SECURITY PROFILE FOR SUBSTATION AUTOMATION

Prepared for:

The **UCAIug SG Security Working Group**

Prepared by:

The Advanced Security Acceleration Project for the Smart Grid (ASAP-SG)

Managed by:

EnerNex Corporation
620 Mabry Hood Road
Knoxville, TN 37923
USA
(865) 218-4600
www.enernex.com

Version
0.15

Revision History

Rev	Date	Summary	Marked
0.04	20120502	Preliminary draft for flow and logic – not content-complete	N
0.05	20120912	Control tables incorporated	N
0.06	20120912	Control table correction & modification	N
0.07	20120917	Control mapping table incorporated, other control table updates, communication objectives diagram incorporated	N
0.09	20120924	Updates to tables throughout; new introductory text for tables	N
0.10	20120925	Accepted changes to date; updated failure tables	N
0.11	20120926	New scope material; failure and control table updates; table formatting	N
0.12	20120927	Edits – primarily to Section 1	N
0.13	20120929	Team comments and edits	N
0.14	20120930	Added Appendix A	N
0.15	20120930	Completed public draft	N

Executive Summary

This document presents the security profile for electric grid substation automation technology. The profile addresses security concerns associated with automated and manual interaction in support of system protection (inter and intra-substation), system control (local and remote), system optimization (e.g., voltage and reactive power), and system monitoring (i.e., equipment health) performed by equipment located in transmission and distribution substations. The recommendations made herein are based on stated system architectural and functional assumptions, and offer a security baseline for overall use of substation automation technology with tailored subsets of recommendations where variations in system deployment or usage occur.

This document defines a reference architecture, a set of roles to define system functionality and communications, and a set of security controls for systems and components that implement the roles. The security controls in this document are inspired by and reference the application of technical requirements found in *NIST Interagency Report (IR) 7628: Guidelines for Smart Grid Cyber Security* to substation automation systems and technology. The underlying approach behind this document was therefore to (1) study real-world use of substation automation systems, (2) define the function of these systems by presenting a reference architecture that defines abstract roles and their interactions through state machines and communications analyses, (3) map the architecture's roles to real-world substation automation systems, (4) define broad security objectives for substation automation systems, (5) identify potential failure modes for each role in the context of the state machines and communications analyses, (6) define security controls to address the failure modes, and (7) assign controls to the appropriate elements of the reference architecture.

The primary audiences for this document are system owners, system implementers, and security engineers within organizations that are developing or implementing solutions requiring or providing substation automation functionality. This security profile is intended to be suitable for review, analysis, evolution, and improvement by the broader research and engineering community through the profile's presentation of details behind the analyses, such as the complete state-machine models for each of the in-scope substation automation roles and the explicit linkage between failure modes and recommended controls.

Table of Contents

Table of Figures

Table of Tables

Acknowledgements

The Advanced Security Acceleration Project for Smart Grid (ASAP-SG) would like to thank:

1. Supporting utilities, including American Electric Power and Southern California Edison.
2. Supporting organizations, including: The United States Department of Energy, the Electric Power Research Institute, and the UCAIug Smart Grid Security Working Group.
3. The utility and vendor representatives that provided ASAP-SG with essential foundational knowledge and insight into the Substation Automation problem space, with a special thanks to Southern California Edison.

ASAP-SG would also like to thank the National Institute of Standards and Technology (NIST) Computer Security Division and the North American Reliability Corporation (NERC) for the works that they have produced that served as reference material for the Security Profile for Substation Automation.

The ASAP-SG Team included resources from EnerNex Corporation, UtiliSec, Oak Ridge National Laboratory, the Software Engineering Institute at Carnegie Mellon University, and Southern California Edison.

Authors

Glenn Allgood

Len Bass

Bobby Brown

James Ivers

Teja Kuruganti

Howard Lipson

Jim Nutaro

Justin Searle

Brian Smith

Edited by: Darren Highfill

1 Introduction

This document presents the security profile for substation automation (SA) technology. System functions considered include system protection (inter and intra-substation), system control (local and remote), system optimization (e.g., voltage and reactive power), and system monitoring (i.e., equipment health). This profile addresses security concerns associated with automated and manual interaction in support of these functions with equipment located in transmission and distribution substations. The recommendations made herein are based on stated system architectural and functional assumptions, and offer a security baseline for overall use of substation automation technology with tailored subsets of recommendations where variations in system deployment or usage occur.

This document defines a reference architecture including role definitions, communication models, and a set of state machines to define system functionality. This document then analyzes the reference architecture and recommends a set of security controls for systems and components that implement the roles as defined herein. The security controls in this document are inspired by and reference the application of technical requirements found in *NIST Interagency Report (IR) 7628: Guidelines for Smart Grid Cyber Security*[1] to substation automation technology. While NIST IR 7628 serves as an industry-wide reference that a utility may use as a starting point to identify intersystem-level security requirements, this document provides the next level of detail by specifically addressing the use of substation automation technology and defining intra-system-level security controls. The controls presented herein may then, in turn, be satisfied by communications protocol definition-level standards and manufacturing specifications.

[1] National Institute of Standards and Technology (NIST), Guidelines for Smart Grid Cyber Security, NIST Interagency Report 7628, August 2010. Available at: http://csrc.nist.gov/publications/PubsNISTIRs.html.

The underlying approach for developing this document was (1) to study the real-world use of substation automation systems, (2) define the function of these systems by presenting a reference architecture that defines abstract roles, communication patterns, and role functionality in the form of UML state machines, (3) map the architecture's roles to real-world substation automation systems, (4) define broad security objectives for substation automation systems, (5) identify potential failure modes for each role based on analysis of the state machines and communication models, (6) define security controls to address the failure modes, and (7) assign controls to the appropriate elements of the reference architecture.

An understanding of the concept of roles is essential to applying the security controls defined in this document. Roles have been defined abstractly to ensure applicability across a range of substation automation applications and products. The key roles for this document are the Application and the Control Authority. An Application is able to make decisions, with or without human supervision, about what actions should be taken in a substation automation system. In this document, we decompose the Application into three constituent roles: the Protection Application, which serves the high-speed automated functions of protective relaying; the Control Application, which facilitates supervised and unsupervised decisions for optimizing equipment operation and configuring the electric grid; and the Monitoring Application, which provides situational awareness and oversight of system function performance. The Control Authority represents the modern and sometimes virtual embodiment of the classic “local-remote” switch, but also serves the more general function of coordinating and authorizing supervisory actions within the substation.

It is important to note that a single device or product may implement multiple roles. Moreover, each role may be implemented in different ways, using different technologies, and by different vendors. By assigning security controls to the abstract roles, no bias is expressed in any of these dimensions. This document addresses security concerns by requiring that products implementing the functionality of a given role satisfy all security controls associated with that role. If a product implements the functionality of multiple roles, it must implement all of the security controls associated with each of the roles.

1.1 Scope

This security profile addresses the security of automated functions found in transmission and distribution substations, including system monitoring, switchgear control, and system protection. Specifically, this security profile addresses processing and communications of measurements, notifications, and control signals within and amongst substation components used to operate, control, and protect the electric grid. Equipment inside the substation perimeter (i.e., fence, building, or other enclosure) is considered “in scope,” as are the interfaces to substation equipment for communications with remote sites and other facilities. Direct communications between substations (e.g., transfer trip) is also considered “in scope.” This document also recognizes that some organizations will only implement a subset of the functions defined herein, and is therefore built to accommodate different configurations and choices.

1.1.1 Equipment

From an equipment perspective, this security profile is scoped to devices with enabled communications interfaces (e.g., intelligent electronic devices) located inside the physical perimeter of a substation boundary and performing functions in support of system automation, control, and monitoring.

1.1.2 Processing

While determination of adequate business processing for substation automation, control, and monitoring is not in scope, this security profile does consider controls for establishing and maintaining the security of those processes to be in scope, including availability, integrity, and confidentiality where applicable.

1.1.3 Applications

This security profile considers substation automation functionality to serve three primary functions: system protection, system optimization, and system monitoring. These functions are considered in scope if performed by a device that may be considered in scope (i.e., delineated in this section). This includes automated and supervisory applications in both local and remote contexts. Specific functions that are considered in scope for this security profile include:

Table 1 – Substation Automation Functions in Scope for this Security Profile

Function	Purpose	Examples
System Protection	Personnel safety Equipment longevity Minimization of outage scope & duration	Protective relaying
System Control	System performance optimization (i.e., Volt/VAR) System reconfiguration	Elective operation of primary switchgear
		Automated response to non-critical system conditions
System Monitoring	Situational awareness Visibility of equipment condition Event forensics System planning Revenue generation / contractual performance obligations	Primary system measurement (e.g., voltage, current, phase angle…)
		Asset monitoring
		Fault / sequence-of-events records
		Metering

1.1.4 Legacy Equipment

In general, this security profile is written from a forward-looking perspective – that is, the perspective of "this is what is required to secure the functionality in question" without making compromises for legacy technology. The failure modes and risks identified in this document are associated with the functionality of the system – not the particular technological implementation – and therefore still apply to legacy equipment. For example, recommendations for protection functions between substations (i.e., transfer-trip) apply even if the function is implemented using

power-line carrier technology[2]. If a certain technological platform inhibits or precludes the implementation of some of the specified controls, the system implementer should examine the failure modes addressed by the recommended controls and document how the risks of these failure modes are mitigated by other means. In other words, if the system implementer cannot implement a recommended control, the burden is on the system implementer to make a case for how an alternate method is equally sufficient to mitigate the risk. Recommendations for other means of mitigating identified potential failures will likely be highly dependent on the specific legacy technology.

1.1.5 Explicit Exclusions

Local system maintenance (i.e., an engineer physically on-site) is out of scope for this security profile, however this document recommends that any engineering change requiring system-level testing prior to return-to-service be performed by qualified on-site engineers according to defined asset owner/operator procedures. Such on-site system maintenance procedures are considered out of scope for this profile.

The authors of this document are also not aware of available and proven technology that sufficiently mitigates the risks posed by the level of access and influence required to remotely initiate, complete, and close maintenance of substation equipment. Therefore this document does not cover the performance of maintenance from physically remote locations on in-scope substation equipment, and considers no use cases that would enable such actions.

Additionally, devices deployed inside the substation boundary for the sole purpose of facilitating communications between distribution assets and the enterprise *without integration into the substation automation systems* (e.g., co-located collectors, aggregators, or repeaters that communicate with residential or industrial meters as part of a stand-alone advanced metering system) are out of scope.

1.2 Approach

The procedure used to develop this security profile is shown in Figure 1. This procedure has five steps and, as illustrated below, these steps are not necessarily sequential and are in fact iterative in nature.

[2] Direct communications between substations are "in scope" regardless of communications path, and include Power Line Carrier (PLC) types of technologies. These direct communications represent a point where communications enter the substation, and making a scope exception for an entire class of technology goes against the standards of rigor for risk analysis used in generating this document. PLC technologies may be difficult to attack as of this writing, but as has been proven with other technologies, that can change rapidly if someone develops a novel means of injection. At that point the attacker would have a direct path into the most sensitive and important area of the protection and control system with presumed authentication and authorization. While obscurity can be a worthwhile layer of defense and should not be dismissed, this document does not endorse relying upon it as the only means of defense.

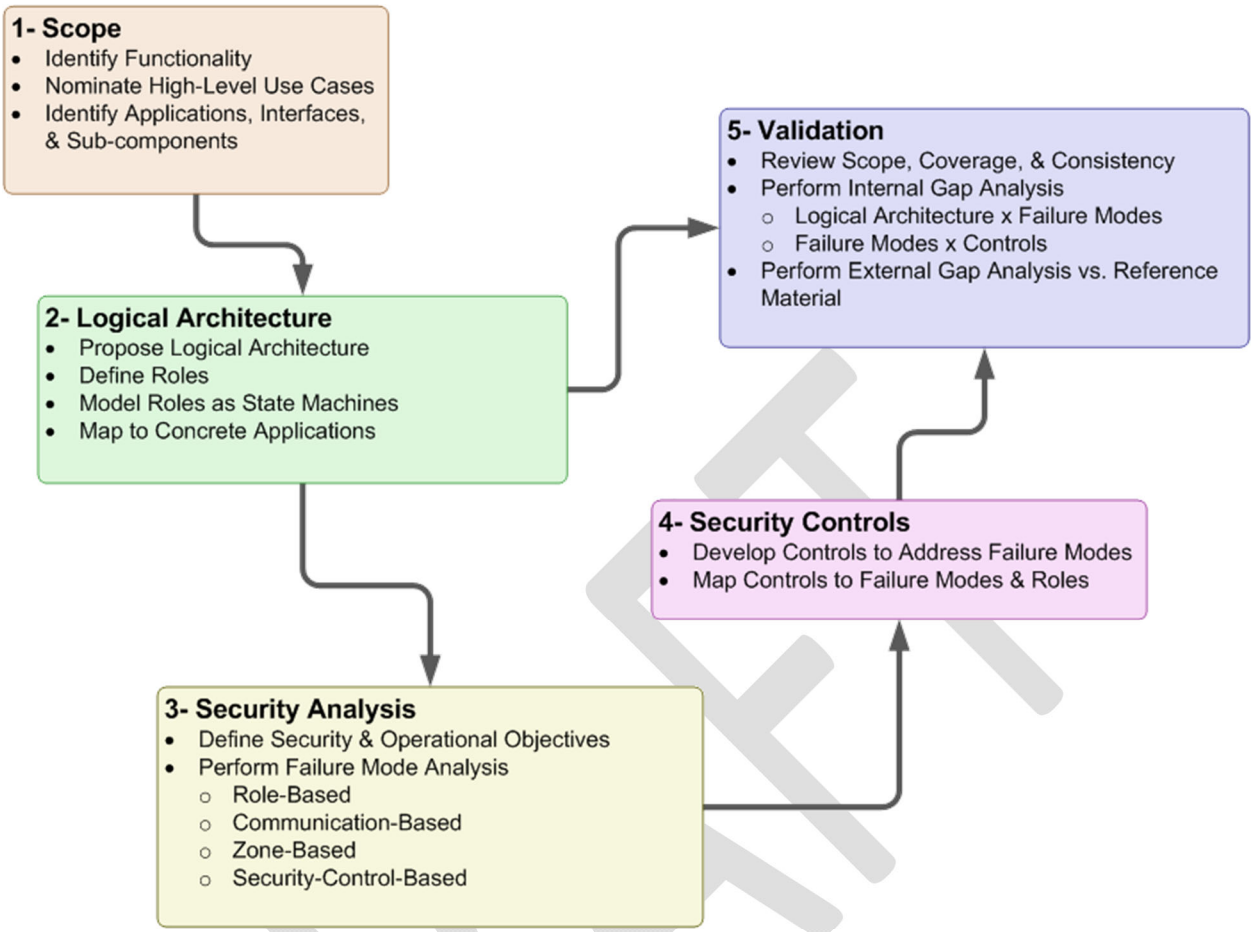

Figure 1 – Overview of Security Profile Development Approach

Steps 1 and 2, which are chiefly concerned with defining the scope of the profile, are repeated several times as the development team works with stakeholders to understand their needs. Steps 3 and 4 define the purpose of security in the system's operation and how security is realized. Steps 2 and 4 join in the final phases of the profile's development when the development team checks that the set of selected controls is complete and relevant. Step 5, which is concerned with validating the convergence of previous steps, proceeds in parallel with steps 3 and 4. The tasks within each step are summarized below:

1. *Define the scope of the security profile.* The first step is to decide what aspects of the system are to be included in the security profile. This step requires discussion with stakeholders, consideration of existing and planned systems that will fall within the scope of the profile, and the construction of a conceptual model of those systems that refines and clarifies the statement of scope. The conceptual model includes applications, subcomponents, and behavioral descriptions that define what uses of the system are addressed by the security profile and identifies the functions performed by the system that are the targets of the security guidance to be developed.

2. *Construct a logical architecture showing the relationships between roles and the behavior of each role.* The logical architecture defines a set of roles encompassing chunks of system functionality, delineates assumptions about how the roles communicate

with each other within the system as well as systems outside the scoping boundary, and describes the desired behavior of each role in terms of state machine models. The logical architecture also ties the conceptual model developed in step 1 above to architectures and concrete applications familiar to stakeholders.

3. *Analyze system needs from a security perspective.* The specific aims of the security profile are defined here in terms of the logical architecture from step 2. These aims include mission-level system objectives, as well as characteristics and capabilities of the system that are to be preserved by recommended security controls (and must be preserved as security controls are put into place). Each element of the logical architecture is then examined in light of the defined security and operational objectives to identify security related failure modes that may inhibit the operation of the system.
4. *Define the security controls.* New security controls are defined and/or existing controls from other security documents are referenced and possibly refined to meet the security objectives defined in step 3. Controls are bound back to individual roles through the failure modes, resulting in a defined set of controls each role is expected to implement.
5. *Validation.* This step involves performing a collection of validation checks, such as ensuring that the selected controls are complete with respect to the identified failure modes (i.e., that failure mode is adequately addressed by recommended security controls) and that there are no superfluous controls (i.e., that each recommended control provides unique mitigation for some failure mode that it addresses). Each control is mapped to the set of failure modes that it addresses, and each failure mode is mapped to the set of security controls that collectively mitigate it.

The products of these steps are the artifacts shown in Figure 2.

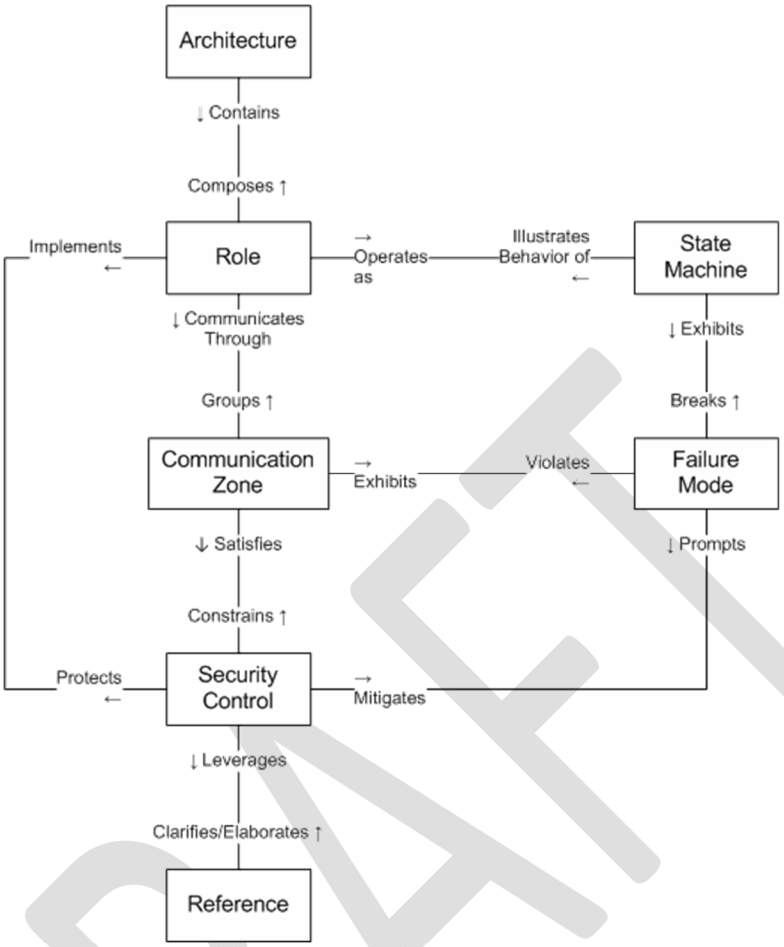

Figure 2 – Substation Automation Security Profile Artifact Relationships

The individual state machines provide a detailed view of the activities that are considered within the scope of the profile. Each state machine illustrates the behavior of a specific role, and that role is responsible for the security controls that mitigate potential failure modes of the state machine. These potential failure modes are identified in step 3 above by considering how the state machines may fail and, consequently, how the failure mode might prevent the system or role from successfully carrying out its objective. Each identified potential failure mode prompts the development of one or more controls to mitigate it.

Though most controls are assigned to specific roles, some failure modes span two or more roles and therefore imply a failure of the communication network that is used by the roles to coordinate their actions. These failure modes are mitigated by network-oriented controls that focus specifically on protecting the movement of information across and within communication zones. Whenever a control is derived from sources identified in step 4, that source (e.g., a reference to a specific NIST IR 7628 requirement number) is noted.

1.3 Audience & Recommended Use

The primary audience for this document consists of organizations that are developing or implementing solutions requiring or providing substation automation functionality as described

in Section 1.1. This document is written for system owners, system implementers, and security engineers with at least a year of experience in securing electric utility field operations. The user is assumed to be experienced at information asset risk estimation. The user is further assumed to be knowledgeable in applying security requirements and guidance. The user will ultimately leverage this profile by reference as the specific set of security controls that must be implemented by substation automation components and systems, above and beyond organizational-level requirements as specified in the NIST IR 7628 and other recommended best practice documents for cyber security as listed in Section 4.1.

Additional sections below discuss how the document should be used by various stakeholders. The profile development approach (summarized in Section 1.2) guides the reader through the process used in this document for determining controls required to address given failure modes associated with the roles and communications infrastructure (i.e., specific undesirable deviations from the functionality that the roles and network infrastructure are expected to implement), thereby providing traceability and justification for each of the controls selected.

1.3.1 Electric Utility

An electric utility may use this document to help achieve multiple security objectives for their organization through activities such as:

1. developing security requirements for substation automation technology procurement activities,
2. configuring and operating substation automation systems, and systems built on substation automation technology, or
3. evaluating planned or deployed substation automation solutions.

