records, equipment, and other media for the smart grid information system.
        - The destruction of written and electronic records, equipment, and other media for the smart grid information system.
    - Procedures to address the implementation of the information and document management security policy and associated smart grid information system information and document management protection requirements.
- Management commitment ensures compliance of the organization's security policy and other regulatory requirements (NISTIR-7628-Vol1, 2014).
- The organization develops and reviews the policies and procedures detailing the handling of information on an organization-defined frequency (NISTIR-7628-Vol1, 2014). The organization ensures that the smart grid information system information and document management policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations (NISTIR-7628-Vol1, 2014).
- Agreements are established for the exchange of information, firmware, and software between the organization and external parties such as third parties, vendors and contractors (NISTIR-7628-Vol1, 2014).
- The smart grid information system automatically labels information in storage, in process, and in transmission in accordance with (NISTIR-7628-Vol1, 2014):
    - Access control requirements.
    - Special dissemination, handling, or distribution instructions.

    - Otherwise as required by the smart grid information system security policy.

Configuration Management Policy and Procedures

Configuration management policy and procedures are used to control modifications to hardware, firmware, software, and documentation to ensure that the information system is protected against improper modifications prior to, during, and after system implementation (NIST-SP-800-82-R2, 2015).

- The organization develops, implements, reviews, and updates on an organization-defined frequency (NISTIR-7628-Vol1, 2014):
    - A documented configuration management security policy that addresses the objectives, roles, and responsibilities for the configuration management security program as it relates to protecting the organization's personnel and assets, and the scope of the configuration management security program as it applies to all of the organizational staff, contractors, and third parties.
    - Procedures to address the implementation of the configuration management security policy and associated configuration management protection requirements.
- The organization ensures that the configuration management security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations (NISTIR-7628-Vol1, 2014).
- These security controls provide policy and procedures for establishing baseline controls for maintaining, monitoring, and documenting configuration control changes (NIST-SP-800-82-R2, 2015) . The organization develops, documents, and maintains a current baseline configuration of the smart grid information system and an inventory of the smart grid information system's constituent components. The organization reviews and updates the baseline configuration as an integral part of smart grid information system component installations (NISTIR-7628-Vol1, 2014).
- A formal change management program should be established and procedures used to insure that all modifications to an ICS network meet the same security requirements as the original components identified in the asset evaluation and the associated risk assessment and mitigation plans (NIST-SP-800-82-R2, 2015) . The organization:
    - Establishes configuration settings for components within the smart grid information system (NISTIR-7628-Vol1, 2014). The current ICS network configuration and device configurations must always be known and documented (NIST-SP-800-82-R2, 2015).
    - Access to configuration settings and security settings of IT products should be restricted and should be set to the most restrictive mode consistent with ICS operational requirements (NIST-SP-800-82-R2, 2015).
    - Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures (NISTIR-7628-Vol1, 2014). Risk assessment should be performed on all configuration changes to the ICS network that could affect security, including the addition of network components, and installation of software (NIST-SP-800-82-R2, 2015).
    - Documents changed configuration settings (NISTIR-7628-Vol1, 2014).
    - Identifies, documents, and approves exceptions from the configuration settings; and Enforces the configuration settings in all components of the smart grid information system (NISTIR-7628-Vol1, 2014).
    - Changes to policies and procedures may also be required (NIST-SP-800-82-R2, 2015).

Inventory management

- The organization develops, documents, and maintains an inventory of the components of the smart grid information system that (NISTIR-7628-Vol1, 2014):
  - Accurately reflects the current smart grid information system configuration.
  - Provides the proper level of granularity deemed necessary for tracking and reporting and for effective property accountability.
  - Identifies the roles responsible for component inventory.
  - Updates the inventory of system components as an integral part of component installations, system updates, and removals.
  - Ensures that the location (logical and physical) of each component is included within the smart grid information system boundary.
- The organization implements policy and procedures to address the addition, removal, and disposal of all smart grid information system equipment and all smart grid information system components and information are documented, identified, and tracked so that their location and function are known (NISTIR-7628-Vol1, 2014).

Smart Grid Information System Maintenance Policy and Procedures

- The organization develops, implements, reviews, and updates on an organization-defined frequency (NISTIR-7628-Vol1, 2014):
  - A documented smart grid information system maintenance security policy that addresses the objectives, roles, and responsibilities for the smart grid information system maintenance security program as it relates to protecting the organization's personnel and assets and the scope of the smart grid information system maintenance security program as it applies to all of the organizational staff, contractors, and third parties.
  - Procedures to address the implementation of the smart grid information system maintenance security policy and associated smart grid information system maintenance protection requirements.
- Management commitment ensures compliance with the organization's security policy and other regulatory requirements (NISTIR-7628-Vol1, 2014).
- The organization ensures that the smart grid information system maintenance security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations (NISTIR-7628-Vol1, 2014).

Remote Maintenance

- The organization policy and procedures for remote maintenance include (NISTIR-7628-Vol1, 2014):
  - Authorization and monitoring the use of remote maintenance and diagnostic activities.
  - Use of remote maintenance and diagnostic tools.
  - Maintenance records for remote maintenance and diagnostic activities.
  - Termination of all remote maintenance sessions.
  - Management of authorization credentials used during remote maintenance.

Legacy Smart Grid Information System Upgrades

- The organization develops policies and procedures to upgrade existing legacy smart grid information systems to include security mitigating measures commensurate with the organization's risk tolerance and the risk to the smart grid information system (NISTIR-7628-Vol1, 2014) .

Audit and Accountability Policy and Procedures

Audit and accountability control family provide policies and procedures for generating audit records, their content, capacity, and retention requirements (NIST-SP-800-82-R2, 2015) . The controls provide safeguards to react to problems such as an audit failure or audit log capacity being reached. Audit data should be protected from modification and be designed with non-repudiation capability (NIST-SP-800-82-R2, 2015).

- The organization develops, implements, reviews, and updates on an organization-defined frequency (NISTIR-7628-Vol1, 2014):
    - A documented audit and accountability security policy that addresses the objectives, roles, and responsibilities for the audit and accountability security program as it relates to protecting the organization's personnel and assets, and the scope of the audit and accountability security program as it applies to all of the organizational staff, contractors, and third parties.
    - Procedures to address the implementation of the audit and accountability security policy and associated audit and accountability protection requirements.
- Management commitment ensures compliance with the organization's security policy and other regulatory requirements (NISTIR-7628-Vol1, 2014).
- The organization ensures that the audit and accountability security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations (NISTIR-7628-Vol1, 2014).
- Supplement guidance on: computer security incident handling and audit log retention, log management, and information security governance and planning, given in specific NIST SP 800-XX documents (NIST-SP-800-82-R2, 2015).
- Periodic audits of the ICS should be performed to validate (NIST-SP-800-82-R2, 2015):
    - The security controls present during system validation testing (e.g., factory acceptance testing and site acceptance testing) are still installed and operating correctly in the production system.
    - The production system is free from security compromises and provides information on the nature and extent of compromises as feasible, should they occur.
    - The management of change program is being rigorously followed with an audit trail of reviews and approvals for all changes.
- Periodic audit results should be expressed in the form of performance against a set of predefined and appropriate metrics to display security performance and security trends. Security performance metrics should be sent to the appropriate stakeholders, along with a view of security performance trends (NIST-SP-800-82-R2, 2015).
- Many of the (legacy) process control devices that are integrated into the ICS have do not have the capability to provide the audit records. Therefore, the applicability of these more modern tools for auditing system and network activity is dependent upon the capabilities of the components in the ICS (NIST-SP-800-82-R2, 2015).