In some cases, a utility will not make use of all functionality described in the logical architecture, which may obviate the requirements for certain controls. The tables within the document can be used to determine security controls needed for a utility's environment and provide traceability and justification for the design requirements and control selection. In other cases, an organization may identify an alternative (mitigating) control that makes a required control unnecessary, but the utility should be sure the proposed alternative addresses all the same failure modes and should perform a risk analysis to confirm the adequacy of the alternative control.

1.3.2 Substation Automation (and Derivative Technology) Vendors

Vendors may use this document to incorporate security controls needed for the development of substation automation products as well as solutions built upon or derived from substation automation technology. This document provides enough requirement detail to allow a vendor to begin design activities, but avoids prescription that would thwart innovation or drive toward specific implementations. The reference architecture and state machines also offer tools for understanding substation automation applications in an abstract sense.

1.3.3 Research and Engineering Community

This security profile is intended to be suitable for review, scientific and engineering analysis, evolution, and improvement by the broader research and engineering community through the

profile's presentation of details behind the analyses, such as the complete UML state-machine models for each of the in-scope substation automation roles and the explicit linkage between failure modes and recommended controls.

2 Functional Analysis

The purpose of the functional analysis is to define a clear picture of the scope, architecture, and functionality of substation automation systems, as addressed by this security profile. The real-world specific performance of substation automation system functions varies in terms of function, scope, and technology from device to device and component to component among different system offerings and deployments. However, this profile approaches the problem by defining a set of abstract roles that capture essential functionality that may be realized through a variety of implementations. For example, the functions of the Substation User Interface role may be performed by a stand-alone component, or rolled into a platform that also performs many of the remote access functions as defined in the Proxy role. Conversely, some implementations may have the decision-making functionality of the Control Authority role distributed among several devices that also implement the Substation User Interface, the Proxy, and possibly even a Control Application. Regardless, this profile defines roles in such a way that the logical architecture and state machine models may be used to represent a wide variety of real-world implementations.

By way of background, the following steps were performed in the functional analysis:

1. Interview domain experts (utility and vendor) and review publicly available resources to understand existing and planned substation automation systems and functions.
2. Define abstract roles that characterize elements of substation automation systems concisely. Roles are neutral to implementation and vendor, and capture the essence of common functionality without the details of particular applications. The logical architecture describing the relationships among the roles (topologically) is presented in Section 2.1. Definitions of the roles are presented in Section 2.2
3. Draft state machines describing intended individual role functionality and behavior. The state machines are modular in nature, which allows organizations to determine which

roles are relevant to their deployments. They also capture raw functionality, without the inclusion of security controls, which ensures that no pre-existing security controls are assumed and allows different controls to be applied without bias. The resulting state machine models are presented in Section 2.4.

4. Validate the roles, communications topology, and state machines by ensuring they adequately describe common real-world implementations. The mapping between roles and real world implementations is presented in Section 2.3.

The security recommendations found in this document are defined in terms of the logical architecture and its constituent roles, both of which are defined in this section. The logical architecture includes some elements that are outside the scope of this profile; however, each such element interacts with substation automation systems in important ways and so these elements are included as context. Specifically, the following roles are in-scope for this profile, and security recommendations are provided for each in Section 4:

- Proxy
- Substation User Interface
- Substation Information Repository
- Substation Control Authority
- Actuator
- Sensor
- Protection Application
- Control Application
- Monitoring Application

As part of a system for substation automation, the above roles interact with systems for distribution, business management, and for remote operation of the substation. Systems that are external to the substation are included in the logical architecture for the substation automation system, but the security of these external systems is not within the scope of the profile. The only exception to this rule is when the substation under consideration communicates with another substation (designated in the logical architecture as "Other Substation"). The operation of this remote substation is also within the scope of this profile to the extent that it implements functions for substation automation; therefore communications between substations are within the scope of this profile.

2.1 Logical Architecture

The roles defined in this profile are *abstract* or *logical* roles; that is, each role does not necessarily map one-to-one with a device or system. It is possible for a device to implement the functionality of multiple roles. However, it is also possible for the functionality of one role to be split among more than one device. As such, this document focuses on defining the roles, their functionality, and ultimately the security controls each role must implement at this abstract level

and leaves the task of mapping roles to specific products, devices, or systems to those developing or procuring these elements (see Section 2.3 for more information). The essential roles involved in substation automation systems are shown in Figure 4, Figure 5, Figure 6, and Figure 6.

2.1.1 Communications Architecture

For the purposes of discussing communication among roles, this profile abstracts the substation communication architecture to the use of five networks (or network segments). Each segment is identified here to help the reader relate to common substation architecture, and to provide context for the types of connections used by communication between roles. Network segment labels and descriptions are provided for convenience, as this profile provides guidance based on communications between specific roles, communications in general (regardless of network segment), and communications within "zones" (introduced in Section 2.5), but not based on particular network types.

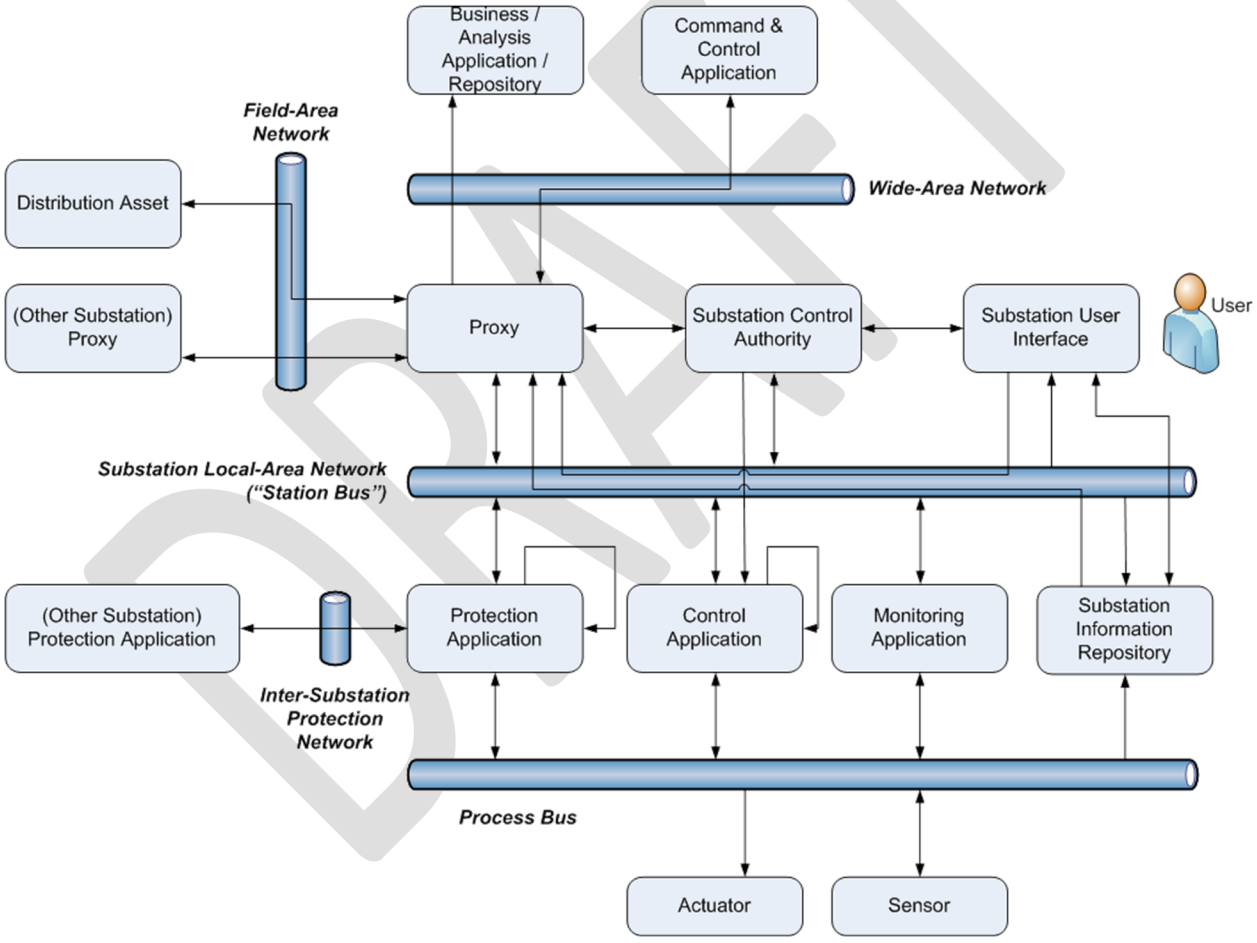

Figure 3 – Logical Architecture – Networks

The network segments identified in the drawing above may be described as follows:

1. **Field Network**: The Field Network connects all of the assets that monitor or directly interact with the electric power system but physically reside outside of substation and within the distribution network. Field network is also utilized to connect to other

substations for the purpose of exchanging control and information messages (e.g., distributed control applications). The Field Network is typically private and owned by utility. Typical assets that reside on this network include switches, fuses, switched capacitor banks, reclosers, etc.

2. **Wide Area Network:** The WAN is typically a public network (non-utility owned) and connects the enterprise wide applications to the substation assets. This network transmits the substation monitoring information to the utility control center in order to provide overall power grid situational awareness. Remote command and control messages are also sent from the utility control center to the substation through this network.
3. **Inter-Substation Protection Network:** The ISPN connects protection applications between substations. This network is typically dedicated media (e.g., microwave, fiber, or power-line carrier) that transmits a specific set of protection signals like direct transfer trip (DTT), remote inter-locking, and other elements of protection schemes involving more than one substation. The ISPN has the most stringent latency and quality of service requirements for a geographically dispersed electric utility network.
4. **Process Bus:** The Process Bus connects the substation applications (protection, monitoring, control, and repository) to the power system sensors and actuators (CT/PT, relays, etc.). Implementation of the process bus ranges from copper twisted pair (analog measurements) to digital networks (serial multidrop point-to-point network). Digital implementations of the Process Buss tend to have extreme low latency requirements.
5. **Station Bus**: The Station Bus connects substation-level operations (substation gateway, HMI, and/or control authority) to various substation-specific applications such as protection, control, and monitoring as well as things like the information repository, and also facilitates the majority of communications between those same substation-specific applications. Substation-level supervisory control messages are sent across this network. The Station Bus is a typically a point-to-multi-point (e.g., Ethernet-like) network.

Lines between roles represent interactions with arrows indicating the direction of primary interaction. The mechanics of negotiating and managing the information flow are not represented. For example, acknowledgements and protocol-specific exchanges are not shown, nor are exceptional messages such as error reports. Arrows looping back to the same role indicate where one instance of a role may communicate with another instance of the same role (i.e., role instance multiplicity). Multiplicities between roles are not depicted, but are generally many-to-many. For example, a device serving the Monitoring Application role may receive data from multiple Sensors and may also interact with multiple Control Applications. Arrows connecting to or from a network segment indicate the role communicates with all other roles connected to that segment with a corresponding arrow (e.g., the Substation Information Repository may receive information from the Proxy, the Control Authority, a Protection Application, a Control Application, a Monitoring Application, and/or a Sensor). Arrows crossing through a network segment indicate the information flow may use the network segment for transport, but is exclusive between the connected roles (e.g., the Substation Information Repository sends information to the Proxy, but not directly to any other roles connected to the Substation LAN). All software/hardware roles are assumed to have some inherent communications ability (i.e., distinct communications elements such as network interface cards associated with each software/hardware role are not modeled).

As with the concept of roles, each of these network segments may or may not map one-to-one with a distinct physical or logical network segment in an actual substation, and not all may be present in a given instance. Specifically, some implementations may use a single network to serve the purpose of more than one network as defined above. One example might be that the Inter-Substation Protection Network may use the same physical infrastructure as either the Field-Area Network or the Wide-Area Network. Another example might be that the Process Bus is either not physically implemented as a network (i.e., Actuators and Sensors hardwired in to relays that serve the Protection Application, Control Application, and/or Monitoring Application roles), or that the Process Bus is implemented on the same physical infrastructure as the Station Bus.

For the purposes of analyzing communications and their potential failure modes, this document decomposes communications among roles into three categories – inform, operate, and configure – as depicted in the following diagrams.

2.1.2 "Inform" Communications

Communications that constitute a notification of a change in condition or circumstance are labeled as "Inform" data flows. Any decisions about required actions resulting from "Inform" data flows reside with recipient.

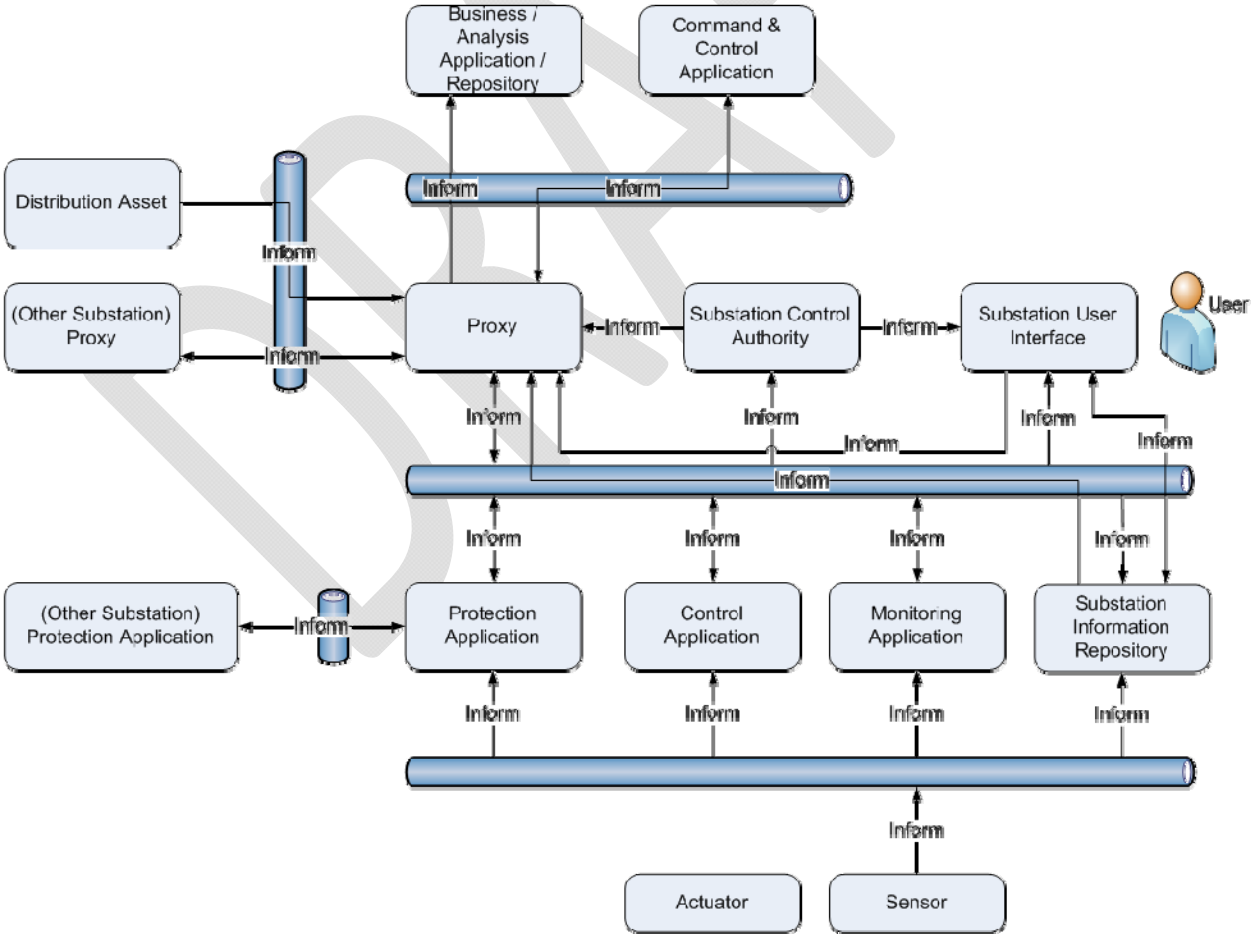

Figure 4 – Logical Architecture – Inform

Examples of "Inform" data flows include sensor readings, alarms, notifications, and status updates or changes.

2.1.3 "Operate" Communications

Instructions or direct requests to change the state of the physical electrical system (i.e., configuration of the power system) are considered "Operate" data flows.

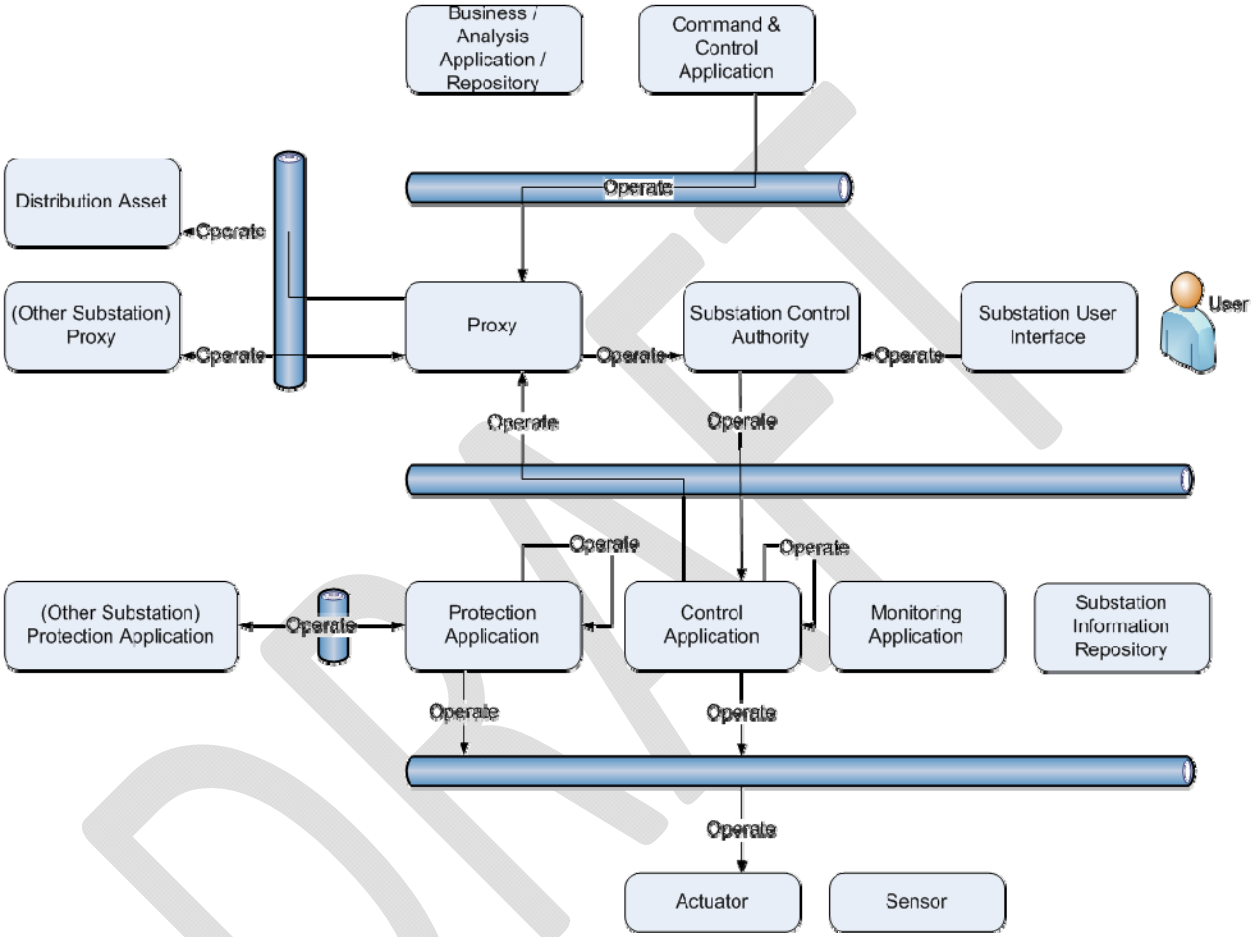

Figure 5 – Logical Architecture – Operate

Examples of "Operate" data flows include commands to trip a breaker, open/close a switch, or change the position of a load tap changer.

2.1.4 *"Config" Communications*

Behavior changes that do not require system-level testing prior to return-to-service are considered "Config" (short for "Configure") data flows.

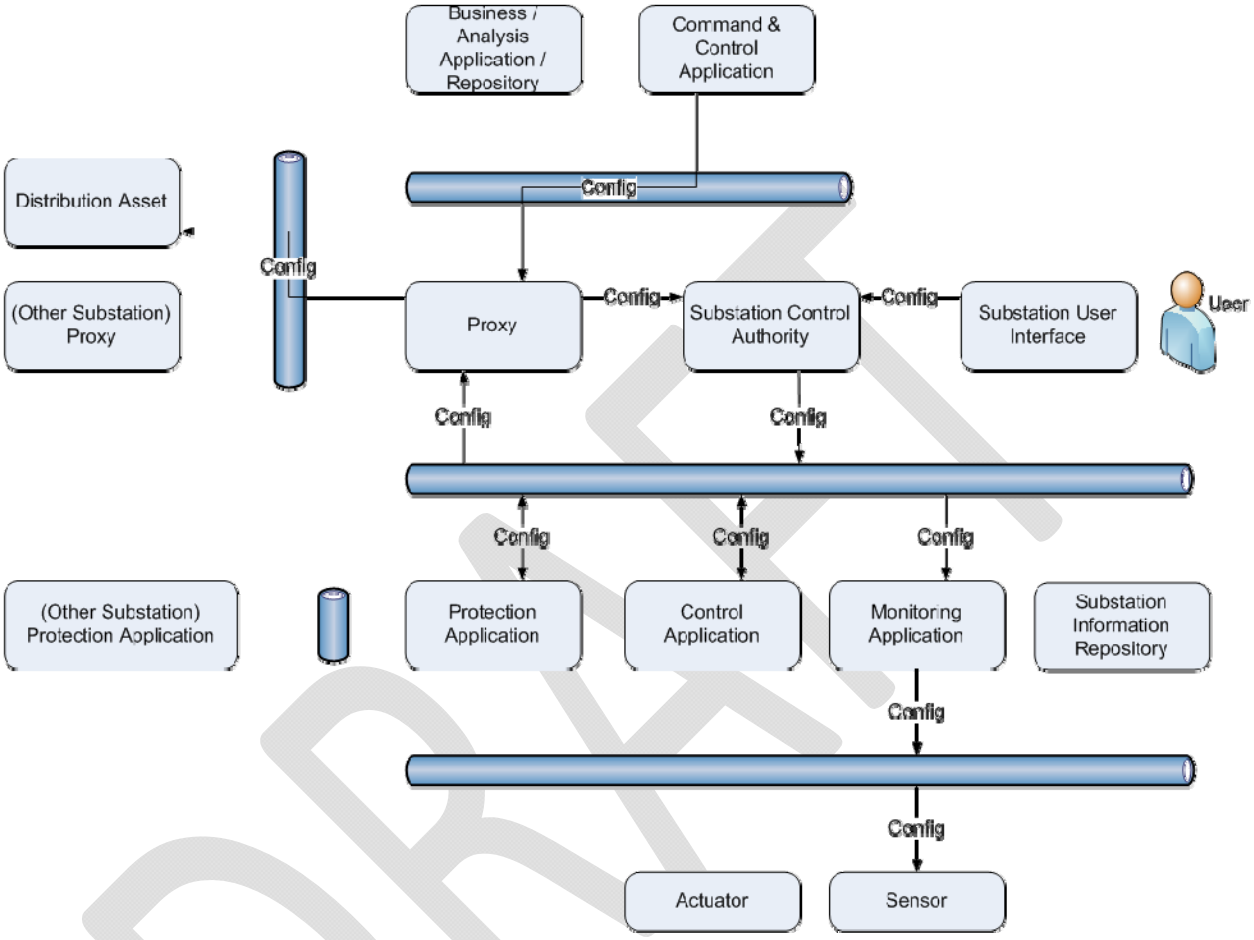

Figure 6 – Logical Architecture – Config

Examples of "Config" data flows include changes to the operational mode of the substation ("local" or "remote") or equipment (placement in "test"), setpoints, relay settings changes, time synchronization, and sampling rate.

2.2 Role Definitions

All roles are defined in the following sub-sections.

2.2.1 *Proxy*

This role acts as an intermediary for requests from clients (e.g., applications) requesting data or issuing control commands to roles with which they have no direct interaction. It may provide additional functionality including:

- Protocol Conversion

- Data Concentration
- Terminal Services

2.2.2 Substation User Interface

This role allows Users to interact with the substation automation system or its components. A user interface can be at the system level or a component level and provides a User with:

- Input to manipulate the system or its components
- Output to monitor the system or component and make operational decisions.

2.2.3 Substation Information Repository

This role represents a secondary store of information that is used as a unified resource for any role within the substation automation system needing data. It is mainly used to provide a secondary location for data which is no longer needed or available in the primary storage location such as an Application or Sensor.

2.2.4 Substation Control Authority

This role arbitrates and coordinates the dispatch of OPERATE and CONFIG messages originating from the remote Command and Control application(s) and/or local user interface(s) to applications within the substation automation system. Multiple instances of a Control Authority role may be present within a substation automation system at both the system and component levels. A Control Authority is only used to govern OPERATE and CONFIG messages sent to Actuators and Applications and does not participate in requests to retrieve data from Sensors or Applications.

2.2.5 Actuator

This role encompasses the ability to take action on the physical electric system (e.g., trip a breaker). Actuators do not detect existing conditions or make decisions; they execute the actions they have been directed to take.

NOTE: The position of equipment operated by an Actuator would be monitored and reported by a Sensor, not the Actuator.

2.2.6 Sensor

This role encompasses the ability to gather data about the physical electric system, including equipment that may be directly connected by an electrical signal. Sensors only detect and forward information; they do not make decisions or take actions.

2.2.7 Protection Application

This role represents the responsibility to take an automatic and prompt action to protect personnel and power system equipment. Typically, these applications focus on removing from service a power system element which is in a faulted state or starting to operate in any abnormal

manner that poses immediate risk to equipment or people. A secondary goal of these applications is to minimize the impact to power system reliability as a result of these protection actions.

Examples of Protection Applications include:

- Power System Protection - (distance, over voltage, over current, under/over frequency, ground detect, differential, breaker failure, unbalance, thermal, pressure, etc.)

2.2.8 Control Application

This role represents the capability to make an automated or manually initiated decision based on local and/or remote inputs. These decisions can result in the output of a control action directed internally to the control application (e.g., application behavior modification) or externally to an actuator or another application. These applications are generally aimed at optimizing safety (e.g., pre-emptive configuration for maintenance), performance, and cost-effective operation of the local power system elements.

Examples of Control Applications include:

- Sync check
- Reclosing
- Bay control
- Load Tap Changer Control
- Capacitor Bank Control

2.2.9 Monitoring Application

This role collects and/or presents power system data to one or more Applications. It may manipulate data by calculating values from actual data and serves as the primary store for collected and processed data.

Examples of Monitoring Applications include:

- Merging Unit
- Meter/Digital Transducer
- Power Quality Monitor
- Digital Fault Recorder
- Phasor Measurement Unit
- Circuit Breaker Monitor
- Transformer Monitor

2.2.10 Command and Control Application

This role represents one or more applications which are utilized for real-time operation of the power system within a utility control center environment. In addition to retrieving data from the SA system, this role may initiate changes to the power system or SA configuration.

NOTE: The connection to the Command and Control Application is an external interface to the SA system. While it interacts with roles inside the substation, the Command and Control Application is not within the scope of this Security Profile.

2.2.11 Business Analysis Application/Repository

This role represents one or more Business Analysis Applications or Information Repositories which are typically utilized for non-critical analysis of power system performance outside of the utility control center environment. This role only retrieves data from the SA system and does not send OPERATE or CONFIG messages.

NOTE: The connection to the Business Analysis Application/Repository is an external interface to the SA system. While the Business Analysis Application/Repository role interacts with roles inside the substation, the role itself is out of scope for development of controls in this document.

2.2.12 Distribution Asset

This role represents a device which is associated with a power system asset supporting the distribution of electrical power and is located outside the confines of the substation physical security measures. This role is an aggregate representation and may contain one or more of the roles: Sensor, Actuator, Control Application, Monitoring Application, and Control Authority. These devices typically have weak physical security due to their physical location.

Examples of Distribution Assets include:

- Switch controller
- Recloser controller
- Cap bank controller
- Voltage regulator controller
- Remote Terminal Unit

NOTE: The connection to the Distribution Asset role is an external interface to the SA system. While the Distribution Asset role interacts with roles inside the substation, the role itself is out of scope for development of controls in this document; however, security recommendations for these assets are covered under the Security Profile for Distribution Management[3].

[3] UCA International Users Group (UCAIug) Smart Grid Security Working Group, Security Profile for Distribution Management v1.0, February 2012. Available at: http://osgug.ucaiug.org/utilisec/Shared%20Documents/Distribution%20Management%20Security%20Profile/DM%20Security%20Profile%20-%20v1_0%20-%2020120220.docx.

2.3 Role Mappings

This section demonstrates several examples of how the logical architecture presented in Section 2.1 and roles presented in Section 2.2 can be realized in different deployment settings. These examples are not intended to be exhaustive, but are meant to demonstrate several common implementations and how they relate to the logical architecture and roles used in this document.

2.3.1 Example Substation Architecture

Figure 7 is an example of the types of devices (not roles) one might find in a substation. This diagram is illustrative only, and not meant to imply any specific configuration or assembly. Subsequent sections describe the roles these devices might implement. There is no absolute rule regarding what roles a given device (such as a substation gateway) might implement, but the following subsections provide some realistic examples.

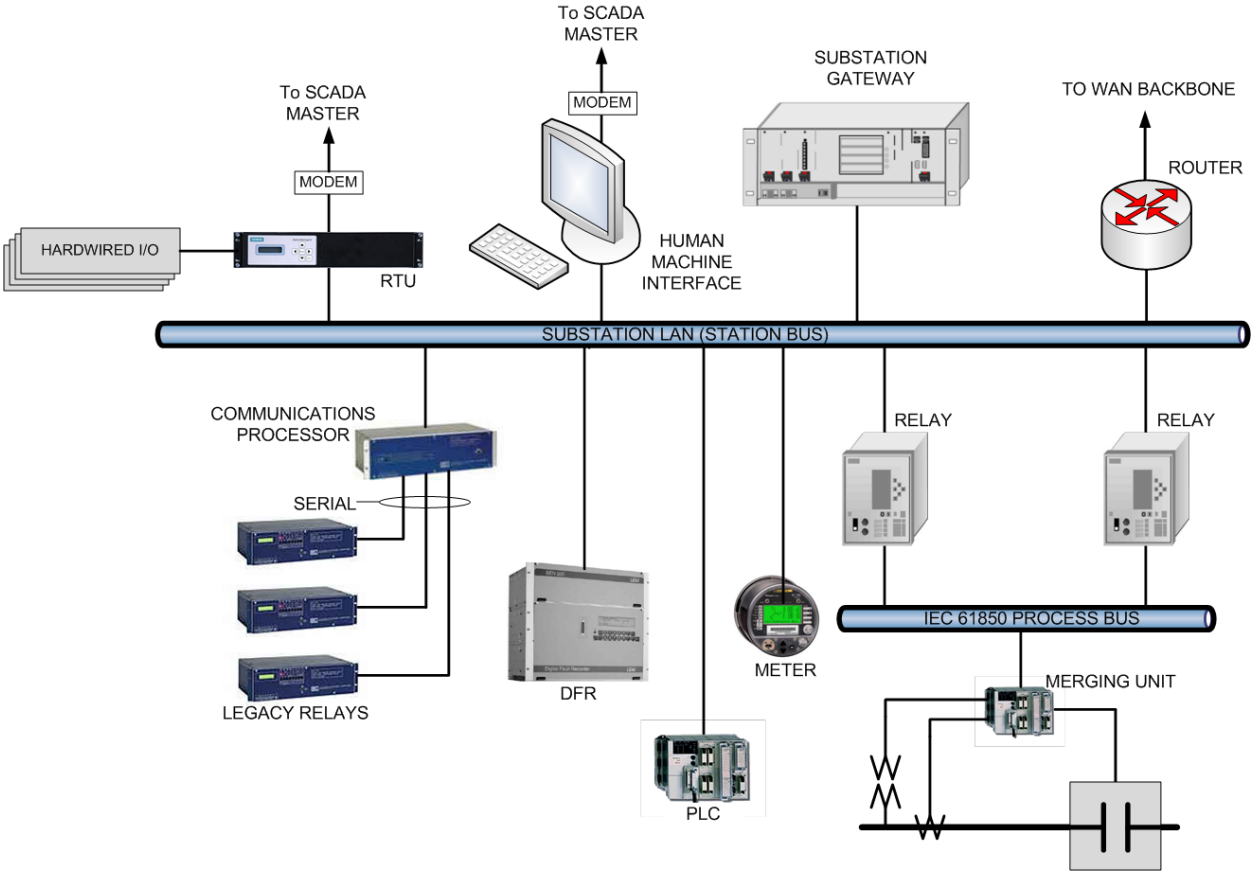

Figure 7 – Example Substation Architecture

2.3.2 *Protection Relay and Merging Unit*

Figure 8 illustrates some of the roles one might find in a protection relay as well as a merging unit. For example, a relay might implement the five roles illustrated to the upper right of the drawing. This relay might be a piece of equipment that implements the Protection Application, Monitoring Application, and Control Application roles by providing protection, monitoring, and control logic for a circuit breaker. The device could also implement the Actuator role if it were equipped with wired connections to the physical breaker, or a Sensor role if it were connected directly to current and voltage transformers.

A merging unit might implement the two roles illustrated in the lower right of the drawing. It can implement the Sensor role by providing conversion of current and voltage (or other analog signals) to formatted digital output to be shared by the process bus. The merging unit might also implement the Actuator role by offering digital control of a piece of physical equipment such as a motor-operated disconnect switch.

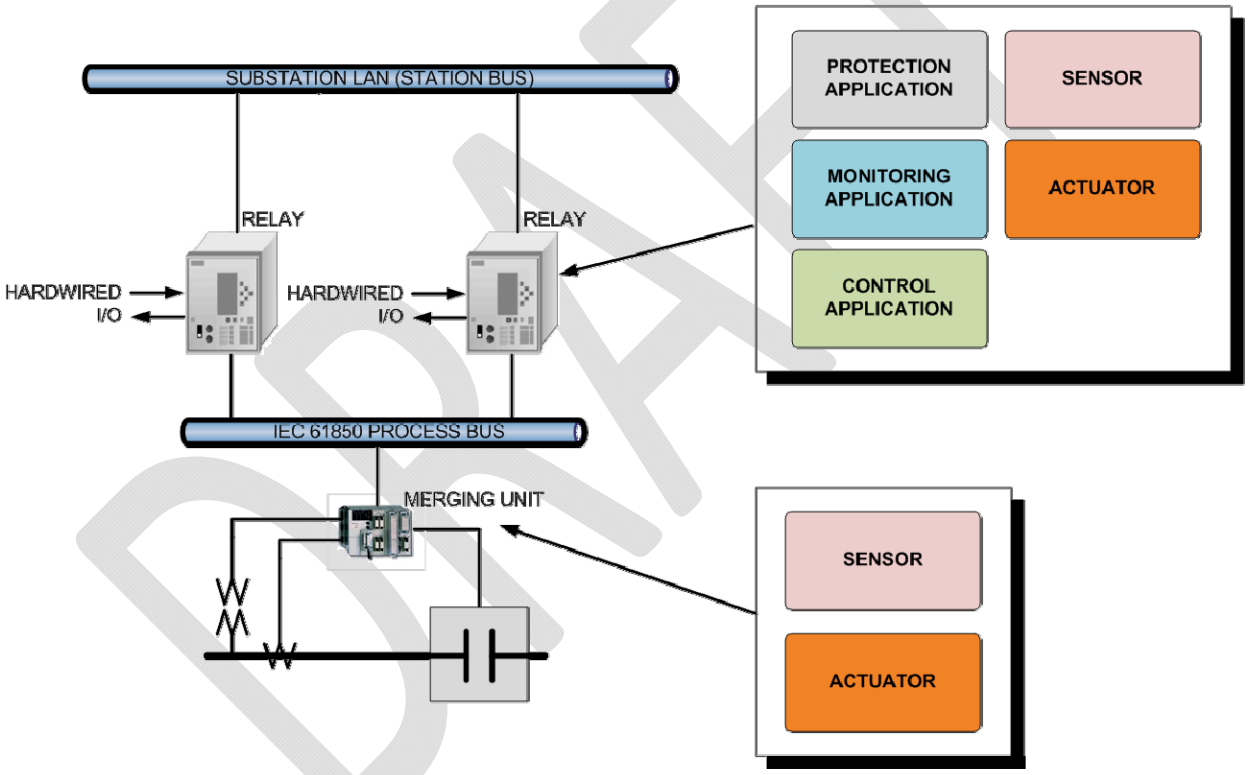

Figure 8 – Protection Relay and Merging Unit

2.3.3 *Communications Processor*

Figure 9 illustrates the roles that a communications processor might implement. A communications processor translates various protocol formats received from end devices like Relays and transmits the information to the Station Bus implementing the role of a Proxy. A communications processor might also implement the Control Application role by hosting the control logic to read the input and generate control actions to the Actuator.

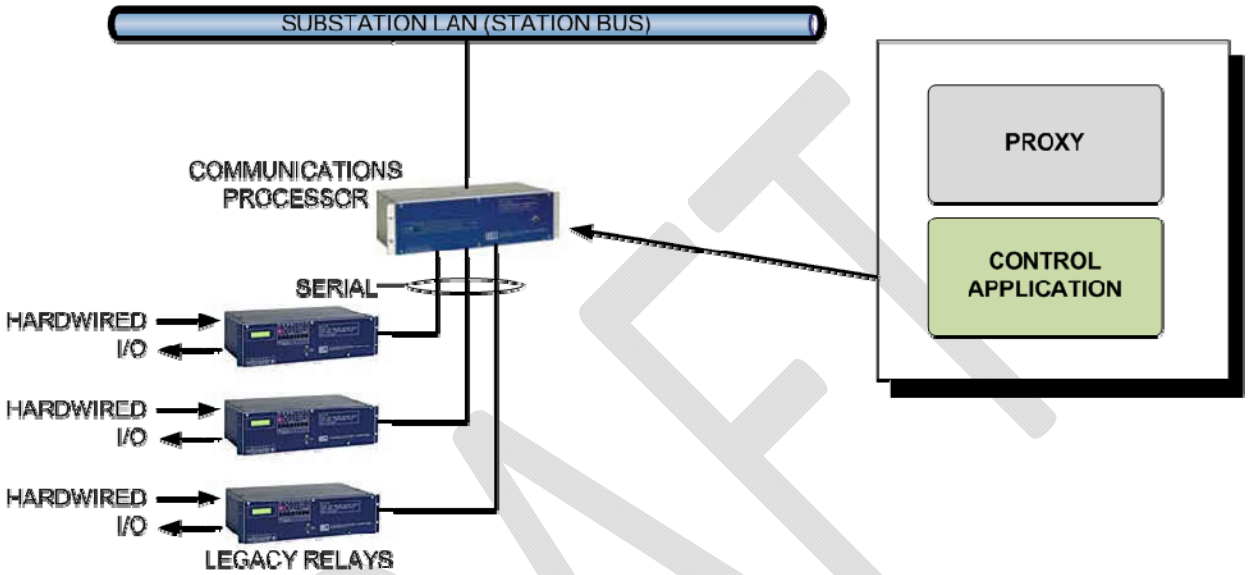

Figure 9 – Communications Processor

2.3.4 Digital Fault Recorder and Meter

Figure 10 illustrates the roles that can exist in a digital fault recorder (DFR) and a meter. A digital fault recorder stores the time-domain digital record of state of electric grid measurements (voltage, frequency, harmonics, fault current, etc.) usually triggered by power system disturbances. On the other hand, the meter consists of the current transformer (CT) and potential transformer (PT) that physically monitor the electric grid along with signal processing applications to digitize the data (sampled values).

The meter might implement the roles Sensor and Monitoring Application, and could even generate event triggers to a DFR, whereas a DFR unit might implement the Monitoring Application and Substation Information Repository roles. In either a DFR or a meter, the Monitoring Application interfaces with the Sensor to observe events in the electric grid and adaptively determines configurations like sampling rate, etc. The DFR also implements the Substation Information Repository role to archive the data for post-event analysis applications. The meter will also store some amount of the data it reads on-board; but this would be the primary location for a limited amount of data, and therefore not typically represent an implementation of the Substation Information Repository.

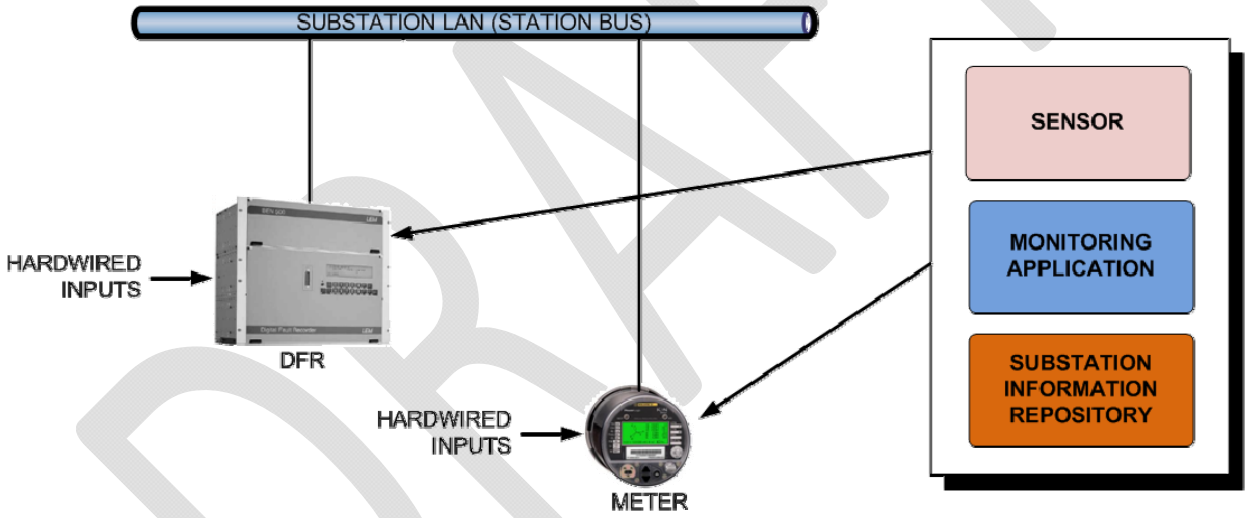

Figure 10 – Digital Fault Recorder and Meter

2.3.5 *Human Machine Interface*

Figure 11 illustrates roles that can be associated with a human machine interface (HMI). In its simplest form, the HMI provides a means for a local user to interact with the substation automation system (Substation User Interface role). In other cases, additional functions can be hosted as well on the HMI, such as an interface to a Command and Control Application role (via the Proxy role), arbitration between two or more valid controlling applications with which it interfaces (Substation Control Authority role), automated or manually initiated control logic (Control Application role), or providing information that has been interpreted from multiple sources within the SA system (Monitoring Application role) to the User or connected applications.