3.2 Personnel requirements

Personnel security

The security controls that fall within personnel security family provide policies and procedures to reduce the risk of human error, theft, fraud, or other intentional or unintentional misuse of informational assets (NIST-SP-800-82-R2, 2015).

- Main aspects of personnel security (NIST-SP-800-82-R2, 2015):
    - Hiring policies. This includes pre-employment screening such as background checks, the interview process, employment terms and conditions, complete job descriptions and detailing of duties, terms and condition of employment, and legal rights and responsibilities of employees or contractors. In particular, personnel should be screened for the critical positions controlling and maintaining the ICS.
    - Organization policies and practices. Organization policies to be enforced should be documented and readily available to all workers through an employee handbook, distributed as email notices, located in a centralized resource area, or posted directly at a worker's area of responsibility. Such policies include security policies, information classification, document and media maintenance and handling policies, user training, acceptable usage policies for organization assets, periodic employee performance reviews, appropriate background checks, and any other policies and actions that detail expected and required behavior of organization employees, contractors, and visitors.
    - Terms and conditions of employment. This includes job and position responsibilities, notification to employees of terminable offenses, disciplinary actions and punishments, and periodic employee performance reviews.
- There shall be a personnel security policy established, clearly stating the organization's commitment to security and the security responsibilities of personnel. Personnel include employees, prospective employees, contract employees, and third-party contractors (IEC62443-2-1, 2010).
- Unless government regulation prohibits it, all personnel with access to the IACS (both physical and cyber), including new hires and internal transfers to sensitive positions shall be screened, including validation of their identity and background checks, during the job application process (IEC62443-2-1, 2010).
- Personnel should also be subject to ongoing scrutiny for changes that might indicate a conflict of interest or concern for performing the job in an appropriate manner (IEC62443-2-1, 2010).
- The personnel security policy should address security responsibilities from recruitment through the end of employment, especially for sensitive positions (IEC62443-2-1, 2010).
- Security expectations and responsibilities shall be clearly documented and regularly communicated to personnel (IEC62443-2-1, 2010).
- Terms and conditions of employment shall clearly state the personnel's responsibility for cyber security. These responsibilities shall extend for a reasonable period of time after employment ceases (IEC62443-2-1, 2010).
- Duties should be segregated amongst personnel to maintain appropriate checks and balances, so that no single individual has total control over actions that change the functional operation of the IACS (IEC62443-2-1, 2010).
- Training programs should be carefully developed to ensure that each employee has received training relevant and necessary to his job functions. Further, ensure that the employees have demonstrated their competence in their job functions (NIST-SP-800-82-R2, 2015).

Screening and confidentiality

- A strict screening process for key personnel (ISO/IEC, 2017; NISTIR-7628-Vol1, 2014).
- The organization provides employees, contractors, and third parties with expectations of conduct, duties, terms and conditions of employment, legal rights, and responsibilities (NISTIR-7628-Vol1, 2014).
- Roles and responsibilities need to be defined for the trusted partners, for example who will patch updates and on what schedule, who has system privileges, or who will purchase components from which suppliers (NISTIR-7628-Vol1, 2014).
- Strict screening, appropriate training and confidentiality agreement with third party personnel and contractors connecting to process control systems (CPNI, 2008e; NISTIR-7628-Vol1, 2014).

Least Privilege to users

- The organization assigns the most restrictive set of rights and privileges or access needed by users for the performance of specified tasks and configures the smart grid information system to enforce the most restrictive set of rights and privileges or access needed by users (NISTIR-7628-Vol1, 2014).

Separation of Duties

- The organization establishes and documents divisions of responsibility and separates functions as needed to eliminate conflicts of interest and to ensure independence in the responsibilities and functions of individuals/roles (NISTIR-7628-Vol1, 2014).
- The organization enforces separation of functions through assigned access authorizations and restricts security functions to the least amount of users necessary to ensure the security of the smart grid information system (NISTIR-7628-Vol1, 2014).

Security Awareness and Training

All personnel that perform risk management, IACS engineering, system administration/maintenance and other tasks that impact the CSMS should be trained on the security objectives and industrial operations for these tasks (IEC62443-2-1, 2010). The organization should provide basic security awareness briefings to all smart grid information system users (including employees, contractors, and third parties) on an organization-defined frequency (NISTIR-7628-Vol1, 2014).

- A comprehensive program of education, training, practical experience, and awareness is necessary. The organization shall design and implement a cyber security training program (IEC62443-2-1, 2010). Professionalization and certification licensing provide a validated and recognized expert cadre of system administrators (NISTIR-7628-Vol1, 2014).
- The cyber security training program shall be revised, as necessary, to account for new or changing threats and vulnerabilities (IEC62443-2-1, 2010).
- The training program should be validated on an on-going basis to ensure that personnel understand the security program and that they are receiving the proper training (IEC62443-2-1, 2010).
- All personnel (including employees, contract employees, and third-party contractors) shall be trained initially and periodically thereafter in the correct security procedures and the correct use of information processing facilities (IEC62443-2-1, 2010). Training should be provided before authorizing access to the smart grid information system or performing assigned duties, when required by smart grid information system changes and on an organization-defined frequency thereafter (NISTIR-7628-Vol1, 2014).

- The organization trains key personnel on various topics such as policies and standards, procedures, incident response, architecture, vendor specific training and detailed technical training using internal training and/or external training courses and approved third party training (CPNI, 2008d). The organization establishes links between IT security and process control teams in order to build working relationships, share skills, and facilitate knowledge transfer (CPNI, 2008d).
- Continuity of Operations/Contingency Plan Training (NIST-SP-800-82-R2, 2015; NISTIR-7628-Vol1, 2014): The organization trains personnel in their continuity of operations/contingency roles and responsibilities with respect to the smart grid information system and provides refresher training on an organization-defined frequency.
- Incident Response Training (NISTIR-7628-Vol1, 2014): Personnel are trained in their incident response roles and responsibilities with respect to the smart grid information system and receive refresher training on an organization-defined frequency.
- The organization maintains a record of awareness and training for each user in accordance with the provisions of the organization's training and records retention policy (NISTIR-7628-Vol1, 2014). Records of employee training and schedules for training updates should be maintained and reviewed on a regular basis (IEC62443-2-1, 2010).

Maintenance Personnel

The organization documents authorization and approval policies and procedures for maintaining a list of personnel authorized to perform maintenance on the smart grid information system (NISTIR-7628-Vol1, 2014); and when maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the smart grid information system (NISTIR-7628-Vol1, 2014).

3.3 Technical requirements

IED access control

- All electronic access to the IED, whether locally through a control panel, locally through a communication/diagnostic port with a test set or personal computer, or remotely through communications media, shall be protected by unique user identification (ID) and password combinations (IEEE-1686, 2014).
- The IED shall have an open and documented interface to change user accounts, passwords, and roles, which can be enacted through the use of a third party products (IEEE-1686, 2014).
- The IED shall have no means, undisclosed to the implementing entity, whereby the user-created ID/password control can be defeated or circumvented (IEEE-1686, 2014).
- The minimum number of individual users supported by the IED shall be ten (IEEE-1686, 2014).
- The IED shall have a timeout feature that automatically logs out a user who has logged in after a period of user inactivity (IEEE-1686, 2014).
- The IED shall have the capability to assign authorization using role-based access control with at least four user-defined roles (IEEE-1686, 2014).