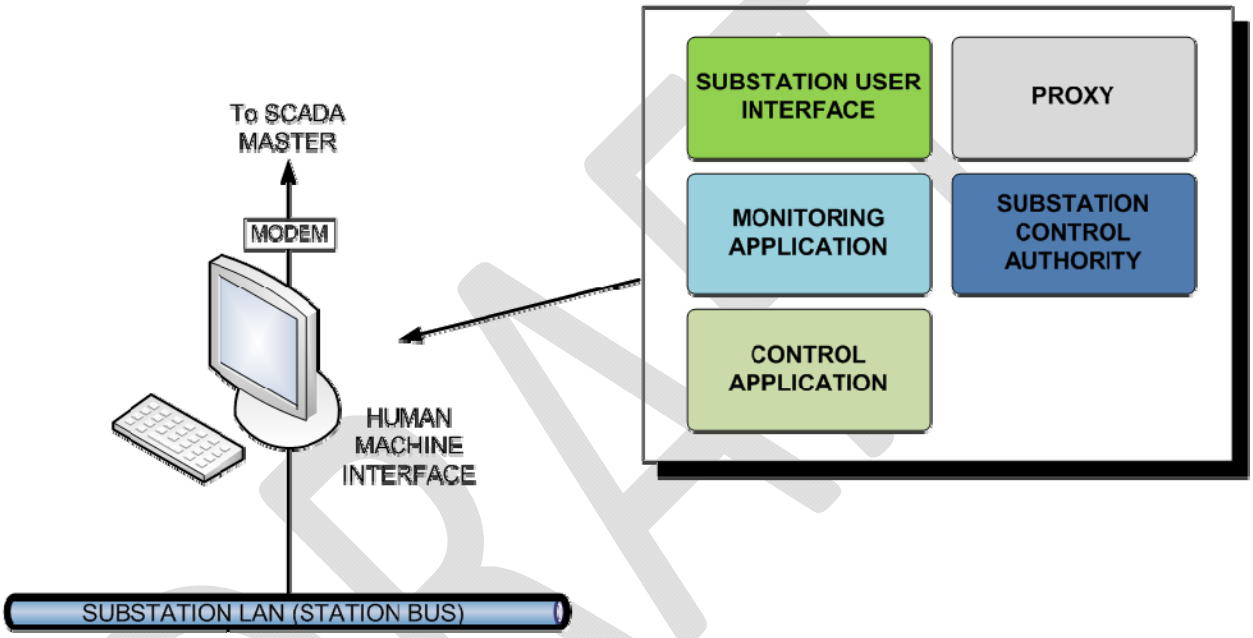

Figure 11 – Human Machine Interface

2.3.6 *Substation Gateway*

Figure 12 outlines how roles can be mapped to a substation gateway. Typically, the substation gateway is implemented to serve as an interface for external, non-protection applications (Proxy role). In addition to the Proxy role however, some implementations of a substation gateway may provide functionality such as arbitrating between two or more valid controlling applications with which it interfaces (Substation Control Authority role), automatically or manually initiating control logic (Control Application role), providing information that has been interpreted from multiple sources within the SA system to connected applications (Monitoring Application role), or providing a persistent store for information which has been offloaded from local applications or sensors for consumption by external applications (Substation Information Repository role).

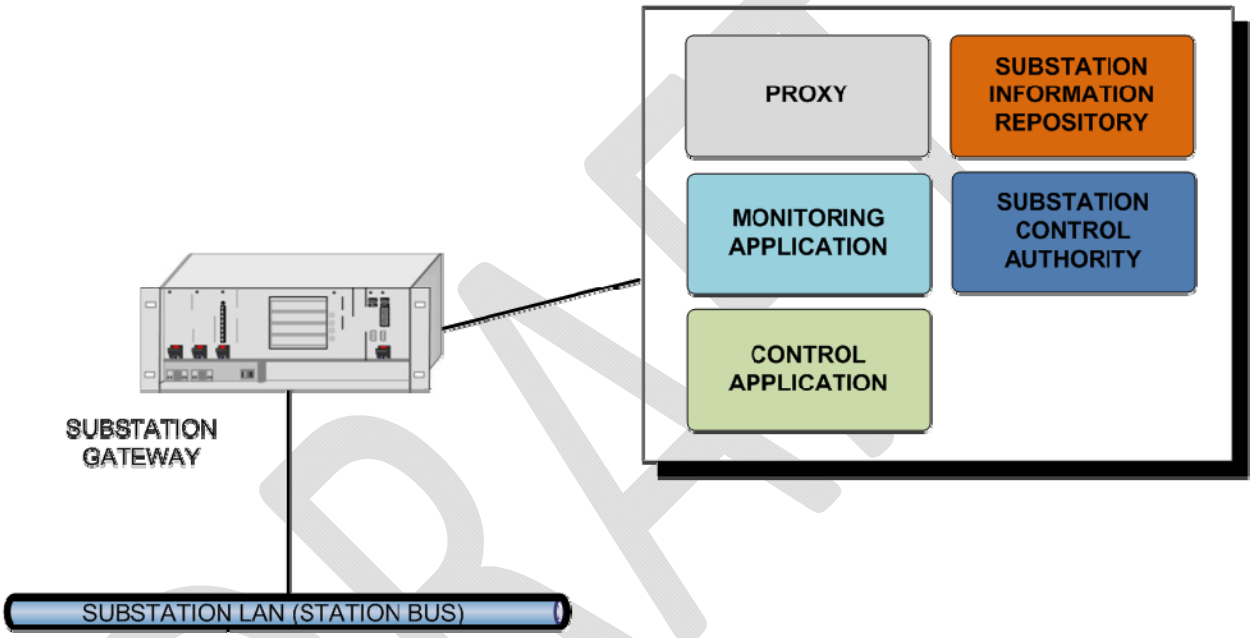

Figure 12 – Substation Gateway

2.3.7 *Remote Terminal Unit (RTU)*

Figure 13 outlines how roles can be mapped to a remote terminal unit (RTU). Typically, the RTU is implemented to serve as an interface for external Command and Control Application roles (via the Proxy role). In addition to the Proxy role however, some implementations of an RTU may provide functionality such as arbitrating between two or more valid Command and Control Application roles with which it interfaces (Substation Control Authority role), automatically or manually initiating control logic (Control Application role), or interfacing with physical equipment if equipped with traditional hardwired input/output modules (Sensor and Actuator roles).

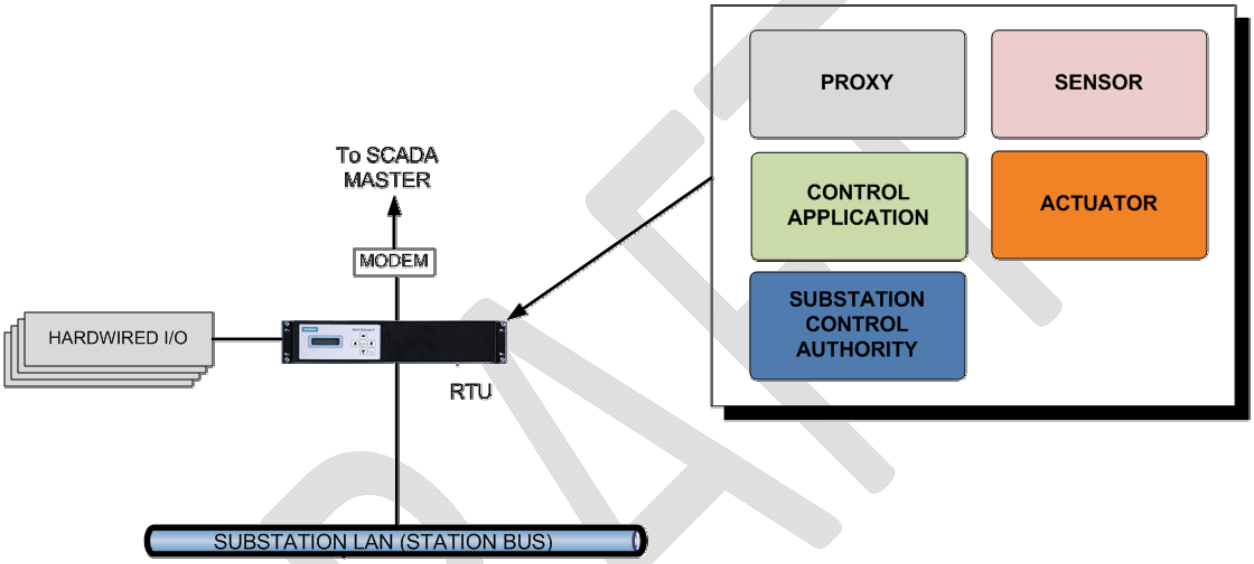

Figure 13 – Remote Terminal Unit (RTU)

2.3.8 Programmable Logic Controller (PLC)

Figure 14 illustrates the roles performed by a programmable logic controller (PLC). A PLC consists of hardwired input and output terminals that can be connected to a Sensor or an Actuator, although sometimes the Actuator is actually part of the PLC (e.g., programmable logic relay). The PLC can also interface with the Sensor for configuration and data acquisition (Monitoring Application role), and may implement the logic that generates outputs to the Actuator based on the inputs (Control Application role). The PLC may also implement a current transformer (CT) and potential transformer (PT) to observe the current and voltage on the electric grid (Sensor role).

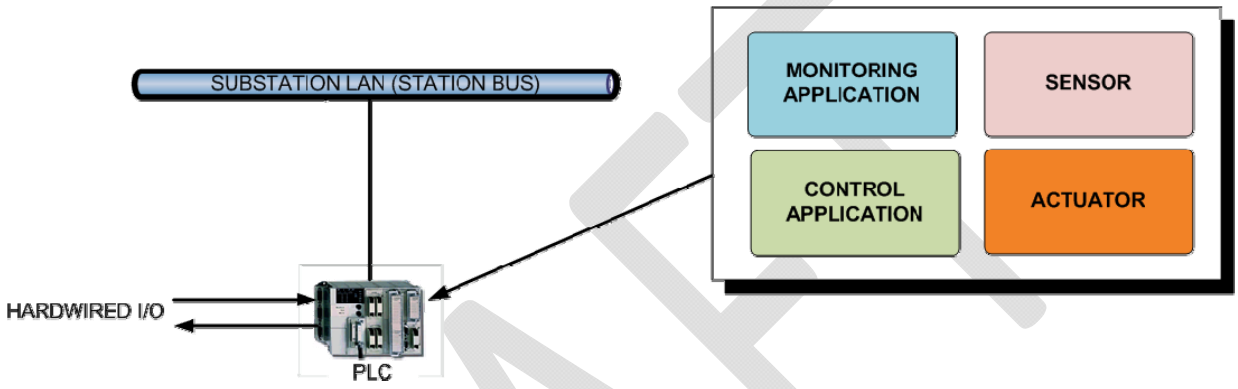

Figure 14 – Programmable Logic Controller

2.4 State Machines

This section contains state machine models for each of the in-scope roles. Each model describes the behavior that a given role will exhibit during operations. While a use case shows a particular portion of behavior of a collection of roles, a state machine shows all possible behaviors of a particular role. As such, these role-centric models focus on internal behavior, showing different activities a role would undertake, in what order, and as triggered by what stimuli. Interactions with other roles are typically shown in two ways—sending and receiving messages.

The syntax and semantics of the state machines found in this profile are those of UML state machines. A brief introduction follows:

- Each role starts in an initial state, represented by a solid black circle.
- States are shown as large rounded rectangles. Each state has a label in the diagram, and is further elaborated in notes following the diagram. The notes describe activities that occur within that state. Activities include things like performing some calculation, sending a message to another role, or setting a timer. Activities are described informally in text.
- Transitions are shown as labeled arrows between states. Each label that is surrounded by square braces is called a guard condition. A guard condition is a Boolean condition that indicates the circumstances under which that transition will be taken. For example, a guard "[operate message received]" will only be taken if an operate message has been received.

- Transitions are only evaluated when all processing within a state has been completed; they do not indicate any kind of interrupt. Additionally, each state machine has an implicit message queue. No separate process is shown that reads messages from a socket and fills this queue; the means by which such a queue is maintained is considered an implementation detail.

The state machines in this document describe core, common behavior across substation automation systems. Individual products may include behavior beyond what is presented here (e.g., additional logging), but all products should engage in this behavior. The security guidance in this document is based on this common behavior. Further, these state machines do *not* include security controls, such as the use of authentication or encryption. This avoids any bias or predetermination of what security controls are needed. Security controls and their mapping to the roles are found in Section 3.3.4.

2.4.1 Actuator State Machine

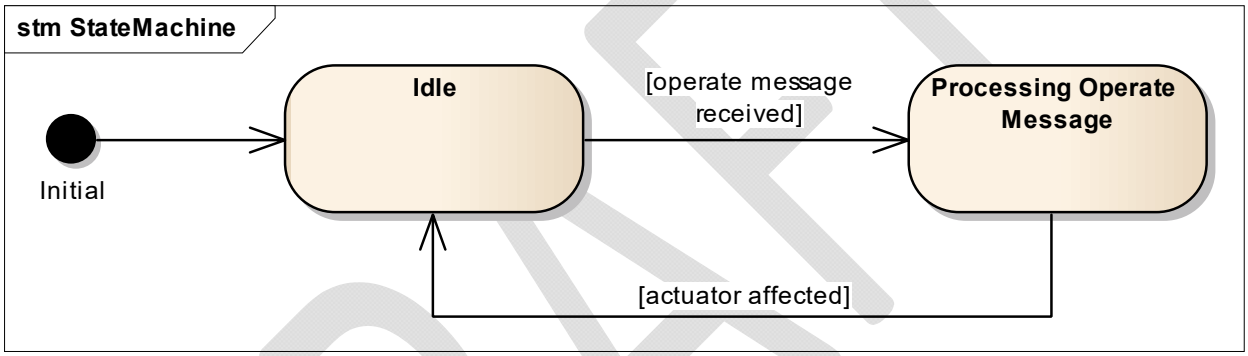

Figure 15 – Actuator State Machine

Idle

Waiting for indication of what should be done next.

Determine if a message is queued. If so, retrieve the message. Otherwise, wait for the next message to arrive.

Transition.

Processing Operate Message

Examine message and determine specific actions required to comply with the operate message.

Take directed action on the physical actuator.

Transition.

2.4.2 Control Application State Machine

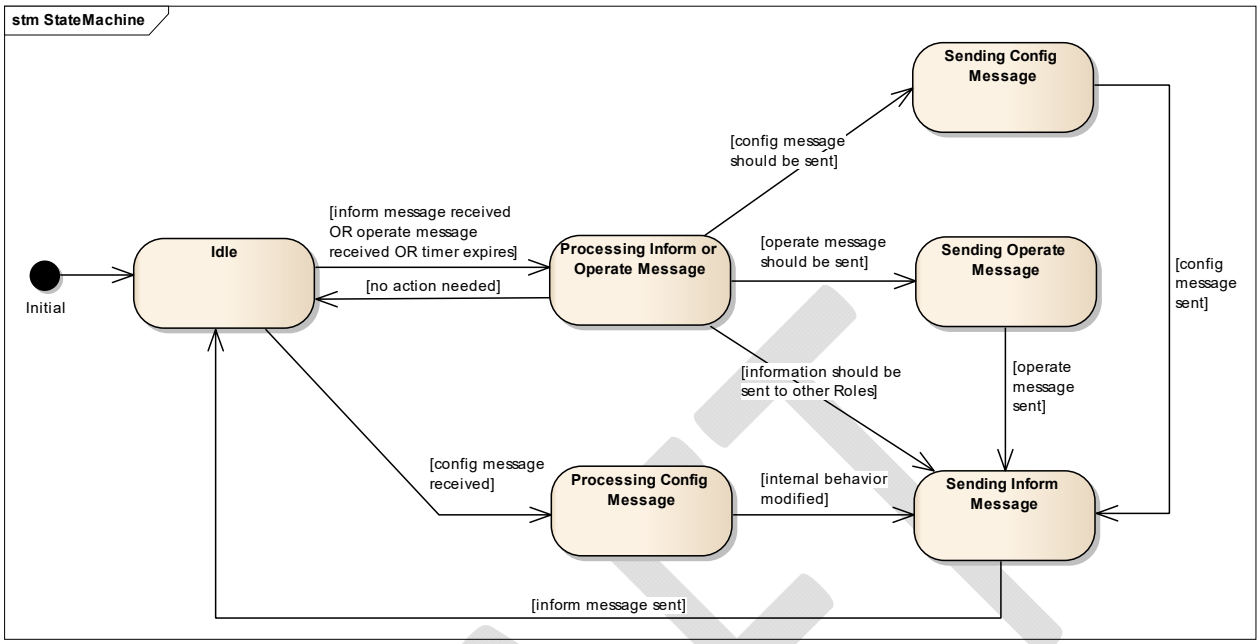

Figure 16 – Control Application State Machine

Idle

Waiting for indication of what the application should do next.

Check to see if a timer has expired. If so, retrieve timer info. Transition.

If not, see if a message is queued. Retrieve the message. If the message is valid, transition.

If not, wait until either of the previous conditions becomes true.

Processing Config Message

Control Application makes whatever changes to its internal behavior (e.g., setting changes or sampling rates) are needed.

Transition.

Processing Inform or Operate Message

Determine what actions, if any, should be taken in response to the current state.

If a timer expired
  Clear the expired timer.
  <application specific logic>
  Transition.

If a message is being processed
Validate the message.
If the message clears a watch condition, clear the associated timer.
<application specific logic>
Transition.

Sending Config Message

Send a config message to another Role (e.g., to instruct another Control Application to change a set point).

Determine recipient.

Send config message to recipient.

Transition.

Sending Inform Message

Determine recipient.

Send inform message to recipient.

Transition.

Sending Operate Message

Determine recipient.

Send operate message to recipient.

Set a timer to assess success of action.

Transition.

2.4.3 Monitoring Application State Machine

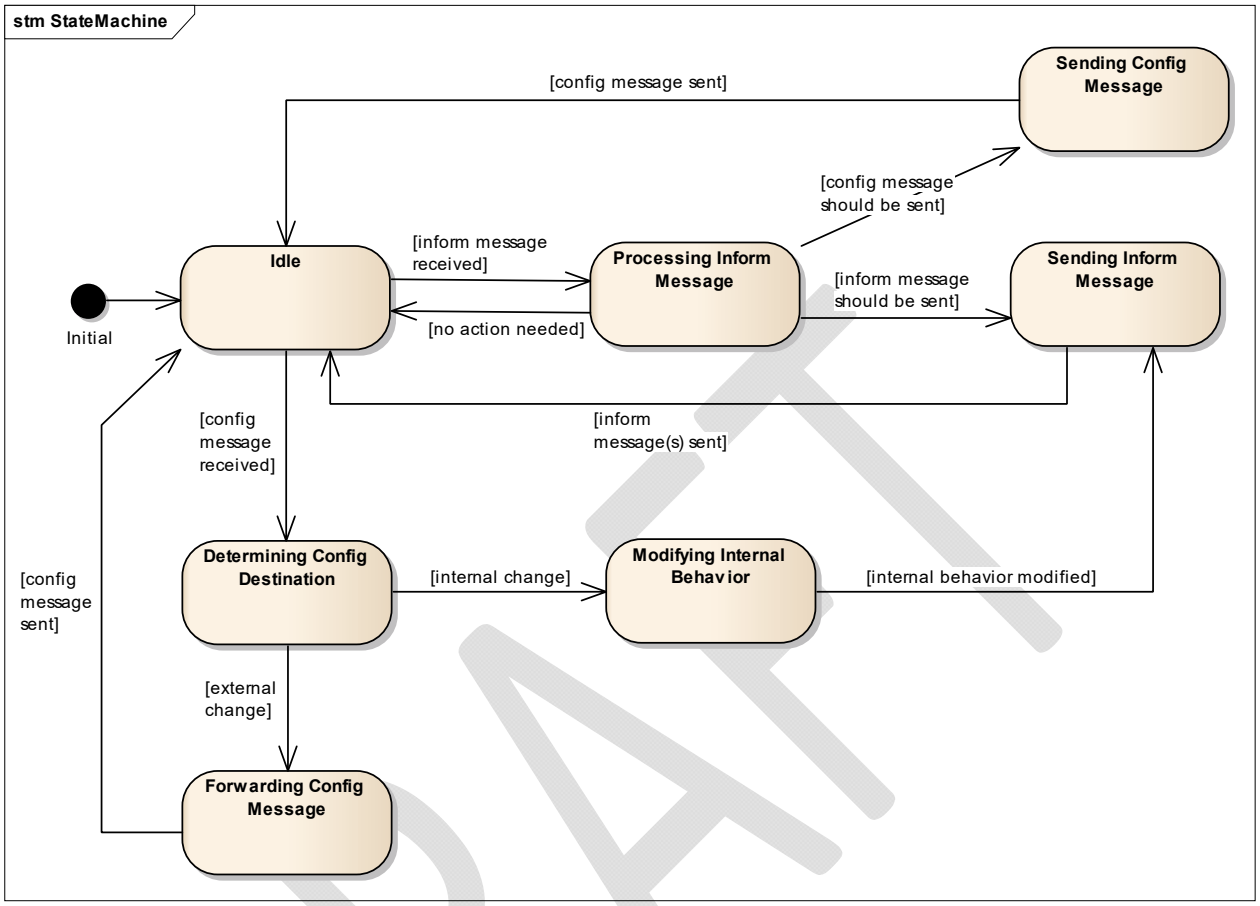

Figure 17 – Monitoring Application State Machine

Determining Config Destination

Monitoring Application examines the destination of the config message to determine if it should be passed on to a Sensor or should affect the behavior of the Monitoring Application itself.

Transition.

Forwarding Config Message

Send a config message to the indicated Sensor.

Transition.

Idle

Wait for new information to arrive.

Determine if a message is queued. If so, retrieve the message. Otherwise, wait for the next message to arrive.

NOTE: whether data arrives through push or pull is protocol dependent.

Transition.

Modifying Internal Behavior

Monitoring Application makes the indicated change to its internal behavior (e.g., setting changes or sampling rates).

Transition.

Processing Inform Message

Determine what actions, if any, should be taken in response to received data.

Perform application-specific computation to determine whether any action is needed (e.g., sending and inform or config message to another Role).

Transition.

Sending Config Message

Send a config message to change another Role's behavior (e.g., to change the sampling rate of a Sensor).

Determine appropriate recipient(s).

For each recipient, send a config message to that recipient.

Transition.

Sending Inform Message

Send appropriate data to all Roles that should be informed.

Determine appropriate recipient(s).

For each recipient, send an inform message to that recipient.

Transition.

2.4.4 Protection Application State Machine

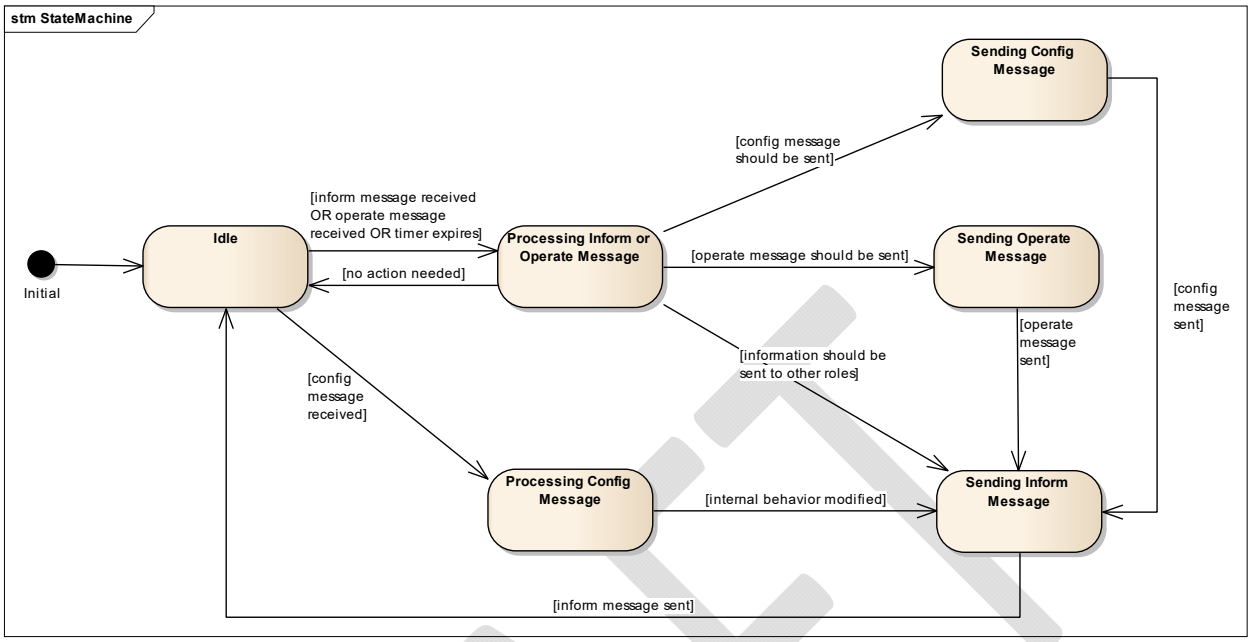

Figure 18 – Protection Application State Machine

Idle

Waiting for indication of what the application should do next.

Check to see if a timer has expired. If so, retrieve timer info. Transition.

If not, see if a message is queued. Retrieve the message. If the message is valid, transition.

If not, wait until either of the previous conditions becomes true.

Processing Config Message

Protection Application makes whatever changes to its internal behavior (e.g., setting changes or sampling rates) are needed.

Transition.

Processing Inform or Operate Message

Determine what actions, if any, should be taken in response to the current state.

If a timer expired
Clear the expired timer.
<application specific logic>
Transition.

If a message is being processed
Validate the message.
If the message clears a watch condition, clear the associated timer.
<application specific logic>
Transition.

Sending Config Message

Send a config message to another Role (e.g., to instruct another Protection Application to change a set point).

Determine recipient.

Send config message to recipient.

Transition.

Sending Inform Message

Determine recipient.

Send inform message to recipient.

Transition.

Sending Operate Message

Determine recipient.

Send operate message to recipient.

Set a timer to assess success of action (e.g., when executing an outer ring of protection that allows more time for a response).

Transition.

2.4.5 *Proxy State Machine*

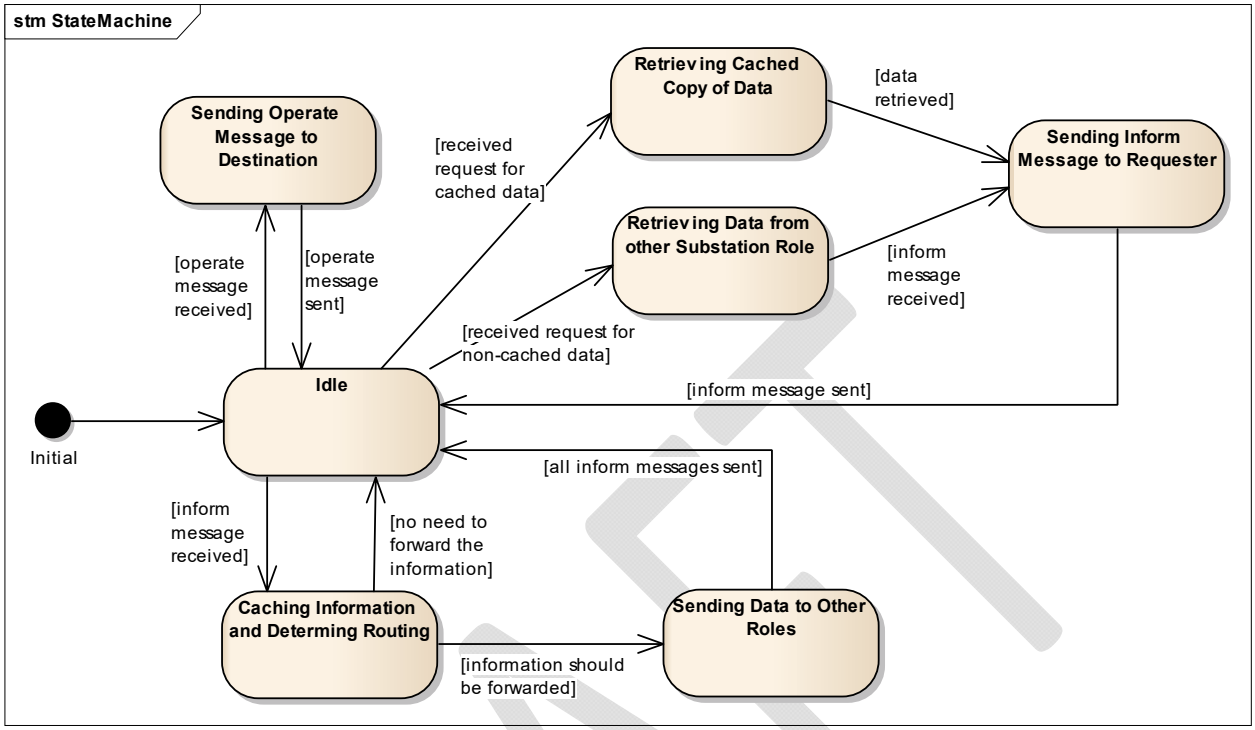

Figure 19 – Proxy State Machine

Caching Information and Determing Routing

Store a local copy of the unsolicited data and determine which Role(s) should be notified.

Store a local copy of the unsolicited data.

Identify all Roles (within or outside the substation), if any, that should be sent a copy of the data.

Transition.

Idle

Wait for indication of what the Proxy should do next.

Determine if a message is queued. If so, retrieve the message. Otherwise, wait for the next message to arrive.

Examine the message and determine its type (inform, operate, or request for data).

If the message is a request for data, determine whether the Proxy already has a cached copy of the requested data.

Transition.

Retrieving Cached Copy of Data

Get a local copy of the requested data.

Lookup local copy of requested data.

Transition.

Retrieving Data from other Substation Role

Get a copy of the requested data from another Role within the substation.

Determine which Role has the requested data.

Send message requesting that data from the appropriate Role within the substation.

Wait for the requested data to arrive.

Transition.

Sending Data to Other Roles

Send a copy of the data to all relevant Roles inside and outside the substation.

For each Role that should receive a copy of the data:
Assemble an inform message containing the data.
Send the message to that Role.

Transition.

Sending Inform Message to Requester

Forward the requested data to the requester.

Assemble an inform message containing the requested data.

Send the message to the requester.

Transition.

Sending Operate Message to Destination

Forward the operate message to its destination.

Examine operate to determine its destination.

Send the message to the appropriate Role (in most cases, this is the Control Authority).

Transition.

2.4.6 Sensor State Machine

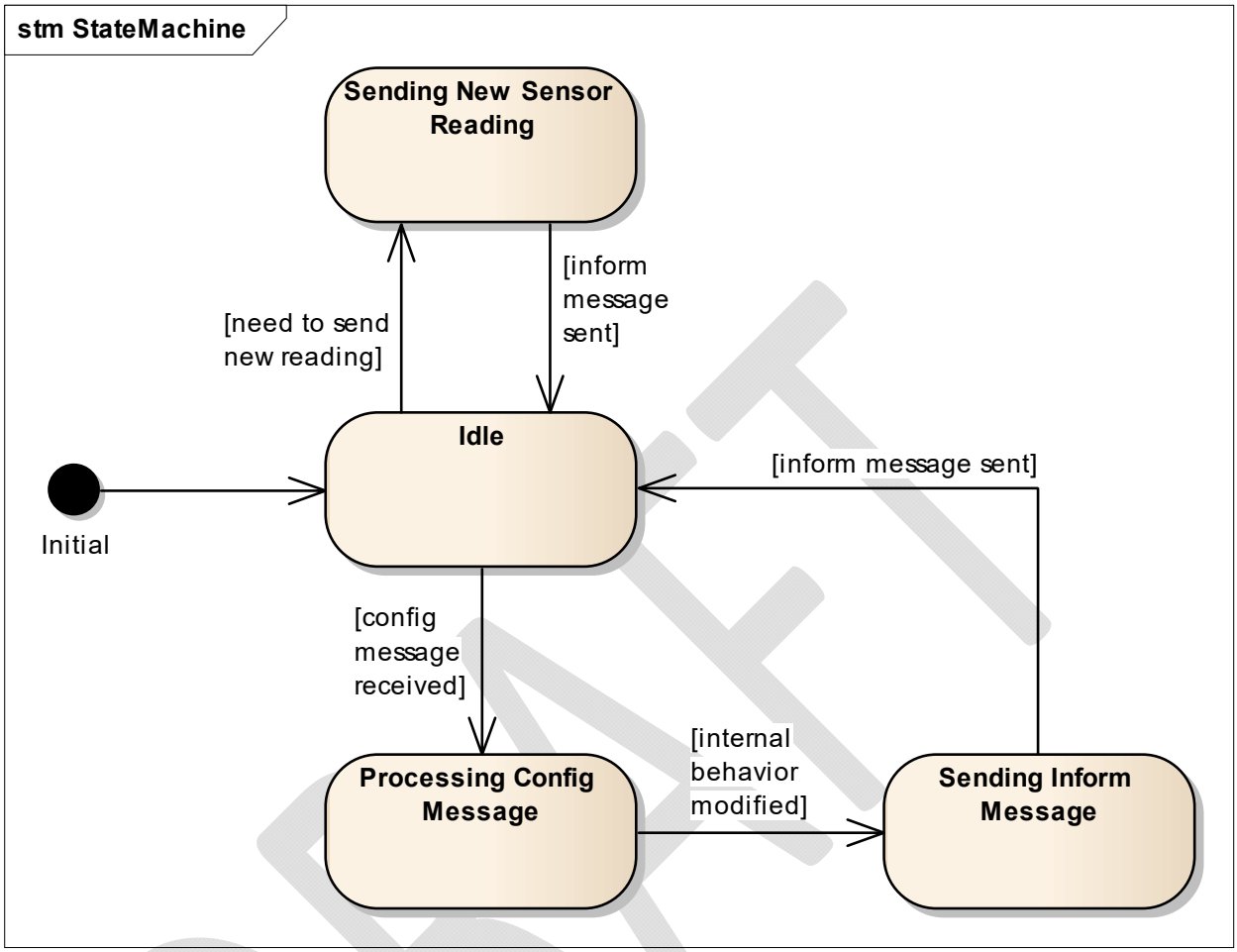

Figure 20 – Sensor State Machine

Idle

Waiting for indication of what should be done next.

Determine if a new sensor reading needs to be sent to other Roles. This decision could be based on time (a clock) or a request for a reading. If so, transition.

Determine if a message is queued. If so, retrieve the message and transition.

If not, wait until either of the previous conditions becomes true.

Processing Config Message

Sensor makes whatever changes to its internal behavior (e.g., calibration changes or sampling rates) are needed.

Transition.

Sending Inform Message

Determine recipient.

Send inform message to recipient.

Transition.

Sending New Sensor Reading

Assemble an inform message containing the new sensor reading.

Send the inform message to all appropriate Roles.

Transition.

2.4.7 Substation Control Authority State Machine

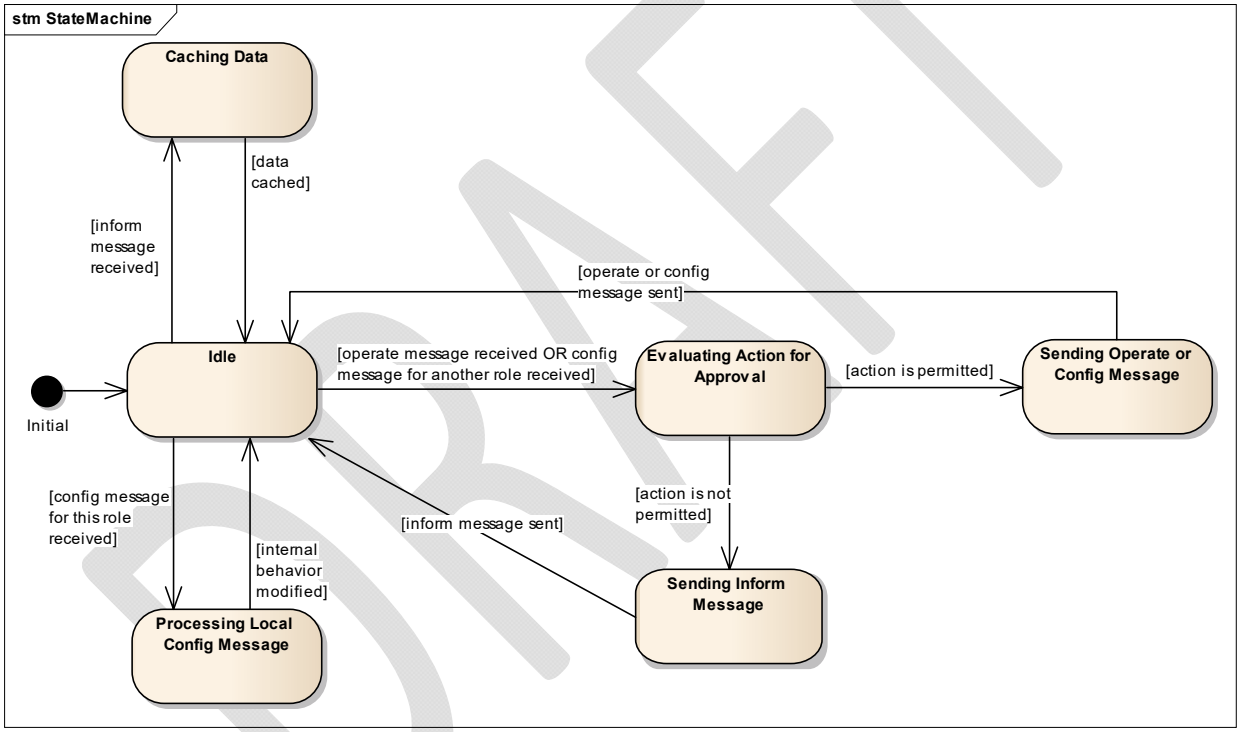

Figure 21 – Substation Control Authority State Machine

Caching Data

Store a local copy of the unsolicited data for use in evaluating future operate and config requests.

Store a local copy of the unsolicited data.

Transition.

Evaluating Action for Approval

Determine if the requested control action is valid given current operational conditions.

Extract requested control action from the message.

Examine all information needed to determine the validity of the requested control action.

Determine if the requested control action is valid given current operational conditions (i.e., that the control action is safe and appropriate).

Transition.

Idle

Wait for indication of what the Substation Control Authority should do next. Inform, Operate, or Config messages may be received; Config message may be intended to change the behavior of the Substation Control Authority itself or may need to be evaluated before being sent to another role.

See if a message is queued. If so, retrieve the message. Transition.

If no message is queued, wait for new message to arrive. Retrieve the message. Transition.

Processing Local Config Message

Substation Control Authority makes whatever changes to its internal behavior are needed (e.g., setting a local/remote flag).

Transition.

Sending Inform Message

Send an inform message explaining why an action is not permitted.

Identify communication path to send inform message to intended Role.

Assemble inform message.

Send message to Role.

Transition.

Sending Operate or Config Message

Send an operate or config message to the intended Role. The message type that is sent corresponds to the type of action that was requested.

Identify communication path to send a message to intended Role.

Assemble an operate or config message.

Send the message to intended Role.

Transition.

2.4.8 Substation Information Repository State Machine

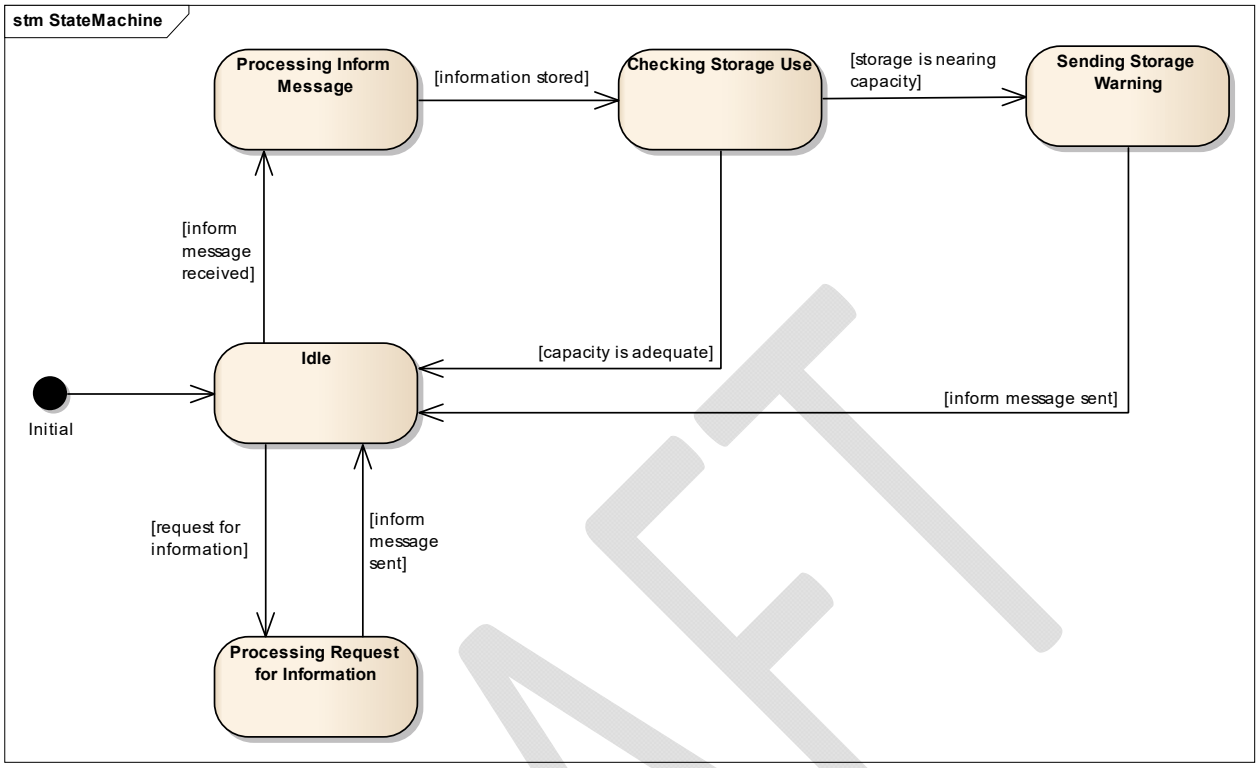

Figure 22 – Substation Information Repository State Machine

Checking Storage Use

Check storage use against capacity to see if a warning should be generated.

Transition.

Idle

Waiting for indication of what should be done next.

Determine if a message is queued. If so, retrieve the message. Otherwise, wait for the next message to arrive.

Transition.

Processing Inform Message

Store the received information.