Access control – identity and account administration

- Access privileges implemented for access accounts shall be established in accordance with the organization's authorization security policy (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- As for all cyber security controls, the choice of access accounts for individuals versus access accounts for a crew shall be determined by considering threats, risks and vulnerabilities. In this case, considerations include HSE risks of individual controls, mitigation using complementary physical security controls, requirement for accountability and administrative/operational need (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- Access shall be granted, changed, or terminated on the authority of an appropriate manager.
- A record shall be maintained of all access accounts, including details of the individual(s) and devices authorized to use the account, their permissions and the authorizing manager.
- Access accounts shall be suspended or removed as soon as they are no longer needed (for example, job change) (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- All established access accounts shall be reviewed regularly to ensure that the individual(s) and devices have only the minimum required permissions (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- Default passwords for access accounts shall be changed before the IACS is put into service (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- Periodic reviews of compliance to the account administration policy should be performed (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- The control system shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- The control system shall provide the capability to support the management of identifiers by user, group, role or control system interface (IEC62443-2-1, 2010; IEC62443-3-3, 2013).

Access control – identification and authentication

- Companies shall have an authentication strategy or approach that defines the method(s) of authentication to be used (IEC62443-2-1, 2010; IEC62443-3-3, 2013).

- All users shall be authenticated before using the requested application, unless there are compensating combinations of entrance control technologies and administrative practices (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- Strong authentication practices (such as requiring strong passwords) shall be used on all system administrator access accounts and application configuration access accounts (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- Log files should record all access attempts to critical systems and should be reviewed for successful and failed access attempts (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- The organization shall employ an authentication scheme with an appropriate level of strength to positively identify a remote interactive user (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- The organization shall develop a policy addressing remote login by a user and/or remote connections (for example, task-to-task connections) to the control system which defines appropriate system responses to failed login attempts and periods of inactivity (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- After some number of failed login attempts by a remote user, the system should disable the access account for a certain amount of time (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- After a defined period of inactivity, a remote user should be required to re-authenticate before the remote user can re-access the system (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- Systems should employ appropriate authentication schemes for task-to-task communication between applications and devices (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- The control system shall provide the capability to: a) initialize authenticator content; b) change all default authenticators upon control system installation; c) change/refresh all authenticators; and d) protect all authenticators from unauthorized disclosure and modification when stored and transmitted (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- For control systems utilizing password-based authentication, the control system shall provide the capability to enforce configurable password strength based on minimum length and variety of character types (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- The control system shall provide the capability to obscure feedback of authentication information during the authentication process (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- The control system shall provide the capability to identify and authenticate all software processes and devices. This capability shall enforce such identification and authentication on all interfaces which provide access to the control system to support least privilege in accordance with applicable security policies and procedures (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- The control system shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel (IEC62443-2-1, 2010; IEC62443-3-3, 2013).

Access control – authorization

- The permission to access IACS devices shall be logical (rules that grant or deny access to known users based on their roles), physical (locks, cameras, and other controls that restrict access to an active computer console), or both (IEC62443-2-1, 2010; IEC62443-3-3, 2013).

- Access accounts should be role based to manage access to appropriate information or systems for that user's role. Safety implications shall be considered when defining roles (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- In critical control environments, multiple authorization methods should be employed to limit access to the IACS (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- The control system shall provide the capability to enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period. The control system shall provide the capability to deny access for a specified period of time or until unlocked by an administrator when this limit has been exceeded (IEC62443-2-1, 2010; IEC62443-3-3, 2013; NISTIR-7628-Vol1, 2014).
- The control system shall provide the capability to monitor and control all methods of access to the control system via untrusted networks (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- On all interfaces, the control system shall provide the capability to enforce authorizations assigned to all human users for controlling use of the control system to support segregation of duties and least privilege (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- The control system shall provide the capability to automatically enforce configurable usage restrictions that include: a) preventing the use of portable and mobile devices; b) requiring context specific authorization; and c) restricting code and data transfer to/from portable and mobile devices (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- The control system shall provide the capability to enforce usage restrictions for mobile code technologies based on the potential to cause damage to the control system that include: a) preventing the execution of mobile code; b) requiring proper authentication and authorization for origin of the code; c) restricting mobile code transfer to/from the control system; and d) monitoring the use of mobile code (NISTIR-7628-Vol1, 2014).
- The control system shall provide the capability to prevent further access by initiating a session lock after a configurable time period of inactivity or by manual initiation. The session lock shall remain in effect until the human user who owns the session or another authorized human user re-establishes access using appropriate identification and authentication procedures (NISTIR-7628-Vol1, 2014).

Access control - access management

- Smart grid information systems are designed and implemented with mechanisms to restrict access between the smart grid information system and the organization's enterprise network (NISTIR-7628-Vol1, 2014).
- The control system shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity or manually by the user who initiated the session (IEC62443-3-3, 2013).
- The control system shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device) to a configurable number of sessions (IEC62443-3-3, 2013; NISTIR-7628-Vol1, 2014).

Remote access

- The organization authorizes, monitors, and manages all methods of remote access to the smart grid information system (NISTIR-7628-Vol1, 2014).
- Devices such as modems allow remote access to control system equipment and possible "back door" entry points for exploits on the network or directly on the control system equipment. Telephony firewalls with authorized list, automatic block, and alarm during unauthorized access and automatic log review, encryption, authentication, automated

monitoring of modem and control device connection logs should be used to protect the device (Finco et al., 2007).

- TCP/IP stack requires external mitigations (e.g. encryption, authentication, proper network partitioning, and correct firewall configuration) and good software security solution e.g. IP Security (IPsec), which provides the ability to authenticate and encrypt IP traffic within the protocol stack (Finco et al., 2007).
- Web-based interfaces to control systems are often poorly designed and configured, making these interfaces vulnerable to exploits. Therefore, secure coding practices such as authentication, input validation should be followed to handle vulnerabilities such as Remote File Include (RFI), Cross-Site Scripting (XSS) for all Web-based interface software (Finco et al., 2007).
- Virtual private networks (VPNs), if poorly configured, creates easily exploitable vulnerabilities. Therefore encrypted traffic and protected authentication mechanism should be used to make a VPN secure (Finco et al., 2007).
- Serial communications security protocols used in serial communications can be exploited to gain control of network devices which can then be leveraged by an attacker to gain further control of the network. Mitigation strategies e.g., patching applications supporting the protocol or the protocol itself, link encryptors, must be employed to prevent exploitations from occurring within the serial domain (Finco et al., 2007).

Audit trail, events and logs

- The IED shall record in a sequential circular buffer (first in, first out), an audit trail (audit log) listing events in the order in which they occur. There shall be no capability to erase or modify the audit trail purposes (IEEE-1686, 2014).
- The control system shall provide the capability to generate audit records relevant to security for the following categories: access control, request errors, operating system events, control system events, backup and restore events, configuration changes, potential reconnaissance activity and audit log events. Individual audit records shall include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result (IEEE-1686, 2014).
- The control system shall allocate sufficient audit record storage capacity according to commonly recognized recommendations for log management and system configuration. The control system shall provide auditing mechanisms to reduce the likelihood of such capacity being exceeded (IEEE-1686, 2014).
- The control system shall provide the capability to alert personnel and prevent the loss of essential services and functions in the event of an audit processing failure. The control system shall provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations (IEEE-1686, 2014).
- The control system shall provide timestamps for use in audit record generation (IEEE-1686, 2014).
- The control system shall protect audit information and audit tools (if present) from unauthorized access, modification and deletion (IEEE-1686, 2014).
- The control system shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis (IEEE-1686, 2014).

Alarms

- Alarms should be raised in case of an unauthorized activity such as unsuccessful login attempt, reboot, attempted use of unauthorized configuration software, invalid configuration or firmware download, unauthorized configuration or firmware file, time signal out of tolerance, invalid field hardware changes (IEEE-1686, 2014).