Transition.

Processing Request for Information

Retrieve a local copy of the requested data.

Assemble and send an inform message to the requestor with the requested data.

Transition.

Sending Storage Warning

Assemble an inform message noting that storage use is nearing capacity.

Send the inform message.

Transition.

2.4.9 Substation User Interface State Machine

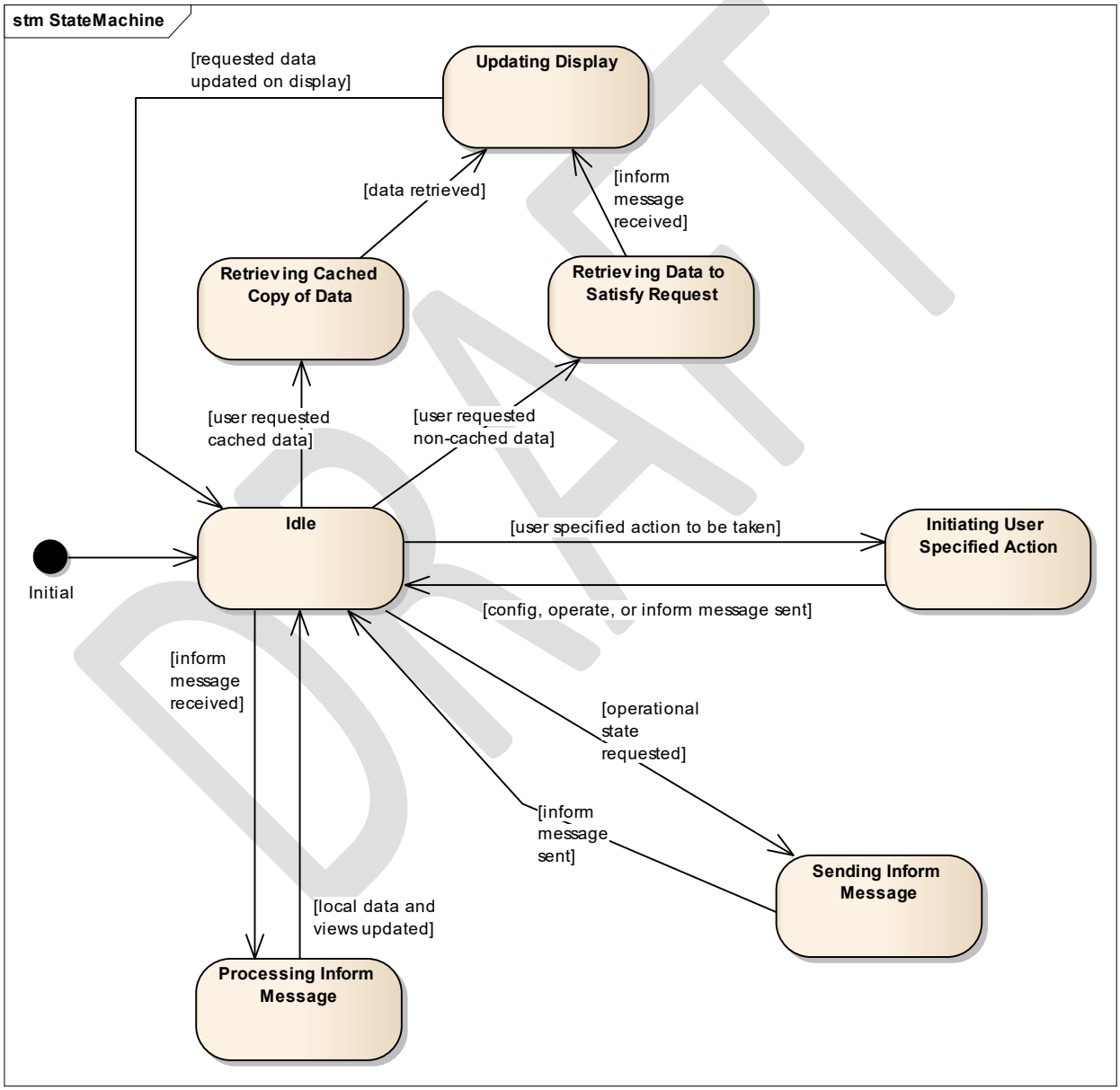

Figure 23 – Substation User InterfaceState Machine

Idle

Waiting for indication of what should be done next.

See if a user has provided the system with input (e.g., a request for information or instruction to take some action). If so, determine the type of input and transition.

See if a message is queued. Retrieve the message and transition.

If neither condition holds, wait until either of the previous conditions becomes true and proceed as stated above.

Initiating User Specified Action

Initiate the user specified action.

Determine which Role(s) should be instructed to take an action.

For each Role, construct the appropriate type of message and send the message to that Role. For example:

- a config message will be sent if the user specifies a set point change
- an operate message will be sent if the user specifies an action that should be taken on primary equipment
- an inform message will be sent if the user specifies an annotation that should be applied to data in the Substation Information Repository

Transition.

Processing Inform Message

Process a newly received inform message.

Cache the data locally.

Update the user display if relevant to current view.

A display update includes decisions regarding how to present the information, such as flagging specific information or raising an alarm.

Transition.

Retrieving Cached Copy of Data

Get a local copy of the requested data.

Lookup local copy of requested data.

Transition.

Retrieving Data to Satisfy Request

Get a copy of the requested data from another Role within the substation.

Determine which Role has the requested data.

Send message requesting that data from the appropriate Role within the substation.

Wait for the requested data to arrive.

Transition.

Sending Inform Message

Provide an update on the system's operational state.

Assemble appropriate information in an inform message.

Send the message to the requester (likely routed to the control center).

Transition.

Updating Display

Use the retrieved data to update the display for the user.

Transition.

2.5 Zone Definitions

This section defines security zones that group roles that share common characteristics and security objectives. For example, the Protection zone represents the set of roles that are essential to performing protection functions in a substation. As such, roles that are not needed for protection functions, like Distribution Assets, are not in this zone.

In Figure 24, each zone is shown using a colored border around a collection of roles. For example, the Protection zone is shown as a red border around four roles: Actuator, Sensor, Protection Application, and (Other Substation) Protection Application.

Most zones include interior segments separated by dashed lines; these segments represent subsets of the zone that could provide degraded functionality in the event of failures within the segments. For example, in the Protection zone, loss of the segment containing (Other Substation) Protection Application would reduce coordination between substations, but would not prevent local protection functions from operating. The meanings of such segments are defined in the elaboration for each zone.

Zones are not mutually exclusive, and some roles (e.g., the Proxy) satisfy the definitions of multiple zones. The Proxy, by its very nature, lives at the intersection of several zones and bridges communication among zones. Zones are abstract, descriptive elements that facilitate a security analysis; they do not correspond to particular systems, devices, or networks.

In the following subsections, each zone is described in terms of its operational requirements and corresponding security requirements.

- **Operational requirements:** these are functional requirements that all elements of the zone must satisfy and that express particular concerns relevant to the zone and its characteristics.

- **Corresponding security requirements:** these are security requirements derived from the corresponding operational requirements.

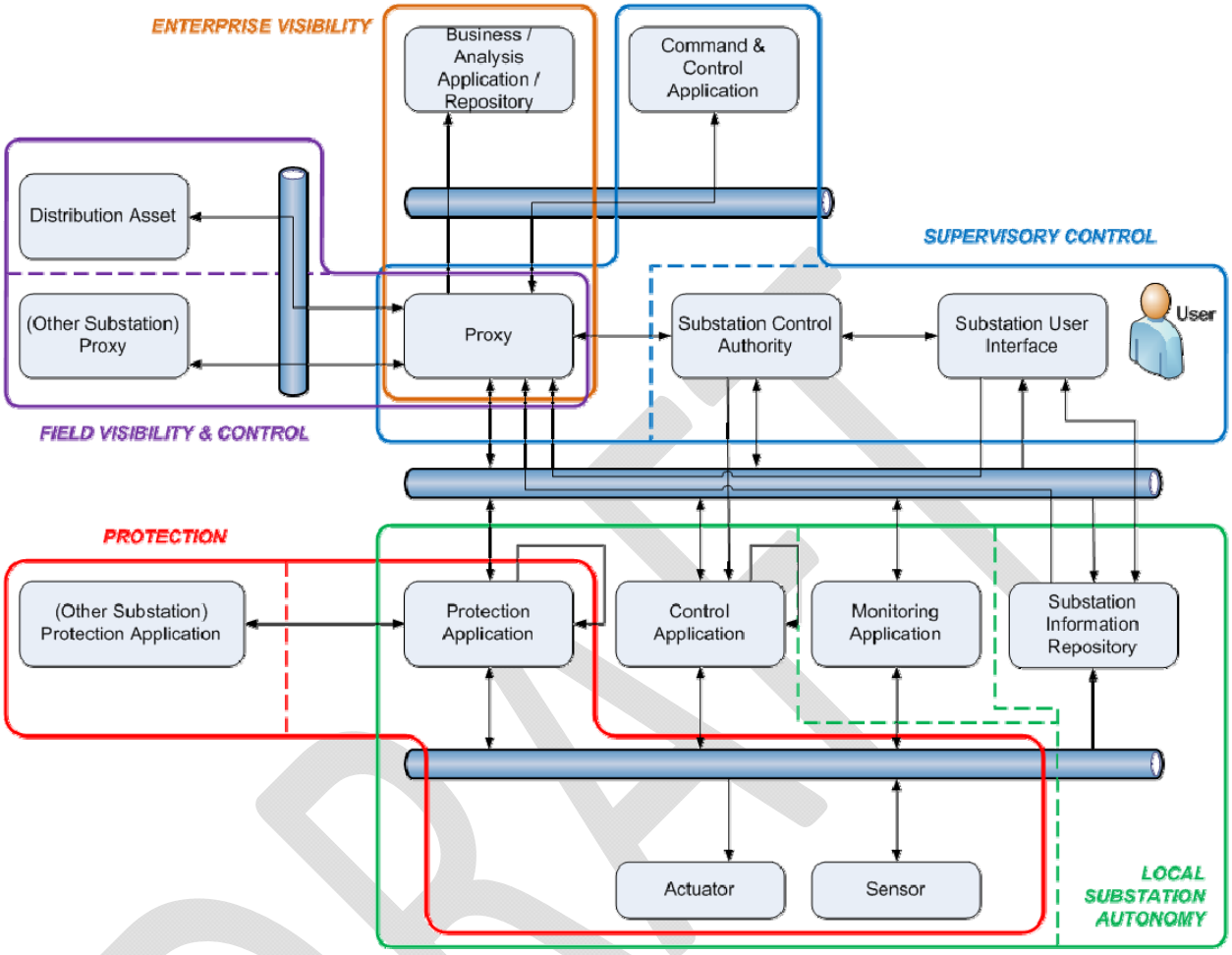

Figure 24 – Zone Analysis

2.5.1 Overarching Requirements for All Zones

There are three overarching themes under which the operational and security requirements for all zones can be clustered.

1- **Latency:** A minimum speed requirement applies to all messages types (operate, config, and inform) within a given zone, except for the protection zone which has additional special message subtypes. Latency requirements are expressed in terms of tiered prioritization and quality of service (QoS).

2- **Permissions:** These are requirements about "Who has permission to send Config and/or Operate messages to whom?" and "Who has permission to receive and act on Config or Operate messages?" Although the reader may consider these to simply be role requirements, zones are a convenient way to cluster them.

3- **Information Traceability (i.e., with respect to origin) and Granularity:** These requirements are about extracting information from a substation. Aggregation increases efficiency and traffic flow, but sometimes roles must be able to reach back and get original fine-grained data from the source (e.g., to verify proper operation or to provide the information needed to recover from an adverse event.)

Operational and security requirements in a zone are mediated by prioritization based on the tier to which a zone or portion of a zone belongs. Tiers are an ordered ranking of the criticality of the roles in the zone and messages originating in the zone. Tier 1 corresponds to the highest criticality and tier 10 the lowest. The higher criticality tiers also have more stringent latency requirements for messages between roles within a zone than the lower tiers. Table 2 lists the tiers to which each zone or subzone (i.e., portion of a zone) belongs. The message latency requirements for a given zone (or portion of that zone) are specified in Table 3.

The "Priority" column in Table 2 below is a reference to allowable IEEE 802.1p levels for the associated Tier.

Table 2 – Zone Prioritization Tiers

Tier	Priority	Message Latency Req't #	Zone or Subzone	Roles in this Zone or Subzone
1	4-7	LR-1	Local Portion of ***Protection Zone***	***Protection Zone***, without Protection App from Other Substation
2	4-7	LR-1	***Protection Zone***	Protection App, Actuator, Sensor, and Protection App from Other Substation
3	1-3	LR-2	Control Portion of ***Local Substation Autonomy Zone***	***Local Substation Autonomy Zone***, without Monitoring App and without Local Substation Information Repository
4	1-3	LR-2	Control & Monitoring Portion of ***Local Substation Autonomy Zone***	***Local Substation Autonomy Zone***, without Local Substation Information Repository
5	1-3	LR-2	***Local Substation Autonomy Zone***	Control App, Actuator, Sensor, Protection App, Monitoring App, and Substation Information Repository
6	1-3	LR-3	Local Portion of ***Supervisory Control Zone***	***Supervisory Control Zone***, without Proxy and without Command & Control Application
7	1-3	LR-3	***Supervisory Control Zone***	Substation Control Authority, Substation User Interface, Proxy, and Command & Control Application
8	1-3	LR-3	Other Substation Portion of ***Field Visibility and Control Zone***	***Field Visibility &Control Zone,*** without Distribution Asset
9	1-3	LR-3	***Field Visibility & Control Zone***	Proxy, Other Substation Proxy, and Distribution Asset
10	0	LR-4	***Enterprise Visibility Zone***	Proxy and Business/Analysis Application/Repository

Table 3 – Zone Latency Requirements for Messages

Message Latency Req't #	Zone(s)	Message Latency Requirements
LR-1	Protection Zone	Messages between roles located within this zone must satisfy latency requirements for the applicable performance class of Type 1, Type 4, and Type 6 messages as outlined in IEC 61850-5, Section 13 (Message Type 1 - fast messages, Type 4 - raw data messages, Message Type 6 - time synchronization messages, Performance Classes P1, P2, or P3).
LR-2	Local Substation Autonomy Zone	Messages between roles located within this zone must satisfy latency requirements for Type 2, and Type 6 (Time Performance Class T2) messages as outlined in IEC 61850-5, Section 13 (Message Type 2 - medium speed messages, Message Type 6 - time synchronization messages).
LR-3	Supervisory Control Zone, or Field Visibility & Control Zone[4]	Messages between roles located within these zones must satisfy latency requirements for Type 3, Type 6 (Time Performance Class T1), and Type 7 messages as outlined in IEC 61850-5, Section 13 (Message Type 3 - low speed messages, Message Type 6 - time synchronization messages, Message Type 7 - command messages with access control).
LR-4	Enterprise Visibility Zone	Messages between roles located within this zone must satisfy latency requirements for Type 5 messages as outlined in IEC 61850-5, Section 13 (Message Type 5 - file transfer functions).

2.5.2 Communication within and between zones

The following generic rules for communications are imposed on the network infrastructure to restrict the delivery of messages between roles. Tiers are subsets within zones as indicated by dotted lines in Figure 24 – Zone Analysis.

GR 1. Messages between roles located in different zones shall satisfy the least stringent latency requirements of the involved zones.

GR 2. A zone must be able to provide essential functionality in the event of loss of communication with lower priority (higher numerical) tier zones.

GR 3. Messages from a lower priority (higher numerical) tier zone shall not cause a higher priority (lower numerical) tier zone to violate the higher priority tier zone's latency requirements or otherwise fail to fulfill its mission.

GR 4. Messages of any type from the same or higher priority (lower numerical) tier take priority over messages from a lower priority (higher numerical) tier. For messages within the same

[4] Note that the latency requirements for the Field Visibility & Control Zone are the same as for the Supervisory Zone. In particular, both zones must satisfy the latency requirements for Type 6 (time synchronization messages). There is a need for time synchronization on a limited basis in the Field Visibility & Control Zone, so Type 6 messages must be addressed (though the need is not as prevalent as in the Supervisory Zone). Likely, the Proxy is involved with time synchronization out to roles in the Field Visibility & Control Zone.

priority tier, OPERATE and CONFIG messages shall be delivered before INFORM in the event of traffic overload. Conflicts are otherwise resolved by first-in-first-out (FIFO) queuing.

GR 5. Any role may request information from any other role as allowed by communications architecture and function.

GR 6. In cases where a role from a low priority (high numerical) tier makes a data request of a role in a high priority (low numerical) tier by way of intermediate roles, those intermediate roles may add information to a response, but may not modify any material produced within a higher priority (lower numerical) tier.

GR 7. Roles may only share INFORM messages with roles in the same or lower priority (higher numerical) tiers. (This does not apply to OPERATE or CONFIG messages.)

GR 8. Roles and communication services in each zone must be adequately provisioned for the zone. Roles must be capable of prioritizing network traffic appropriately, and communication services shall provide and enforce QoS functionality.

2.5.3 Enterprise Visibility

Operational Requirements

1. Communications in this zone must provide sufficient network capacity to support the transport of large files / large amounts of data.
2. Roles dependent upon communications through this zone must have access to unaltered and original data from roles in zones with closer proximity to the physical electric system.
3. Roles in this zone must be able to identify the device that originated each data item entering the enterprise visibility zone.
4. Messages and information within this zone must satisfy basic latency criteria as described in IEC 61850-5 Section 13.
5. Substation operations shall not depend on information exchange within the enterprise visibility zone. Information exchange within the enterprise visibility zone shall not degrade the performance of the substation.
6. Roles within this zone must be able to suspend large file transfers from other zones in the event of the need to send and receive higher-priority messages.

Corresponding Security Requirements

1. Services provided by roles in this zone shall preserve the integrity and origin of data transported.
2. Roles in this zone must be able to authenticate remote devices/components.
3. Roles in this zone must protect the confidentiality of sensitive business and operational (e.g., historical power system) data.
4. The trustworthiness of the entity implementing the enterprise interface to the substation shall be explicitly verified and continuously monitored by a security mechanism.

5. Impacts to the non-persistent data store shall not impact the integrity or availability of the original data, or source of the data.
6. Roles in this zone shall employ security mechanisms to contain attacks and compromises, and prevent their propagation to other zones.

2.5.4 Field Visibility & Control

Operational Requirements

1. Roles in this zone must have an interface to a communications path from one geographically distinct location to another (e.g., separate physical facilities).
2. Roles in this zone must be able to identify remote devices/components and to identify the original source device/component that generated any particular data element.
3. Messages between roles located within this zone must satisfy latency requirements for Type 3 (low-speed messages), Type 6 (time synchronization messages – Performance Class T1), and Type 7 (command messages with access control) messages as outlined in IEC 61850-5, Section 13.
4. Roles in this zone shall defer coordination of communications to operations of the Proxy.
5. Roles in this zone may support connection between substations in a temporary and explicitly authorized emergency-only mode.

Corresponding Security Requirements

1. Roles in this zone must employ mechanisms to detect and mitigate, or prevent, where possible, snooping and modification of data in transit.
2. Roles in this zone must employ mechanisms to detect tampering or unauthorized modification of the configuration of data sources (e.g., devices, components, or applications).
3. Roles in this zone must be able to authenticate remote devices/components.
4. Communications infrastructure in this zone must require devices/components to authenticate prior to network admission.
5. Roles in this zone shall be provisioned such that security controls do not inhibit operations for longer than 1 second at a time before addressing the message queue.
6. The Proxy must be able to selectively shut off communications with other devices/components in this zone based on behavior.

2.5.5 Supervisory Control

Operational Requirements

1. Roles in this zone must be capable of providing monitoring and control of substation functionality by coordinating and instructing the activities of devices within the substation.
2. Roles in this zone must be able to provide essential core functionality in the face of lost communications outside the zone.

3. Messages between roles located within this zone must satisfy latency requirements for Type 3 (low speed messages), Type 6 (time synchronization messages – Performance Class T1), and Type 7 messages (command messages with access control) as outlined in IEC 61850-5, Section 13.
4. Roles in this zone must continue to provide monitoring and control of local equipment when communications with other physical locations (i.e., geographically distinct) are unavailable.

Corresponding Security Requirements

1. Roles in this zone follow automated procedures for basic operation.
2. Roles in this zone follow a secondary set of automated procedures for escalated operation, allowing more direct operation of substation equipment.
3. Local authentication and authorization must not depend upon a connection to roles outside of the substation.

2.5.6 Local Substation Autonomy

Operational Requirements

1. Safety-related functions have the highest priority within this zone.
2. Roles in this zone must be able to provide essential core functionality in the face of lost communications outside the zone.
3. Messages and information within this zone take priority over messages and information coming from less critical zones.
4. Messages between roles located within this zone must satisfy latency requirements for Type 2 (medium speed messages), and Type 6 (time synchronization messages – Performance Class T2) as outlined in IEC 61850-5, Section 13.
5. Given incomplete or uncertain data, the system should take no action.

Corresponding Security Requirements

1. Roles within this zone must be able to designate functions as safety-related, distinguish safety functions from other operational functions, and assign safety functions the highest priority.
2. Roles within this zone must protect the classification and declassification of functions as safety-related.
3. Local authentication and authorization must not depend upon a connection to roles outside of the zone.
4. Roles in this zone must be able to distinguish the source of messages and assign priority accordingly.
5. Roles in this zone must be able to provide essential core functionality in the face of lost communications outside the zone, identify the loss of any functionality, and restore lost functionality in a timely manner.

2.5.7 Protection

Operational Requirements

1. Protection functions shall have a higher priority than any other functions. (Protection functions are considered a subset of safety-related functions for this context.)
2. Roles in this zone must be able to provide essential functionality in the face of lost communications outside the zone.
3. Messages between roles located within this zone must satisfy latency requirements for the applicable performance class of Type 1 (fast messages), Type 4 (raw data messages), and Type 6 (time synchronization messages – performance classes P1, P2, or P3) as outlined in IEC 61850-5, section 13.
4. Roles in this zone must be sufficiently understood in their configuration and operation so as to inspire confidence in predicting responsive behavior, and therefore have a strongly established trust relationship with other roles in the protection zone.
5. Single points of failure must not prevent the operation of protection functions.
6. Power system components (transmission line, breaker, bus) must not operate in the absence of designated minimum protection functionality, and shall be disabled in the event of any loss of such protection functionality.
7. The status of protection functions shall be available at all times locally, and to all connected systems.
8. Protection functionality shall not be considered available in the absence of any required input.

Corresponding Security Requirements

1. Protection functionality must not depend upon a connection to roles outside of the zone.
2. Roles outside the zone must not be capable of disabling protection functions.
3. Roles in this zone must be capable of performing authentication and authorization functions in a parallel (i.e., background) activity (e.g., continuously maintained preauthorization check).
4. Roles within this zone must be able to designate functions as protection-related, distinguish protection functions from other operational functions, and assign protection functions the second highest priority (after safety).
5. Roles within this zone must protect the classification and declassification of functions as protection-related.

3 Failure Analysis

The underlying approach used to create this security profile begins with defining the functions of the substation automation system through abstract roles, zone-based analysis of communications, and state machines. The development of the zone analysis and state machines, and the definition of roles take into account a foundational set of security and operational objectives that is also used in the next step of the process, failure analysis. The failure analysis is the focus of this section, beginning with a description in Section 3.1 of the process for identifying failure modes that represent deviations from desired behavior of the substation automation system. A brief overview of the foundational security and operational objectives is presented in Section 3.2 and a more detailed view of the identified failure modes is presented in Section 3.3.

3.1 Failure Analysis Process

The failure modes identification process is loosely based on a Failure Modes and Effects Analysis (FMEA) of the substation automation logical architecture presented in Section 2, however the analysis is performed with a security bias to failure identification. As applied to this security profile, a FMEA is a qualitative procedure for analyzing potential system failures and their associated modes as a function of assemblies, subassemblies, components, and subcomponents. The procedure used here is as follows:

1. Through consultation with subject matter experts and relevant documentation, establish an understanding of the enterprise/system/process under consideration by gathering all relevant information and invoking a proper review process.
2. Based on (1), develop a functional hierarchy of roles and their responsibilities.
3. At an appropriate level of abstraction, identify potential failure modes.

4. Develop security controls for each failure mode.

Omitted from this profile are the two following steps, which complete the FMEA process. These steps take into account the specific needs of the organization that owns or operates the system, so the outcome of these steps is necessarily specific to that organization and is not covered by this profile.

5. Qualitatively assign a risk for each failure mode through a Risk Priority Number (RPN) calculation.
6. Perform a cost-benefit evaluation for controls (with respect to risk reduction) and provide a balanced decision process for corrective action implementation.

For this security profile, failure analysis centers on the roles, state machines, and security zones defined in Sections 2.2, 2.3.1, and **Error! Reference source not found.**, and the causes of potential failures in a substation automation system. The resulting list of failure modes serves as a basis for (1) justifying the set of selected controls, as each control must address an identified failure mode, and (2) identifying and remediating gaps in the selected controls, as each failure mode must be addressed by at least one control.

3.1.1 Role-based Failure Mode Identification

This section describes the process that was used to identify the failure modes associated with each in-scope role. The analysis is based on functional behavior that is modeled in each role's state machine (see Section 2.4), including the annotations describing what happens in each state. These models exclude any security functions, which avoids introducing any bias due to pre-conceived recommendations for security controls.

Each role is analyzed individually. Behavior at a role's interface (e.g., sending or receiving a message) is included in the analysis, but failures that could occur between roles (e.g., messages in transit) are not part of the role-base failure mode analysis. That behavior is analyzed in the communication-based failure mode analysis (see Section 3.3.2).

Role-based failure mode analysis is organized around two concepts: variable analysis and state analysis. In variable analysis, a small number of variables are defined that abstract key concepts, information, or dependencies that significantly influence the role's behavior. Each variable is examined to determine what failure modes could lead to discrepancies between the role's actual and indicated values of that variable (e.g., believing that no messages are available when valid messages are queued). In state analysis, each state of the state machine model is examined to determine what failure modes could lead to the role entering that state by unexpected or unallowable paths (e.g., entering a state to react to a message when no message has been received).

In each analysis, only first-order failures are considered. That is, examples in which one failure mode is followed by another are not examined. This is because while each such combination could result in a new failure (with different effects or consequences), the combination would be unlikely to yield new failure modes.

Variable Failure Mode Analysis

This analysis begins by studying the role's state machine model to identify key factors that influence its correct behavior. Selection of such factors requires judgment and will influence the types of failure modes that are identified in the analysis. Examples include:

- data that directs behavior, like the availability and types of messages received by the role
- current accumulated state at the role, like whether information is stored locally or whether storage is exhausted
- use of a timer, like whether a time-sensitive message or instruction is pending, expired, or not set (has not yet arrived)
- external dependencies, like whether a pending request for information has been satisfied

Each factor is encoded as a variable and the next step is to enumerate the variable's range (i.e., the complete set of possible values for the variable). For example, a variable that abstracts the dependency on another role to provide information (Request) could have the following range values:

- **none:** the Request has not yet been sent
- **pending:** the Request has been sent and the sender is awaiting a Response
- **satisfied:** the sender has received a Response
- **no response:** the sender did not receive a Response within the acceptable time window

It is important that the variable and each range value have an accompanying description; writing such descriptions can trigger new thoughts, which may result in additional range values.

Each variable is next analyzed in isolation. For each variable, a table like the following is constructed that contains all combinations of range values for the variable. The two columns are prefixed with "Actual" and "Indicated." The "Actual" version of the variable represents the state that the role should be in, while the "Indicated" version represents the state that the role "thinks" that it's in.

Table 4 - Example Variable Failure Mode Analysis

Actual Request	Indicated Request	Failure Modes
none	none	
none	pending	
none	satisfied	
none	no response	
pending	none	
pending	pending	
pending	satisfied	
pending	no response	
…	…	

The purpose of this analysis is to identify failure modes that could lead the role to enter an inconsistent state. For each row, the analysis assumes that the role begins in a safe, consistent state (e.g., among other factors, the two versions of the variables match). Each row then represents a new role state in which the two versions of the variable have the new values; if those new values match, then no failure is considered. If the new values do not match, the analysis team brainstorms failure modes that could lead to this particular kind of inconsistency (i.e., some failure has occurred, but the analysis is focused more on the why than the what).

Of course, such variables may not exist in the real-world implementation of the role, but they serve as an effective tool for examining an abstract model in a focused, deliberate analysis of potential causes of failures.

State Failure Mode Analysis

The state analysis follows a similar focused, but abstract approach to identify failure modes. A similar table is constructed (as shown below), but the columns are different. The first column identifies the state (from the role's state machine model) that the role is entering. The second column identifies different "paths" by which the role could enter that state. The "Path" column always identifies the same three kinds of paths for each state

- **expected:** the path from the previous state to the new state matches a path in the state machine model; the role's behavior matches what is in the state machine.
- **unexpected:** the role has entered a new state that is allowable from the previous state, but not by an expected path (e.g., transitioning when the guard condition is not satisfied or processing in the previous state has not been completed).
- **unallowable:** the role has entered a state that should not be reachable from the previous state.

Table 5 - Example State Failure Mode Analysis

New State	Path	Failure Modes
idle	expected	
idle	unexpected	
idle	unallowable	
sendinfo	expected	
sendinfo	unexpected	
sendinfo	unallowable	
…	…	

As with the variable analysis, each row is examined with the assumption that the role begins in a safe, consistent state. For each row where the role has followed an expected path, no failure modes are considered as no failure related to the state transition is indicated. Otherwise, the analysis team brainstorms failure modes for each combination.

3.1.2 Communication Analysis Process

The analyses of role-based failure modes in this profile are based on potential deviations from the expected behavior of individual substation automation roles. The expected behavior of each role is characterized and formally specified by the role's state machine diagram. However, since the role-based failure analyses consider only the behavior of the individual roles in isolation, then even in aggregate they paint only a partial picture of the ways in which anomalous behavior of the SA system as a whole can arise.

Therefore role-based failure analyses alone are not sufficient. To garner a more complete picture of the failure modes to which an SA system can be subject, complementary failure analyses are needed based on both the communications between roles and on the five zones specified in the SA architecture diagram. This section considers failure analyses based on communication between roles. A zone-based failure analysis is considered in the next section.

A *communication failure analysis* attempts to capture the anomalous behavior (in terms of failure modes) that can be associated with communications between roles. To determine the failure modes associated with communications between roles, this profile begins by considering the most basic act of communication: "Role *A* sends message *M* to role *B*."

Below are listed four essential communication objectives for the action "Role *A* sends message *M* to role *B*." Underneath two of the objectives are specific corollaries that are implied by the objectives.

1) *M* should arrive at *B* in a timely fashion
    a. *M* should arrive
2) *M* should arrive at *B* unaltered[5]
3) *M* should not be delivered to any role other than *B*
    a. *M* should arrive at *B* unobserved
4) *M* should not originate from any role other than *A*

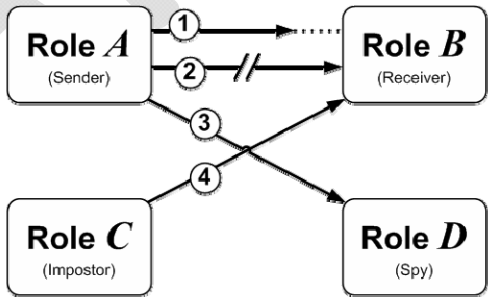

Figure 25 – Communication Objectives

[5] This objective can fail in one of two primary ways, (i) M is readable, but altered or (ii) M is unreadable.

As the next step in the analysis process, this profile uses the communication objectives as a starting point to derive a set of potential communication failure classes. This is achieved for each objective by creating a statement describing a communication event that directly violates the objective (i.e., by negating the description of a communication event that directly satisfies the objective).

So, the set of communication failure classes becomes:

1) *M* does not arrive at *B* in a timely fashion
    a. *M* does not arrive

2) *M* arrives at *B* altered (readable but altered, or unreadable)

3) *M* is delivered to a role other than *B*
    a. *M* arrives at *B* but was observed by others

4) *M* originated from a role other than *A*

Starting with the communication failure classes, a team of subject matter experts (SMEs) that included not only cyber security experts, but also power systems engineering expertise, used experience and brainstorming to generate a set of *failure modes* (which specify how, or why, or ways in which a communication event could fail to meet any of the overarching communication objectives). The resulting set of communication failure modes can be found in Table 5 in section 3.3.2 below. The table also indicates which of the essential communication objectives are violated by each of the failure modes.

3.1.3 Zone-Based Analysis Process

This profile's analyses of role-based failure modes thus far are based on potential deviations from the expected behavior of individual substation automation roles and the anomalous behavior associated with communications between zones. To complete the picture of the failure modes to which an SA system can be subject, a complementary failure analysis is needed based on the zones specified in the SA communications architecture diagram. The five zones that are the focal points of the SA architecture are the (1) protection zone, (2) local substation autonomy zone, (3) supervisory control zone, (4) field visibility and control zone, and (5) enterprise visibility zone. A *zone-based failure analysis* attempts to capture the anomalous behavior (in terms of failure modes) that can be associated with the specific operational requirements[6] that each zone imposes on any role within its boundaries (as described in Section 2.5).

As the next step in the analysis process, this profile uses operational objectives for each zone as a starting point to derive a set of potential zone-based failure classes. For each objective a statement is created describing a zone-specific event that directly violates the objective (i.e., by negating the description of a zone-specific event that directly satisfies the objective.)

[6] The role-based, communication-based, and zone-based failure analyses are based on identifying potential deviations from expected operational (i.e., functional) behavior, and do not consider security requirements until the security control development phase.

Starting with the zone-based failure classes, a team of SMEs that included cyber security and power systems engineering expertise, used experience and brainstorming to generate a set of failure modes that specify ways in which a zone-specific event could fail to meet an operational objective for that zone. The next step is to eliminate those zone-based failure modes that were already covered by existing communication-based or role-based failure modes that had been identified during earlier analyses. However, if a zone-specific failure mode appears to be covered by an existing failure mode, but the nature of the operational requirements for the zone means that the security controls would need to be different or unique for that zone (e.g., due to latency requirements), then the zone-specific failure mode is retained. For example, the first zone-based failure mode (in Table 8 in Section 3.3.3) is "FZ1 – Messages required for system protection do not arrive in a timely manner." Although this appears to be covered by a few of the communication-based failure modes, a couple of unique security controls are needed to specifically deal with this failure mode in the protection zone (see controls IPC and VE in Table 10 in Section 4.1). From a process standpoint, this means that some zone-based failure modes that appear to be covered by existing failure modes are retained during the first elimination pass if one or more team members could make the case that special zone-specific controls might be needed. If no unique controls for an apparently redundant zone-based failure mode are found to be necessary during the security control development phase, then the overlapping zone-specific failure mode is eliminated. If unique controls were confirmed to be necessary, the zone-specific failure mode is retained.

The elimination of the overlap with communication-based and role-based failures modes for which no zone-specific security controls are needed produced a set of zone-based failure modes, found in Table 8 in Section 3.3.3 below. The table also indicates which of zone-based operational objectives are violated by each of the failure modes.

3.1.4 Failure Analysis Process for Security Controls

The failure analysis processes described in the previous subsections are based on exploring the possible ways in which the expected functional behaviors inherent in substation automation operations could be disrupted by role-based, communications-based, and zone-based failures. However, failure analyses that only examine a substation's expected functional behaviors based on the substation's operational requirements do not paint a complete picture of the set of potential failure modes.

Specifically, the interventions used by system designers and security engineers to mitigate potential failures modes for substation operations are themselves subject to failure. In particular, the security controls used to deter, protect, detect, respond to, or recover from the failure modes associated with a substation's expected operational behaviors can fail in ways that not only inhibit a control's own security functionality, but may also inadvertently disrupt the proper operation of the substation (i.e., interfere with its operational objectives), for example by locking out operator access during an emergency.

Security controls are subject to integrity, confidentiality, and availability failures that violate the security objectives the controls were meant to fulfill. Moreover, if not carefully designed configured and deployed, security controls may interfere with the operational objectives they are meant to protect.

The general security objectives that security controls are meant to fulfill are outlined in the subsection on "Security and Operational Objectives" (Section 3.2) below. For example, the first principle states that "Security controls should not interfere with the missions of the SA system," such as by delaying execution of a protection function to the extent that power system assets are damaged. This security objective is "baked into" the design of the security controls themselves, for instance, by addressing (where appropriate) the latency requirements associated with the zones in our substation automation logical architecture. The other general security objectives in Section 3.2.3 are also addressed and "baked in" as necessary during the design of the controls.

However, there is an additional overarching principle that applies to the *protection of security functions*, and this is expressed as a security requirement at a level above the security requirements for protecting substation automation operations.

> *Security Function Protection: The integrity, confidentiality, and availability of the information needed to make and execute proper security decisions (including recovery from adverse security events) must be protected.*

The failure analysis process for security-control-based failures involves the direct derivation of failure modes that violate the above security objective.

3.2 Security and Operational Objectives

The goal of this document is to establish a cyber environment in which a substation automation system can successfully and securely operate. Meeting this goal requires that a number of security and operational objectives that support that goal are achieved. This section defines the assumptions made regarding the operational context for these systems and how the systems will be operated, and then presents a set of security objectives around which the remainder of the document revolves.

3.2.1 Contextual Assumptions

This document assumes that the following conditions, largely or wholly outside of the organization's control, apply to the environment in which a substation automation system will be deployed:

1. Integration with (or incorporation of) legacy systems that have limited security capabilities may be difficult (i.e., impractical) to avoid.
2. The nature of protection functionality presents significant dependency and challenges in differentiating between true observations and false (i.e., maliciously manipulated) input. (A deep understanding of system operation by an adversary presents significant opportunity for the system to be turned against itself using intended design functionality.)
3. Adding functionality to SA systems and devices places additional performance burdens on device capabilities, and may inhibit the device's ability to perform its core function.
4. Adding complexity to SA systems increases the:
    a. Difficulty of understanding cause-and-effect and sequence-of-events
    b. Opportunity for unintended consequences

5. Integration of increased functionality demands more, broader, and deeper expertise, which in turn increases opportunity for organizational dysfunction.

3.2.2 Core Operational Assumptions

This document assumes that organizations will operate substation automation systems in the following manner:

1. The primary mission of the substation automation system is to protect personnel safety.
2. The secondary mission of the substation automation system is to protect the integrity of power system assets.
3. The tertiary mission of the substation automation system is power system reliability, which includes maintaining service with minimal interruptions (with respect to duration and number of customers affected) and quick restoration when an outage does occur.
4. Local substation functions should be able to continue operations in the absence of external communications.
5. Automated system protection decisions should not be executed based solely on data from non-utility assets.
6. Protection should not be disabled on energized equipment.
7. No ability to remotely disable protection. Disabling protection functionality requires someone on-site.
8. For a given Actuator, there is at most one Control Application that can send control actions to that Actuator. (NOTE: Protection Applications do not follow this constraint.)

3.2.3 Security Principles

Six overarching security objectives for the substation automation system are identified and utilized throughout the profile development process. These objectives serve as the security "ground rules" for the substation automation systems and help with use case development and failure identification. The objectives are as follows:

1. Security controls should not interfere with the missions of the SA system.
    a. SA protection functions are particularly sensitive to reduced availability and added latency.
    b. SA monitoring and control functions are particularly sensitive to reduced availability.
    c. Security controls must not inhibit manual emergency override capabilities.
    d. Security controls should provide clear visibility/indication of the sequence of security events, automated control actions taken, and expedient operator actions for restoration/recovery of substation automation systems.

e. Security controls should provide for the maximum amount of operational flexibility (e.g., updates of access control lists should not require a full re-evaluation of the entire system).

2. Security controls should protect the system from unauthorized actions that could endanger personnel or equipment, or adversely impact power system reliability.
    a. Users should not be allowed to perform any action that falls outside of their assigned role.
        i. Generally, local operation takes precedence over remote operation.
        ii. Configuration and operation of the system should be performed by separate roles.
    b. No unauthorized or unauthenticated remote access should be granted by a SA system device or component.
        i. Remote access should be restricted to designated systems and locations.
        ii. All remote access should utilize designated points for ingress/egress.
    c. No unauthorized or unauthenticated control commands should be processed by a SA system device or component.
        i. Only control commands from designated systems and locations should be executed.
        ii. Control commands should use designated points for ingress/egress.
    d. No unauthorized or unauthenticated changes to system behavior or operation should be permitted.
3. Security controls should provide evidence of SA system behavior and operation.
4. Any SA system device or component should be able to validate the authenticity and integrity of all data acquired from another SA device or component.
5. Asset owners should not solely rely on security measures outside their direct observation and control.
    a. Responsibility for system behavior, operations, and associated monitoring may be outsourced; however accountability remains with the system owner/operator.
6. If full operations cannot be sustained due to an incident, operations should be gracefully degraded in a defined order of precedence (i.e., protection is more important than control, control is more important than monitoring, etc.).

3.3 Failure Modes

Failure analysis for roles is done by examining undesired transitions of the state machine model for each role. This analysis is restricted in most cases to a single transition that causes a change in a single state variable, though analysis is extended to two transitions involving two state variables in special cases.

Failure analyses for security zones and communications infrastructure identify failure modes that could lead to a violation of the security principals and objectives or interfere with the functional goals of the substation automation system.

Failure analysis for security controls identifies failure modes that could stop recommended security controls from properly mitigating the other classes of failure modes.

Tables 6-9 collect all the failure modes that are identified through the four failure analyses. Each failure mode has a unique failure mode ID and a short definition of the failure mode. It should be noted that the failure mode ID number does not imply any kind of priority assignment.

3.3.1 Role-Based Failure Modes

Table 6 presents the superset of failure modes that can be applied to the roles within the substation automation system.

Table 6 – Role-Based Failure Modes

Failure Mode ID	Failure Mode
FR1	User loads unauthorized code on [Role]
FR2	[Role] executes existing code that should never be executed
FR3	Authorized user loads/accepts unauthorized code on [Role]
FR4	Improperly identified user (incorrect or elevated privileges) loads unauthorized code on [Role]
FR5	[Role] executes unauthorized mobile/active code
FR6	[Role] executes unauthorized code from mobile device
FR7	[Role] executes unreliable (authorized, but not tested) code
FR8	[Role] is poorly implemented, allowing instruction pointer compromise (e.g., buffer overflow)
FR9	[Role] is poorly implemented and starts/restarts in an unknown state
FR10	[Role] does not adequately manage memory (i.e., capacity and integrity) (e.g., memory leaks, bad initialization)
FR11	[Role] receives message from unknown sender (includes unauthenticated sender)
FR12	[Role] receives message from unexpected sender
FR13	[Role] incorrectly acts on, interprets, or discards data not synchronized with [Role]'s clock
FR14	[Role] processes user input without sufficient validation (e.g., syntactic, semantic; timing...)