- Alarm points shall have momentary change detect capability so that the occurrence of an alarm will be reported on the next scan of the IED by the supervisory system (IEEE-1686, 2014).

Backup

- The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the control system without affecting normal plant operations (IEC62443-3-3, 2013).

Communications port access

- All communications ports, whether physical or logical, other than the diagnostic port on the IED shall have the capability to be enabled or disabled through configuration of the IED. When disabled through configuration, no communications shall be possible through the disabled port (IEEE-1686, 2014).

Configuration management/Configuration for least functionality

- The control system shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The control system shall provide an interface to the currently deployed network and security configuration settings (IEC62443-3-3, 2013).
- The smart grid information system is configured to provide only essential capabilities and specifically prohibits and/or restricts the use of functions, ports, protocols, and/or services as defined in an organizationally generated “prohibited and/or restricted” list and is reviewed on an organization-defined frequency or as deemed necessary to identify and restrict unnecessary functions, ports, protocols, and/or services (NISTIR-7628-Vol1, 2014).
- The control system shall provide the capability to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services (IEC62443-3-3, 2013). Unnecessary services and programs must be removed or disabled by the vendor prior to the Factory Acceptance Test (FAT) and the Vendor shall provide documentation on what is removed and/or disabled (Finco et al., 2007).
- The Vendor shall compare the results of cyber security scans run on the control system, as a primary activity of the FAT and Site Acceptance Test (SAT), with an inventory of the required services, patching status, and documentation, to validate this requirement (Finco et al., 2007).
- The control system shall provide the capability to report the current list of installed components and their associated properties (IEC62443-3-3, 2013).

Hardware configuration

- Unnecessary hardware shall be physically disabled, removed, or its configuration altered through software since these can be used to introduce vulnerabilities such as viruses, root kits, malware, bots, key-loggers, etc. (Finco et al., 2007).
- Configuring the network devices to limit access from only specific locations (e.g., IP filtering) or requiring additional verification of user credentials (Finco et al., 2007).
- Local hardening can require similar verification for protecting system BIOS configuration parameters, and limiting system access through local media (e.g., disabling/removing USB ports, CD/DVD drives, and other removable media devices) (Finco et al., 2007).
- System hardening to increase security robustness (NISTIR-7628-Vol1, 2014).

Secure architecture

- The organization develops a security architecture with consideration for the resulting risk to organizational operations, organizational assets, individuals, and other organizations. A logical security architecture should be viewed as a business enabler for the smart grid to achieve its operational mission and promotes an iterative process for revising the architecture to address new threats, vulnerabilities, and technologies (NISTIR-7628-Vol1, 2014).
- Selection of appropriate architecture as a security improvement measure. If possible, use already available standard and proven solutions with known quality standards, ease of management and aim for commonality to minimize cost and complexity (CPNI, 2008b). Secure network architectures contain a combination of network segmentation, traffic control, and traffic monitoring (Finco et al., 2007).
- Use of microgrid model so that availability starts in a local microgrid and that resilience is gained by aggregating and interconnecting those microgrids (NISTIR-7628-Vol1, 2014).
- Defense-in-depth strategy applies security in layers, with one or more security measures implemented at each layer (e.g., firewalls, intrusion detection systems, antivirus software, and cryptography) with a focus on three critical elements namely: people, process, technology, so as to mitigate the risk of one component of the defense being compromised or circumvented (NISTIR-7628-Vol1, 2014).
- Defense-in-breath strategy by using security activities that are planned across the system, network, or subcomponent life cycle in order to identify, manage, and reduce the risk of exploitable vulnerabilities across the life cycles (NISTIR-7628-Vol1, 2014).
- Existing legacy systems need to be considered as the new architecture is designed. Security implications need to be reviewed and updated, both to consider the legacy security mechanisms and the current state of security practice (NISTIR-7628-Vol1, 2014).

Secure development practices

- The organization applies security engineering principles in the specification, design, development, testing and implementation of any smart grid information system (NISTIR-7628-Vol1, 2014).
- The organization manages the smart grid information system using a system development lifecycle methodology that includes security (NISTIR-7628-Vol1, 2014). Projects with direct/indirect process control systems implications should include security requirements in the design and specification of projects along with security design reviews, secure coding reviews, security testing and secure replacement of defective parts containing data (CPNI, 2008f). Build and validate high-level security into software in different phases, beginning at the requirements phase (Finco et al., 2007).

Continuous monitoring and reporting

- The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes ongoing security requirements assessments in accordance with the organizational continuous monitoring strategy and reporting the security state of the smart grid information system to management authority on an organization-defined frequency (NISTIR-7628-Vol1, 2014).
- The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduit model (IEC62443-3-3, 2013).
- The control system shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and

recommendations to detect, characterize and report security breaches in a timely manner (IEC62443-3-3, 2013).
- Heartbeat signals indicate the communication health of the system. The vendor shall identify heartbeat signals or protocols and recommend whether any should be included in network monitoring. The vendor shall create a baseline of the heartbeat communications traffic, to include frequency, packet sizes, and expected packet configurations (Finco et al., 2007).
- The organization's security program implements continuous improvement practices to ensure that industry lessons learned and best practices are incorporated into smart grid information system security policies and procedures (NISTIR-7628-Vol1, 2014).

Cryptographic infrastructure, features and techniques

- Deployment of cryptographic infrastructure supporting key, privilege, and certificate management that enables positive identification of entities using information and communication technologies (NISTIR-7628-Vol1, 2014).
- For IEDs that implement specific communications functions over IP-based networks, cryptographic techniques and versions shall be implemented in the IED e.g. Hypertext Transfer Protocol Secure (HTTPS) for webserver functionality, Secure File-Transfer Protocol (SFTP), Secure Shell (SSH) for text-oriented communication, SNMPv3 for Single Network Management Protocol (SNMP) implementation, NTP v3/4 or SNTP ¾ for Network time synchronization, Virtual Private Network (VPN) for secure tunnel functionality (IEEE-1686, 2014).
- In order to achieve secure communications between IEDs, cryptographic techniques, and combinations of techniques such as block ciphers, block cipher modes, digital signatures, entity authentication, key derivation functions, message authentication, random number generation, secure hashing, key establishment. IEDs shall comply with the current NIST requirements at the time they are manufactured (IEEE-1686, 2014).
- If cryptography is required, the control system shall use cryptographic algorithms, key sizes and mechanisms for key establishment and management according to commonly accepted security industry practices and recommendations (IEC62443-3-3, 2013).

Data confidentiality

- The control system shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit (IEC62443-3-3, 2013).
- The control system shall provide the capability to purge all information for which explicit read authorization is supported from components to be released from active service and/or decommissioned (IEC62443-3-3, 2013).

Emergency power

- The control system shall provide the capability to switch to and from an emergency power supply without affecting the existing security state or a documented degraded mode (IEC62443-3-3, 2013).
- An alternate power supply is available to facilitate an orderly shutdown of noncritical smart grid information system components in the event of a primary power source loss (NISTIR-7628-Vol1, 2014).

Encrypting serial communications

- IEDs that are able to employ serial communications for any remote access application (data transfer, configuration, firmware upload, etc.) shall provide data encryption in accordance with IEEE Std 1711 for all ports designed to permit remote access (IEEE-1686, 2014).

IED configuration software

- The configuration software shall be ID/password controlled (IEEE-1686, 2014).
- The IED shall have a means to authenticate that the configuration software being used to access or change the configuration is a copy that has been authorized by the user (IEEE-1686, 2014).
- The configuration software shall have the capability to generate a digital signature in the configuration and firmware download files indicating the file has been produced by an authorized configuration software program and by an authorized user (IEEE-1686, 2014).

Network segmentation

- A network segmentation countermeasure strategy employing security zones shall be developed for IACS devices based upon the risk level of the IACS (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- High-risk IACS shall be isolated from or employ a barrier device to separate it from other zones with different security levels or risks (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- Process control networks should be appropriately segregated from office networks and outside world by an appropriate means (CPNI, 2008g).
- Barrier devices shall block all non-essential communications in and out of the security zone containing critical control equipment (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- Firewalls shall be installed and firewall rule sets between network zones must be established for perimeter protection (Finco et al., 2007).
- The control system shall provide the capability to prevent general purpose person-to-person messages (such as Facebook, Twitter, etc.) from being received from users or systems external to the control system (IEC62443-2-1, 2010; IEC62443-3-3, 2013).
- The control system shall provide the capability to support partitioning of data, applications and services based on criticality to facilitate implementing a zoning model (IEC62443-2-1, 2010; IEC62443-3-3, 2013).

Canaries

- Canary(ies), which flag that a connection attempt has taken place, shall be implemented in certain network configurations to provide passive network monitoring and reconfigured when network address topologies change (Finco et al., 2007).

Honeypots

- The smart grid information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, analyzing, and tracking such attacks (NISTIR-7628-Vol1, 2014).

.

Non-repudiation

- The control system shall provide the capability to determine whether a given human user took a particular action (IEC62443-3-3, 2013).

Malware Detection and Protection

- Host-based malware detection scheme for the control system network (Finco et al., 2007).

Third party port and protocol usage

- Determine information from vendors related with third party ports and protocols used (CPNI, 2008e).

Patch management

- Patch management tasks include: maintaining current knowledge of available patches, deciding which patches are appropriate for particular systems, ensuring that patches are installed properly, testing systems after installation and documenting all associated procedures, such as specific configurations required remotely across heterogeneous environments according to recognized best practices (IEC62443-2-1, 2010).
- Responsible system and product vendors regularly release updates, patches, service packs, or other fixes to their products to address known and potential vulnerabilities. Therefore, an essential system hardening activity is simply installing the latest versions or updates of any necessary software loaded on a system after necessary testing and validation of the patches (CPNI, 2008g; Finco et al., 2007; NISTIR-7628-Vol1, 2014).A procedure to keep track of - how quickly are patches applied, where are they received from, are all machines patched, etc. The vendor shall provide patch management process and mitigation strategies, for instances, vendor informing the user when not to apply released patches (CPNI, 2008g; Finco et al., 2007).

Physical and environmental security

- One or more physical security perimeters shall be established to provide barriers to unauthorized access to protected assets using methods such as biometrics, passwords, and security tokens/certificates (IEC62443-2-1, 2010).
- Appropriate entry controls shall be provided at each barrier or boundary (IEC62443-2-1, 2010).
- Some form of authentication can be tightly coupled with physical perimeter security (e.g., proximity monitors, keycard access to buildings) and control access and logoff to cyber systems (Finco et al., 2007). Other physical security controls such as locked doors, locked cabinets and/or restricted areas with closed circuit TV, card readers, etc., can be used to monitor and log entry to mitigate risk (NISTIR-7628-Vol1, 2014).
- Manual override controls include mechanisms such as circuit breaker hand switches, valve levers, and end-device panels. Physical access to manual override controls should be heavily restricted to authorized personnel only (IEC62443-2-1, 2010).
- Intra-perimeter communication ensures secure operation thus the communication path must be physically secured to the same level as the components. The length and complexity of the communication channel to be protected should be minimized. The communication channel and access ports should also be hidden from view, out of reach, and/or behind layers of perimeter security if possible (IEC62443-2-1, 2010).
- Assets shall be protected against environmental damage from threats such as fire, water, smoke, dust, radiation, corrosion and impact (IEC62443-2-1, 2010).
- All connections under the control of the organization shall be adequately protected from tampering or damage (IEC62443-2-1, 2010).
- All equipment assets, including auxiliary environmental equipment, shall be properly maintained to ensure proper operation (IEC62443-2-1, 2010).

Public key infrastructure (PKI)

- Where PKI is utilized, the control system shall provide the capability to operate a PKI according to commonly accepted best practices or obtain public key certificates from an existing PKI (IEC62443-3-3, 2013)**.**
- For control systems utilizing public key authentication, the control system shall provide the capability to (IEC62443-3-3, 2013):
    - Validate certificates by checking the validity of the signature of a given certificate.
    - Validate certificates by constructing a certification path to an accepted CA or in the case of self-signed certificates by deploying leaf certificates to all hosts which communicate with the subject to which the certificate is issued.
    - Validate certificates by checking a given certificate's revocation status;
    - establish user (human, software process or device) control of the corresponding private key.
    - Map the authenticated identity to a user (human, software process or device).

Recovery and reconstitution

- The control system shall provide the capability to recover and reconstitute to a known secure state after a disruption or failure (IEC62443-3-3, 2013).

Risk Analysis / Risk Assessment

- The organization shall develop simple network diagrams for each of the logically integrated systems showing the major devices, network types and general locations of the equipment (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- The organization shall clearly identify the SUC (System Under Consideration), including clear demarcation of the security perimeter and identification of all access points to the SUC (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- The organization shall group IACS and related assets into zones or conduits as determined by risk. Grouping shall be based upon the results of the initial cyber security risk assessment or other criteria, such as criticality of assets, operational function, physical or logical location, required access (for example, least privilege principles) or responsible organization (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- IACS assets shall be grouped into zones that are logically or physically separated from business or enterprise system assets (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- Safety related IACS assets shall be grouped into zones that are logically or physically separated from zones with non-safety related IACS assets. However, if they cannot be separated, the entire zone shall be identified as a safety related zone (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- Devices that are permitted to make temporary connections to the SUC should be grouped into a separate zone or zones from assets that are intended to be permanently connected to the IACS (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- Wireless devices should be in one or more zones that are separated from wired devices (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- Devices that are permitted to make connections to the SUC via networks external to the SUC should be grouped into a separate zone or zones (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- The initial risk determined shall be compared to the organization's tolerable risk. If the initial risk exceeds the tolerable risk, the organization shall perform a detailed cyber security risk assessment (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- A list of the threats that could affect the assets contained within the zone or conduit shall be developed (IEC62443-2-1, 2010; IEC62443-3-2, 2020).

- The zone or conduit shall be analysed in order to identify and document the known vulnerabilities associated with the assets contained within the zone or conduit including the access points (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- Each threat scenario shall be evaluated to determine the consequence and the impact should the threat be realized. Consequences should be documented in terms of the worst-case impact on risk areas such as personnel safety, financial loss, business interruption and environment (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- Each threat shall be evaluated to determine the unmitigated likelihood. This is the likelihood that the threat will materialize (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- The unmitigated cyber security risk for each threat shall be determined by combining the impact measure determined and the unmitigated likelihood measure (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- A SL-T (Security Level Target) shall be established for each security zone or conduit (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- The unmitigated risk determined for each threat identified shall be compared to the organization’s tolerable risk. If the unmitigated risk exceeds the tolerable risk, the organization shall determine whether to accept, transfer or mitigate the risk. To mitigate the risk, continue to evaluate the threat. Otherwise, the organization may document the results and proceed to the next threat (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- Existing countermeasures in the SUC shall be identified and evaluated to determine the effectiveness of the countermeasures to reduce the likelihood or impact (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- The likelihood and impact shall be re-evaluated considering the countermeasures and their effectiveness (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- The residual risk for each threat identified shall be determined by combining the mitigated likelihood measure and mitigated impact values.
- The residual risk determined for each threat identified shall be compared to the organization’s tolerable risk. If the residual risk exceeds the tolerable risk, the organization shall determine if the residual risk will be accepted, transferred or mitigated based upon the organization’s policy (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- Additional cyber security countermeasures such as technical, administrative or procedural controls shall be identified to mitigate the risks where the residual risk exceeds the organization’s tolerable risk unless the organization has elected to tolerate or transfer the risk (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- The results of the detailed cyber risk assessment shall be documented, reported and made available to the appropriate stakeholders in the organization. Appropriate information security classification shall be assigned to protect the confidentiality of the documentation. Documentation shall include the date each session was conducted as well as the names and titles of the participants. Documentation that was instrumental in performing the cyber risk assessment (such as, system architecture diagrams, PHAs, vulnerability assessments, gap assessments and sources of threat information) shall be recorded and archived along with the cyber risk assessment (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- A cyber security requirements specification (CRS) shall be created to document mandatory security countermeasures of the SUC based on the outcome of the detailed risk assessment as well as general security requirements based upon company or site-specific policies, standards and relevant regulations. At a minimum, the CRS shall include the following: SUC description; Zone and conduit drawings; Zone and conduit characteristics; Operating environment assumptions; Threat environment; Organizational security policies; Tolerable risk; and Regulatory requirements (IEC62443-2-1, 2010; IEC62443-3-2, 2020).

- A high-level description and depiction of the SUC shall be included in the CRS. At a minimum, the CRS shall include the name, a high-level description of the function and the intended usage of the SUC, as well as, a description of the equipment or process under control (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- The organization shall: a) Produce a drawing or a set of drawings that illustrates the zone and conduit partitioning of the entire SUC. b) Assign each asset in the SUC to a zone or a conduit(IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- The following items shall be identified and documented for each defined zone and conduit (IEC62443-2-1, 2010; IEC62443-3-2, 2020): a) Name and/or unique identifier; b) Accountable organization(s); c) Definition of logical boundary; d) Definition of physical boundary, if applicable; e) Safety designation; f) List of all logical access points; g) List of all physical access points; h) List of data flows associated with each access point; i) Connected zones or conduits; j) List of assets and their classification, criticality and business value; k) SL-T; l) Applicable security requirements; m) Applicable security policies; and n) Assumptions and external dependencies.
- The CRS shall identify and document the physical and logical environment in which the SUC is located or planned to be located (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- The CRS shall include a description of the threat environment that impacts the SUC. The description shall include the source(s) of threat intelligence and include both current and emerging threats (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- Security countermeasures and features that implement the organizational security policies shall be included in the CRS (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- The organization's tolerable risk for the SUC shall be included in the CRS.
- Any relevant cyber security regulatory requirements that apply to the SUC shall be included in the CRS (IEC62443-2-1, 2010; IEC62443-3-2, 2020).
- Asset owner management who are accountable for the safety, integrity and reliability of the process controlled by the SUC shall review and approve the results of the risk assessment (IEC62443-2-1, 2010; IEC62443-3-2, 2020).

Resource availability

- The control system shall provide the capability to operate in a degraded mode during a DoS event (IEC62443-3-3, 2013).
- The control system shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion (IEC62443-3-3, 2013).

System integrity

- The control system shall provide the capability to protect the integrity of transmitted information (IEC62443-3-3, 2013).
- The control system shall provide the capability to employ cryptographic mechanisms to recognize changes to information during communication (IEC62443-3-3, 2013).
- The control system shall provide the capability to employ protection mechanisms to prevent, detect, report and mitigate the effects of malicious code or unauthorized software. The control system shall provide the capability to update the protection mechanisms (IEC62443-3-3, 2013).
- The control system shall provide the capability to detect, record, report and protect against unauthorized changes to software and information at rest (IEC62443-3-3, 2013).
- The control system shall validate the syntax and content of any input which is used as an industrial process control input or input that directly impacts the action of the control system (IEC62443-3-3, 2013).

- The control system shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack (IEC62443-3-3, 2013).
- The control system shall identify and handle error conditions in a manner such that effective remediation can occur. This shall be done in a manner which does not provide information that could be exploited by adversaries to attack the IACS unless revealing this information is necessary for the timely troubleshooting of problems (IEC62443-3-3, 2013).
- The control system shall provide the capability to protect the integrity of sessions. The control system shall reject any usage of invalid session IDs (IEC62443-3-3, 2013).

Security testing and verification

- The control system shall provide the capability to support verification of the intended operation of security functions and report when anomalies are discovered during FAT, SAT and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in this standard (IEC62443-3-3, 2013).

Wireless access management

- The control system shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication (IEC62443-3-3, 2013).
- The control system shall provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the control system according to commonly accepted security industry practices (IEC62443-3-3, 2013).

3.4 Operational requirements

Role-based access control

- Role-based privileges should be provided based on the responsibilities of the users of the utilities (IEEE-C37.240, 2015).

Data protection

- Protection of data at rest and files, whether in hard copy or existing on IEDs, is critical. Engineering manuals, drawings, and lists of passwords should also be secured (IEEE-C37.240, 2015).

Password defeat mechanisms

- The vendor shall disclose any and all mechanisms whereby the user-created ID/password control to the IED can be circumvented. If the vendor represents that no such mechanisms are present in the IED, the vendor shall certify in writing to that effect (IEEE-1686, 2014).

Supervisory monitoring and control

- The IED shall monitor security-related activity and shall make the information available through a real-time communication protocol for transmission to a supervisory system (IEEE-1686, 2014).

Supervisory permissive control

- The IED shall provide a mechanism that, when enabled, requires independent supervisory permission prior to performing actions or requests in the field and/or remotely (IEEE-1686, 2014).
- All diagnostic ports shall have the ability to be enabled and disabled remotely through a supervisory control command (IEEE-1686, 2014).

IED functionality compromise

- Users should be alerted in case of any possible compromise of the primary IED functions during the usage of either the protocol port(s) or diagnostic port(s) (IEEE-1686, 2014).

Firmware quality assurance

- Firmware quality assurance shall be in compliance with IEEE Std C37.231 (IEEE-1686, 2014).

Interface between control systems (substation master) and sensor networks

- Security requirements for such interfaces should be identified and implemented e.g. device identification and authentication, denial of service protection, boundary protection, communication integrity, software and information integrity (NISTIR-7628-Vol1, 2014).

Interface between systems and mobile field crew laptops/equipment

- Mobile field crew may be obtaining and providing substation equipment information, such as location, fault, testing, and maintenance updates, or outage information and providing restoration information, including equipment, materials, and resource information. Security requirements for such interfaces should be identified and implemented e.g., concurrent session control, session lock, remote session termination, permitted actions without identification or authentication, user identification and authentication, device identification and authentication, authenticator feedback, voice over internet protocol, application partitioning, software and information integrity (NISTIR-7628-Vol1, 2014).

Interface between engineering/ maintenance systems and control equipment *e.g., between engineering and substation relaying equipment for relay settings or between engineering and pole-top equipment for maintenance*

- Security requirements for such interfaces should be identified and implemented e.g., permitted actions without identification or authentication, remote access, non-repudiation, user identification and authentication, device identification and authentication, authenticator feedback, security function isolation, boundary protection, communication integrity, voice over internet protocol, application partitioning, software and information integrity (NISTIR-7628-Vol1, 2014).

Physical and environmental security

- Security policies and procedures that address both physical and cyber security in the protection of assets shall be established (IEC62443-2-1, 2010).
- A defense-in-depth solution to physical security should include the following attributes: protection of physical locations, access control, people and asset tracking, environmental factors, environmental control systems, and reliable power for ICS (NIST-SP-800-82-R2, 2015) (NISTIR-7628-Vol1, 2014).
- These policy and procedures include all physical access to an information system including designated entry/exit points, transmission media, and display media. These include controls for monitoring physical access, maintaining logs, and handling visitors, as well as controls for the deployment and management of emergency protection controls such as emergency shutdown of the IT system, backup for power and lighting, controls for temperature and humidity, and protection against fire and water damage The organization approves and monitors the use of smart grid information system maintenance tools (NIST-SP-800-82-R2, 2015; NISTIR-7628-Vol1, 2014).
- The deployment of physical security controls is often subject to environmental, safety, regulatory, legal, and other requirements that must be identified and addressed specific to a given environment. And this must be addressed as part of the overall plant security The organization approves and monitors the use of smart grid information system maintenance tools (NIST-SP-800-82-R2, 2015; NISTIR-7628-Vol1, 2014).
- Employees shall be required to follow and enforce the physical security procedures that have been established (IEC62443-2-1, 2010).
- Depending on security needs and risks, it might also be prudent to disable or physically protect power buttons to prevent unauthorized use. For maximum security, servers should be placed in locked areas and authentication mechanisms protected. The network devices on the ICS network, including switches, routers, network jacks, servers, workstations, and controllers, should be located in a secured area that can only be accessed by authorized personnel. The secured area should also be compatible with the environmental requirements of the devices (NIST-SP-800-82-R2, 2015; NISTIR-7628-Vol1, 2014).
- Procedures shall be established for monitoring and alarming when physical or environmental security is compromised (IEC62443-2-1, 2010).
- The organization retains all physical access logs for as long as dictated by any applicable regulations or based on an organization-defined period by approved policy (NIST-SP-800-82-R2, 2015; NISTIR-7628-Vol1, 2014).
- Procedures should be established and audited with respect to the addition, removal and disposal of all assets (IEC62443-2-1, 2010).

- Procedures shall be established to ensure the protection of critical components during the interruption of operations, for example, due to fire, water ingress, security breach, interruption, natural or any other type of disaster (IEC62443-2-1, 2010).

Risk management and implementation

- The organization shall adopt a risk management framework that includes selection and implementation of IACS devices and countermeasures to manage risk to an acceptable level over the life of the facility (IEC62443-2-1, 2010).
- A common defined set of countermeasures (technical and administrative) to address both physical and cyber security risks should be defined and applied across the organization wherever a specific risk is identified (IEC62443-2-1, 2010).

Risk analysis / Risk assessment

- The organization shall perform a detailed vulnerability assessment of its individual logical IACS, which may be scoped based on the high-level risk assessment results and prioritization of IACS subject to these risks (IEC62443-2-1, 2010).
- Risk assessments shall be conducted through all stages of the technology lifecycle including development, implementation, changes and retirement (IEC62443-2-1, 2010).
- Up-to-date vulnerability assessment records should be maintained for all assets comprising the IACS (IEC62443-2-1, 2010).

System development and maintenance

- The security functions and capabilities of each new component of the IACS shall be defined up front, developed or achieved via procurement, and tested together with other components so that the entire system meets the desired security profile (IEC62443-2-1, 2010).
- A change management system for the IACS environment shall be developed and implemented. The change management process shall follow separation of duty principles to avoid conflicts of interest (IEC62443-2-1, 2010).
- Using clearly defined criteria, proposed changes to IACS shall be reviewed for their potential impact to HSE risks and cyber security risks by individuals technically knowledgeable about the industrial operation and the IACS system (IEC62443-2-1, 2010).
- The security requirements of a new system being installed in the IACS environment in an existing zone shall meet the security policies and procedures required for that zone/environment. Similarly, maintenance upgrades or changes shall meet the security requirements for the zone (IEC62443-2-1, 2010).
- Cyber security change management procedures should be integrated with existing PSM procedures (IEC62443-2-1, 2010).
- The operations and change management policies and procedures shall be reviewed and kept current to ensure that security changes do not increase risks to safety or business continuity (IEC62443-2-1, 2010).
- A procedure for patch management shall be established, documented, and followed (IEC62443-2-1, 2010).
- A procedure for antivirus/malware management shall be established, documented, and followed (IEC62443-2-1, 2010).
- The organization makes and secures backups of critical smart grid information system software, applications, and data for use if the operating system becomes corrupted or destroyed (NISTIR-7628-Vol1, 2014). A procedure for backing up and restoring computer systems and protecting backup copies shall be established, used, and verified by appropriate testing (IEC62443-2-1, 2010).

- The organization schedules, performs, documents, and reviews records of maintenance and repairs on smart grid information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. The organization checks all potentially impacted security requirements to verify that the requirements are still functioning properly following maintenance or repair actions (NISTIR-7628-Vol1, 2014).
- The organization explicitly approves the removal of the smart grid information system or smart grid information system components from organizational facilities for off-site maintenance or repairs (NISTIR-7628-Vol1, 2014).
- The organization sanitizes the equipment to remove all critical/sensitive information from associated media prior to removal from organizational facilities for off-site maintenance or repairs (NISTIR-7628-Vol1, 2014).
- The organization approves and monitors the use of smart grid information system maintenance tools (NISTIR-7628-Vol1, 2014).

Security Responsibility Testing

- The organization tests the knowledge of personnel on security policies and procedures based on their roles and responsibilities to ensure that they understand their responsibilities in securing the smart grid information system (NISTIR-7628-Vol1, 2014);
- The organization maintains a list of security responsibilities for roles that are used to test each user in accordance with the provisions of the organization training policy (NISTIR-7628-Vol1, 2014).
- The organization ensures security responsibility is conducted on an organization-defined frequency and as warranted by technology/procedural changes (NISTIR-7628-Vol1, 2014).

Information and document management

- A lifecycle document management process shall be developed and maintained for IACS information (IEC62443-2-1, 2010).
- Information classification levels (for example, company confidential, restricted and public) shall be defined for access and control, including sharing, copying, transmitting, and distributing appropriate for the level of protection required (IEC62443-2-1, 2010).
- All logical assets within the scope of the CSMS (that is, control system design information, vulnerability assessments, network diagrams and industrial operations programs) shall be classified to indicate the protection required commensurate with the consequence of its unauthorized disclosure or modification (IEC62443-2-1, 2010).
- Policies and procedures should be developed detailing retention, physical and integrity protection, destruction, and disposal of all assets based on their classification, including written and electronic records, equipment and other media containing information, with consideration for legal or regulatory requirements (IEC62443-2-1, 2010).
- Appropriate measures should be employed to ensure long-term records can be retrieved (that is, converting the data to a newer format or retaining older equipment that can read the data) (IEC62443-2-1, 2010).
- Information that requires special control or handling should be reviewed on a periodic basis to validate that special handling is still required (IEC62443-2-1, 2010).
- Periodic reviews of compliance to the information and document management policy should be performed (IEC62443-2-1, 2010).

Incident planning and response

- The organization shall implement an incident response plan that identifies responsible personnel and defines actions to be performed by designated individuals (IEC62443-2-1, 2010).

- The incident response plan shall be communicated to all appropriate organizations.
- The organization should establish a reporting procedure to communicate unusual activities and events that may actually be cyber security incidents (IEC62443-2-1, 2010).
- Employees should be educated on their responsibility to report cyber security incidents and the methods of reporting these incidents (IEC62443-2-1, 2010).
- The organization should report cyber security incidents in a timely manner (IEC62443-2-1, 2010).
- If an incident is identified, the organization shall promptly respond in accordance with the established procedures (IEC62443-2-1, 2010).
- The organization should have procedures in place to identify failed and successful cyber security breaches (IEC62443-2-1, 2010).
- The details of an identified incident shall be documented to record the incident, the response, the lessons learned, and any actions taken to modify the CSMS in light of this incident (IEC62443-2-1, 2010).
- The documented details of an incident shall be communicated to all appropriate organizations (that is, management, IT, process safety, automation and control engineering security and manufacturing) in a timely manner (IEC62443-2-1, 2010).
- The organization shall have a business methodology in place to address issues discovered and ensure they are corrected (IEC62443-2-1, 2010).
- Drills should be conducted to test the incident response program on a routine basis (IEC62443-2-1, 2010).

Item delivery and removal

- The organization authorizes, monitors, and controls organization-defined types of smart grid information system components entering and exiting the facility and maintains records of those items (NISTIR-7628-Vol1, 2014).

Conformance

- The audit program shall specify the methodology of the audit process (IEC62443-2-1, 2010).
- Validate that the IACS conforms to the CSMS. The CSMS shall include periodic audits of the IACS, to validate that the security policies and procedures are performing as intended and meet the security objectives for the zone (IEC62443-2-1, 2010).
- The organization should define performance indicators and success criteria, which are used to monitor conformance to the CSMS. The results from each periodic audit should be expressed in the form of performance against these metrics to display security performance and security trends (IEC62443-2-1, 2010).
- A list of documents and reports required to establish an audit trail shall be developed.
- The organization shall state what non-conformance with the CSMS means, and any related punitive measures shall also be defined (IEC62443-2-1, 2010).
- The required competency for auditing the specific systems that are in scope should be specified. The level of independence required should be determined as part of the governance (IEC62443-2-1, 2010).

Review, improve and maintain the CSMS

- An organization shall be assigned to manage and coordinate the refinement and implementation of the CSMS changes and use a defined method in making and implementing changes (IEC62443-2-1, 2010).
- The managing organization shall periodically evaluate the overall CSMS to ensure the security objectives are being met (IEC62443-2-1, 2010).

- The organization should establish a list of triggers with set thresholds, which would result in a review of related elements of the CSMS and perhaps a change. These triggers include at a minimum: occurrence of serious security incidents, legal and regulatory changes, changes in risk and major changes to the IACS. The thresholds should be based on the organization's risk tolerance (IEC62443-2-1, 2010).
- The organization shall identify and implement appropriate corrective and preventive actions that modify the CSMS to meet security objectives (IEC62443-2-1, 2010).
- A review of the organization's tolerance for risk should be initiated when there are major changes to the organization, technology, business objectives, internal business and external events including identified threats and changes in social climate (IEC62443-2-1, 2010).
- Management system owners should monitor the industry for CSMS best practices for risk assessment and risk mitigation and evaluate their applicability (IEC62443-2-1, 2010).
- The organization shall identify applicable and changing legislation relevant to cyber security (IEC62443-2-1, 2010).
- Employee feedback on security suggestions should be actively sought and reported back to senior management as appropriate on performance shortcomings and opportunities (IEC62443-2-1, 2010).

References

CPNI. (2008a). Good Practice Guide: Process Control and SCADA Security Guide 1. Understand the Business Risk. *Centre for the Protection of National Infrastructure*.

CPNI. (2008b). Good Practice Guide: Process Control and SCADA Security Guide 2. Implement Secure Architecture. *Centre for the Protection of National Infrastructure*.

CPNI. (2008c). Good Practice Guide: Process Control and SCADA Security Guide 3. Establish Response Capabilities. *Centre for the Protection of National Infrastructure*.

CPNI. (2008d). Good Practice Guide: Process Control and SCADA Security Guide 4. Improve Awareness and Skills. *Centre for the Protection of National Infrastructure*.

CPNI. (2008e). Good Practice Guide: Process Control and SCADA Security Guide 5. Manage Third Party Risk. *Centre for the Protection of National Infrastructure*.

CPNI. (2008f). Good Practice Guide: Process Control and SCADA Security Guide 6. Engage Projects. *Centre for the Protection of National Infrastructure*.

CPNI. (2008g). Good Practice Guide: Process Control and SCADA Security Guide 7. Establish Ongoing Governance. *Centre for the Protection of National Infrastructure*.

Finco, G., Lee, K., Miller, G., Tebbe, J., & Wells, R. (2007). Cyber Security Procurement Language for Control Systems Version 1.6. *INL Critical Infrastructure Protection/Resilience Center, Idaho Falls, USA*.

IEC62443-2-1. (2010). ISA/IEC 62443-2-1 Industrial Communication Networks - Network and System Security - Part 2-1: Establishing an Industrial Automation and Control System Security Program. In: IEC.

IEC62443-3-2. (2020). 62443-3-2: 2020: Security for industrial automation and control systems- Part 3-2: Security risk assessment for system design. *Geneva, Switzerland.*

IEC62443-3-3. (2013). IEC 62443-3-3: Industrial Communication Networks—Network and System Security—Part 3-3: System Security Requirements and Security Levels. In *International Electrotechnical Commission, Brussels*.

IEEE-1686. (2014). Std 1686-2013 - IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities. In (pp. 1-29).

IEEE-C37.240. (2015). IEEE Std C37.240-2014 - IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems. In (pp. 1-38).

IEEE. IEEE Smart Grid. Retrieved from https://smartgrid.ieee.org/resources/webinars

ISO/IEC27001. (2013). Information technology — Security techniques — Information security management systems — Requirements. In (pp. 23).

ISO/IEC. (2017). ISO/IEC TR 27019:2017: information technology security techniques - information security controls for the energy utility industry.

Leszczyna, R. (2018a). Cybersecurity and privacy in standards for smart grids–A comprehensive survey. *Computer Standards & Interfaces, 56*, 62-73.

Leszczyna, R. (2018b). A review of standards with cybersecurity requirements for smart grid. *Computers & Security, 77*, 262-276. doi:https://doi.org/10.1016/j.cose.2018.03.011

Leszczyna, R. (2018c). Standards on cyber security assessment of smart grid. *International Journal of Critical Infrastructure Protection, 22*, 70-89.

NIST-1108-R2. (2012). NIST framework and roadmap for smart grid interoperability standards, release 2.0. In *National Institute of Standards and Technology (NIST), Tech. Rep. NIST Special Publication 1108R2* (pp. 2-0).

NIST-SP-800-82-R2. (2015). Guide to supervisory control and data acquisition (SCADA) and industrial control systems security, Special Publication NIST-SP-800-82-Rev. 2-2015. In: Gaithersburg: National Institute of Standards and Technology.

NIST-SP-800-82. (2011). Guide to industrial control systems (ics) security: Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC). In: National Institute of Standards & Technology.

NISTIR-7628-Vol1. (2014). NIST Interagency/Internal Report (NISTIR) 7628 Revision 1: Guidelines for Smart Grid Cybersecurity. In *Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements* (pp. 278). U.S.A.: National Institute of Standards and Technology

Statnett. Retrieved from https://www.statnett.no/en/

Tipton, H. F., & Nozaki, M. K. (2007). *Information security management handbook*: CRC press.

Tokas, S., Houmb, S. H., & Hugo, A. (2021). *Digitalization of power grid: major drivers, cyber security, and challenges* (2021:00292- Restricted). Retrieved from

Von Solms, R. (1999). Information security management: why standards are important. *Information Management & Computer Security*.

NTNU
Norwegian University of
Science and Technology