Failure Mode ID	Failure Mode
FR15	[Role] processes message input without sufficient validation (e.g., syntactic, semantic; timing...)
FR16	[Role] uses incorrect or corrupt corroboration data for validation of message sender
FR17	[Role] does not have access to sufficient storage to perform its functions
FR18	[Role] Improperly manipulates data
FR19	Authenticated user performs unauthorized action on [Role]
FR20	Unauthorized user successfully guesses credentials to account
FR21	Role does not sufficiently distinguish between users
FR22	[Role] enables improper use of authorized session / enables session hijacking
FR23	[Role]'s login interface enables unauthorized account access
FR24	[Role] experiences unexpected process restart or shutdown
FR25	[Role] uses incorrect / improper data for evaluation during processing
FR26	[Role's host] supplies data to application that is false
FR27	[Role] improperly manages its data store (e.g., unneccessarily overwriting data)
FR28	[Role] does not have access to sufficient processing resources to perform its functions on time
FR29	[Role] does not have access to sufficient memory to perform its functions
FR30	[Role's host] does not adequately manage memory integrity
FR31	[Role] does not have access to sufficient communications resources (e.g., NIC) to perform its functions on time
FR32	[Role] sends spurious message
FR33	Authorized user misconfigures [Role] settings

3.3.2 Communication Failure Modes

Table 7 presents failure modes that would undermine the four primary communications objectives listed in Section 3.1.2. Column 1 of this table contains failure mode IDs. The second column is the description of each failure mode. The third column gives an example of the failure mode. The table's fourth column lists the communication objective violated by the failure mode.

Table 7 – Communication Failure Modes

Failure Mode ID	Failure Mode	Example	Objective
FC1	Message to or from [Role] is blocked, dropped, or delayed because the network is saturated	DDoS, Spurious message generation, Authorized network device consuming network resources	1
		Network under-provisioned; network over-allocated (e.g., addition of devices/functionality over time)	1
FC2	Message to or from [Role] is blocked, dropped, or delayed because of interference on the network medium	Insufficient signal-to-noise ratio, electromagnetic interference	1(a)
FC3	Message to or from [Role] is blocked, dropped, or delayed because a device or service in the network infrastructure is not available or functional	Incorrect firmware update, DNS not available	1(a)
FC4	Message to or from [Role] is inappropriately blocked by a network device	Incorrect configuration. Traffic is getting to a router or switch, but protocol parameters are incorrect (e.g., frame size, baud rate, data rate).	1(a)
FC5	Unauthorized device views messages through unauthorized access to transmission medium (logical or physical access)	Wiretap, wireless snooping, incorrect network configuration, unauthorized use of communication port	3(a)
FC6	Message delivered to unintended (additional) recipients due to misuse of broadcast or multicast protocol	Incorrect network configuration	3
FC7	Inappropriate connection between networks allows information to leak between domains	Unauthorized bridge between networks established in end device, cable inadvertently installed between switches in separate networks.	3
FC8	Message is delayed or exposed to unintended recipients because network infrastructure routes traffic over inappropriate path	Network device advertising incorrect network, duplicate IP address, network device sends message to wrong interface, incorrect metrics in router configuration	1, 3
FC9	Network accepts a message from an unauthorized source	Rogue device attaches to network	4
FC10	Network accepts an unauthorized message type	Device sends message using unauthorized protocol	4
FC11	Message attributes (header or payload) are corrupt or manipulated	Unauthorized/erroneous modification of message header	2

Failure Mode ID	Failure Mode	Example	Objective
FC12	Network device is subverted to mis-handle (e.g., block, delay, mis-route, inject, or manipulate) communications.		1, 2, 3, 4

3.3.3 Zone-Based Failure Modes

Table 8 presents the failure modes associated with the zones in the substation automation architecture. These are the specific failure modes related to violations of the operational requirements associated with the cluster of roles within each zone. A Zone may be Protection, Local, Supervisory, Field, or Enterprise.

Table 8 – Zone-Based Failure Modes

Failure Mode ID	Failure Mode	Example	Zone Objective Violated by Failure Mode
FZ1	Messages required for system protection do not arrive in a timely manner	Overloaded network or device (throughput)	LR-1 (Protect: O-3)
FZ2	Coordination among replicated, redundant, and/or independent roles within protection zone (i.e., coordinated protection scheme) produces incorrect result.	Compromise of 1 out of 1+ redundant devices;	Protect: O-5, O-8
FZ3	Protection function misoperates due to incorrect data.	Interception/injection of specific protection messages (due to rogue device on protection network);	Protect: O-3, O-4
FZ4	Protection function not available or deficient due to device failure or compromise.	Protective relay compromised, removing it from service – no redundant device; multiple devices of same type disabled by class break; failover switch compromised, preventing backup device from providing coverage;	Protect: O-5
FZ5	Loss of communication with roles outside the zone or subzone prevents Role from performing core functionality	Core functionality fails due to data disruption or delay caused by comm failures to/from outside the zone or subzone; A process gets hung waiting for a response from outside the zone or subzone. (Does not have appropriate timeout.)	Protect: O-2

3.3.4 Security-Control-Based Failure Modes

Table 9 presents a set of failure modes that violate the primary security objective for the protection of security functions, as described in Section 3.1.4. "The integrity, confidentiality, and availability of the information needed to make and execute proper security decisions (including recovery from adverse security events) must be protected." The failure modes are derived directly from the statement of the security objective, by negating the desired outcome.

In Table 9, this document uses the term "security information" as shorthand to represent "information needed to make and execute proper security decisions."

Table 9 – Failure Modes for Security Functions

Failure Mode ID	Failure Mode	Example	Security Objective Violated by Failure Mode
FS1	Integrity of security information is compromised.	Password files are tampered with. Log files are corrupted.	Security Function Protection
FS2	Security information is not available.	Forensic information is deleted by an unauthorized user or never collected.	Security Function Protection
FS3	Confidentiality of security information is violated.	Passwords are stored, or transmitted, in clear text.	Security Function Protection

4 Security Controls

This section defines the set of recommended security controls for substation automation systems and components as they satisfy the functionality of the roles delineated in Section **Error! Reference source not found.**. Many of the security controls in this document are inspired by and intended to cover the technical requirements found in NIST IR 7628 as applied to substation automation technology. The controls presented herein may then, in turn, be satisfied by communications protocol definition-level standards and manufacturing specifications.

This section first defines the full set of recommended security controls and the failure modes from Section **Error! Reference source not found.** that each control addresses. Next, it presents the recommended allocation of each security control to elements of a substation automation system (e.g., to specific roles or elements of the underlying network infrastructure). Finally, each failure mode from Section **Error! Reference source not found.** is presented and mapped against the set of security controls that are recommended as mitigations for each failure mode.

4.1 Control Definitions

The process for defining the controls in this document was based on an analysis of the roles, their state transition models, and failure modes as defined in this profile, along with careful examination of the NIST IR 7628, the Distribution Management Security Profile, and other collections of security standards and best practices. The process for deriving the controls included the following steps (with natural iteration and review):

1. Examine each failure mode to determine potential security controls that provide mitigation. Candidate security controls were drawn from the Distribution Management Security Profile and WAMPAC Security Profile.
2. Review the set of candidate security controls for coverage. Draft new controls for aspects of a failure mode that are not adequately mitigated. Remove or consolidate redundant and overlapping candidate controls.
3. Re-write the remaining controls to specialize for substation automation. Verify, augment, or correct the mapping of each re-written control to the substation automation failure modes.
4. Allocate each control to substation automation system elements (e.g., roles or network infrastructure).
5. Map each control against the technical requirements in the NIST IR 7628. Assess coverage of technical requirements in the NIST IR 7628 by the substation automation controls.
6. Perform a gap analysis to identify missing failure modes. Each security control in the NIST IR 7628 is mapped against security controls in this security profile; any security controls that are not addressed in this profile fell into one of two categories.
    - the gap pointed to a missing security control that should be included in this security profile. In such cases, the failure mode analysis was revisited and the gap was addressed from failure mode forward to new security controls.
    - the gap pointed to an issue that was not in the scope of this security profile, and the rational was documented in Appendix A:.

This document does not attempt to cover general information technology cyber security, cyber security best practices for other control systems, or organizational-level cyber security requirements that would apply to all or multiple smart grid systems. Substantial guidance is already available on these subjects, and may be found in such documents as:

- COBIT – the Control Objectives for Information and related Technology is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations. COBIT emphasizes regulatory compliance, helps organizations to increase the value attained from IT, enables alignment and simplifies implementation of the COBIT framework. (http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx)
- ISO 27000 series – consists of several parts numbering from 27001 – 27006 that provide a specification for an information security management system (ISMS). This work supersedes the BS7799 standard. (http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41933)
- ITIL (Information Technology Infrastructure Library) - ITIL is a widely adopted approach for IT Service Management in the world. It provides a practical, no-nonsense

framework for identifying, planning, delivering and supporting IT services to the business. (http://www.itil-officialsite.com)

- NIST SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations – provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government to meet the requirements of FIPS 200, Minimum Security Requirements for Federal Information and Information Systems. The guidelines apply to all components of an information system that process, store, or transmit federal information. (http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf)

This document's primary point of reference for broader cyber security guidance is the NIST IR 7628, and as such, these controls do not address the requirements in the NIST IR 7628 as applied to the organization. The controls herein are strictly focused on detailed recommendations for building and implementing substation automation systems and technology where guidance may not be found in other broadly accepted reference material.

Table 10 defines technical security controls that, if implemented, will improve the security of substation automation systems. They include:

- **Control ID:** This ID is short identifier for cross-referencing.
- **Control Name:** This is a short description of the intent of the security control.
- **Control Definition:** This text defines the control itself.
- **References:** These are the requirements from the NIST IR 7628 that are partially or fully satisfied by the control.
- **Failure Modes:** The failure modes from Section **Error! Reference source not found.** that are addressed by the control. As a reminder, failure modes beginning with FR are role-based failure modes (see Section **Error! Reference source not found.**), those beginning with FC are communication-based failure modes (see Section 3.3.2), and those beginning with FZ are zone-based failure modes (see Section **Error! Reference source not found.**).

Table 10 – Control Definitions

Control ID	Control Name	Control Definition	References	Failure Mode ID
AAM	Automated Account Management	The system shall provide the ability to centrally manage user accounts including deactivation of inactive and terminated users. User accounts shall identify the individual user and authorized role(s). The system shall create an audit trail of account creation, modification, disabling, permission changes, and termination.	SG.AC-3	FR21, FC4, FC12, FS2

Control ID	Control Name	Control Definition	References	Failure Mode ID
AE	Access Enforcement	<Role|device> shall enforce access control policies and associated privileges for users and devices based on identity, role, and attributes. The <role|device> shall be able to limit the services accessible by users and devices.	SG.AC-4, SG.AC-15	FR18, FC4, FC12
AF	Authenticator Feedback	<Role> shall obscure the feedback of authentication information during the authentication process, for example by masking passwords and providing login failure messages that do not reveal valid user accounts.	SG.IA-6	FR23, FS3
AVC	Alternate Value Comparison	<Role> shall (1) utilize an independent means (alternate data sources and/or computations to derive equivalent values) to validate the integrity of power system information utilized as input for decision making by protection or critical automated control applications, (2) continually compare independently derived results, and (3) have procedures in place to handle inconsistencies that are deemed to be significant according to organizationally defined criteria.		FR25
BPR	Backup Power Requirement	Components essential for closed loop control functions shall be capable of operating for a minimum of 1 hour upon loss of primary power source. This requirement can be met by the use of a UPS, battery backup, or alternate power source.	SG.PE-9	FR24, FC3
CAR	Content of Audit Records	<Role|device> shall produce audit records for each event with information including 1) date and time of the event, 2) the identity of the user/<role>/component where the event occurred, 3) type of the event, 4) the identity of the user/<role>/component that detected the event, and 5) known details of the event including location (logical and physical). The system shall have the capability to centrally manage content of audit records generated by individual roles/components. Minimal set of auditable events includes: access (whether central, remote, logical, physical, emergency, authorized, or unauthorized), unsuccessful authentication, change in configuration, and health and resource warnings. The list of auditable events and audit records shall be reviewed periodically.	SG.AU-3, SG.AU-15	FS2

Control ID	Control Name	Control Definition	References	Failure Mode ID
CCf	Communication Confidentiality	<Role> employs FIPS 140-2 compliant cryptographic mechanisms to prevent unauthorized disclosure or modification of management (including electronic authenticator distribution) and configuration data during transmission. Latency induced from the use of cryptographic mechanisms must not degrade the operational performance of <role>.	SG.SC-9	FC5
CCp	Communications Consumption	The <Role's host> shall implement communications monitoring and control mechanisms to identify and mitigate communications activity (e.g., one <Role> monopolizing access to the NIC) that inhibits the function of any <Role> on <Role's host>	SG.SC-6	FR31
CFA	Configuration File Authenticity	<Role> shall only accept message payloads containing configuration files (including calibration) that are cryptographically signed by an explicitly trusted source. Acceptable technologies shall be specified by FIPS 186.	SG.CM-2, SG.CM-3, SG.SI-7	FR33
CFSD	Configuration File and Sensitive Data Integrity Check	Configuration files and other sensitive data should include FIPS 180-3 cryptographic integrity checks (e.g., cryptographic hashes) and the integrity of the file should be checked whenever it is read by an application.	SG.CM-2, SG.CM-3, SG.SI-7	FR16, FR18, FR25, FR33
CI	Communication Integrity	The <role> employs FIPS 180 compliant hashing mechanisms and FIPS 186 compliant digital signature on all transmissions to facilitate detection of unauthorized modification of information and verify the identity of sender. Latency induced from the use of hashing or signature mechanisms must not degrade the operational performance of the <role>.	SG.SC-8, SG.SC-20	FC11
CKIM	Cryptographic Key Implementation and Management	The system shall provide an automated mechanism to establish and manage (e.g., create, distribute, renew, backup, and revoke) cryptographic keys.	SG.SC-11, SG.SC-15	FC11
CMA	Cryptographic Module Authentication	<Role|device> shall employ FIPS compliant cryptographic module authentication for authenticating users and devices. <Role|device> shall use Trusted Platform Modules (TPMs) or Hardware Security Modules (HSMs) for device and user identification and authentication.	SG.IA-4, SG.IA-5, SG.SC-3, SG.SC-12, SG.SC-20	FR4, FR11, FR21, FC12

Control ID	Control Name	Control Definition	References	Failure Mode ID
CoM	Communications Monitoring	The system shall provide operator visibility and appropriate alerting for <Role's host's> communications activity, including per <Role> use of network interfaces, status of queues, and message transmit/receive rates.	SG.AC-15, SG.SI-4	FR31
CRDI	Clock Record and Discrepancy Identification	<Role> clock shall record time source used for synchronization and when last synchronized, and shall continually compare 2 or more external time sources to local clock and flag if deviation exceeds an organizationally defined time window (e.g., 3 ms)	SG.AU-8	FR13
CrM	Credential Management	The system shall provide a single point of initiation to distribute, manage, and revoke all logical and physical access credentials for all substation systems and components. Revocation shall be carried out on all systems within 24 hours.	SG.AC-15, SG.PE-3	FR16, FC4, FC5, FC9, FC12
CSM	Concurrent Session Management	<Role> limits the use of concurrent sessions for any user, device, or application. The number of concurrent sessions shall be limited to the minimum necessary for proper operation of the system. (More than 1 concurrent session requires justification.)	SG.AC-11	FR28, FC3
CSW	Configured Size Warnings	The administrator of the data store shall be notified immediately when the logical media becomes 75% full and again when it is 95% full by default, modifiable by the organization.		FR17
CuC	Current Configuration	A designated system or systems shall daily or on request obtain current version numbers, installation date, configuration settings, patch level on <role|device> and compare these with recorded values in the inventory and configuration databases. All discrepancies shall be logged and alerts shall be generated where appropriate.	SG.CM-2, SG.CM-3, SG.CM-6, SG.CM-8, SG.SI-7	FC4, FC6, FC8, FR18, FR25

Control ID	Control Name	Control Definition	References	Failure Mode ID
DUF	Disabling Unnecessary Functions	The system shall ensure that only the minimum functionality, networking, and communication services required for the proper operation and maintenance of <role> are enabled. The full set of allowable functions and services shall be documented, verified at deployment, and verified at an organization-defined frequency thereafter. All non-essential functions shall be uninstalled, removed, or never installed. All networking and communication capabilities not required for the operation or maintenance of <role> (including unused ports and modems) shall be disabled. Agreements with vendors shall specify that all wireless options be set to "off" by default and every modem port and LAN port shall be disabled by default. The organization shall carry out random sample audits upon delivery to verify that initial default configurations are as agreed upon.	SG.AC-16, SG.CM-7, SG.SA-7, SG.SC-13, SG.SC-17, SG.SC-23	FR24, FR28
EI	Endpoint Isolation	The system shall provide the capability to isolate compromised devices from the rest of the system upon detection of compromise.	SG.SC-5, SG-SC-30	FR1, FR19, FC1, FC9, FC12
ENS	Emergency Network Segmentation	If an attack is detected, the system shall label all traffic from compromised network segments as potentially malicious, and provide tools to isolate the compromised segment from network segments that are confirmed as trustworthy and defensible.	SG.AC-5, SG.SC-5, SG.SC-30	FC1
ES	Endpoint Security	<Roles> using a general purpose operating system shall implement end point security mechanisms to scan software for malicious code.	SG.SI-3, SG.SI-4	FR2
ESP	EMI/Surge Protection	Network devices located within or nearby power distribution equipment shall be resistant to EMI and heavy electrical surges that can be expected within an electrical substation. Purchasing equipment that meets IEEE 1613 or IEC 61850-3 specifications will satisfy this requirement.		FC2
FDC	Factory Default Credentials	The system shall force a change of all factory default access and authentication credentials on <role|device> upon installation.	SG.CM-10	FR21, FC12

Control ID	Control Name	Control Definition	References	Failure Mode ID
GD	Graceful Degradation	Zones shall provide all functionality designated by the organization as essential to operations in the event of loss of communication with lower tier zones according to Table 2: Zone Prioritization Tiers.	SG.CP-11, SG.SC-22, SG.SC-30	FZ5
GSRP	GOOSE and SMV Replay Protection	<Roles> in the Protection Zone shall implement message replay detection mechanisms as specified in IEC 62351-6 Sections 7.2.1.5 and 7.2.1.6.		FZ3
HM	Health Monitoring	The system periodically interrogates and validates current connectivity by observing communication from <role> on at least a daily basis. All results shall be recorded in an associated log file. Any results indicating an error (as determined by preset conditions) shall alert the system manager.	SG.SI-4	FR24
ID	Intrusion Detection	The system shall detect anomalous events within network segments and across network segment boundaries. This detection shall be protocol aware. Sources of information about anomalous events can be the network or data logs. Intrusion detection systems have false positives so the alarms generated by the intrusion detection systems shall be screened by an experienced person to determine validity of alarms prior to any responsive action being taken.	SG.SI-4	FR32, FC9, FC11
IPC	Isolation of Protection Communications	All <roles|devices> in the Protection Zone shall isolate Protection traffic from non-Protection traffic using VLANs (IEEE 802.1Q) or physically dedicated networks. All <roles> shall assign all traffic to the appropriate network.	SG.AC-5, SG.SC-30	FZ1
IUA	Inappropriate User Activity	The <role> shall monitor all user activity and report indications of inappropriate or unusual activity as defined by the organization.	SG.SI-4	FR1, FR18, FR19, FC12
IW	Interaction Whitelisting	All <role hosts> shall maintain a list of origins and destinations, with corresponding acceptable message types for each origin and destination, for incoming and outgoing messages. The <role host> shall only send and accept messages compliant with this list. The <role host> shall afford this list the same protections as configuration data.	SG.AC-5, SG.AC-19, SG.SC-5, SG.SI-3	FR12, FR32, FC9, FC10

Control ID	Control Name	Control Definition	References	Failure Mode ID
LFCA	Limited Field Component Access	Supporting systems shall control physical access to devices and network infrastructure (including cables) at all times. This can be accomplished by installation of components within a substation control building, a lockable cabinet, or a wiring closet. The mechanism used for physical access shall provide unique credentials per user which shall be authorized on a per lock basis. Periodic reauthorization shall be required at least every 24 hours and shall automatically expire by default if not re-authorized.	SG.PE-3	FC4, FC5
LP	Least Privilege	<Role|device> shall grant each user, process, or service within a system the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. User roles (or groups) shall be defined in a granular fashion such that job functions do not overlap (separation of duties). User roles and groups shall always include a dedicated user role or group for auditing and log maintenance that has no other obligations or job functions, and no other user role or group shall include the functions of auditing or log maintenance. Remote access privilege shall be approved only when necessary to meet the operational needs of the <role|device>.	SG.AC-1, SG.AC-3, SG.AC-6, SG.AC-7, SG.AC-19, SG.CM-5, SG.SC-19	FR1, FR18, FR19, FC4, FC12
MeC	Memory Consumption	The <Role's host> shall implement memory monitoring and control mechanisms to identify and mitigate memory consumption (e.g., memory leaks) that inhibits the function of any <Role> on <Role's host>	SG.SC-6	FR29
MIC	Manual Input Checking	The <role> employs mechanisms to check manual input for accuracy, completeness, validity, and authenticity.	SG.SI-8	FR14
MId	Message Identities	<Role> shall include in every message the identity of the sender and the intended recipient(s). The mechanisms used to meet the requirement of this control are intended to be applied within the message payload. Data link layer (layer 2) and/or Network layer (layer 3) addressing is not sufficient by itself to meet the requirement of this control.	SG.SC-20	FR11
MIs	Memory Isolation	<Roles> deployed on the same host shall execute in separate processes. Use of shared memory segments for communication shall be minimized.	SG.SC-29	FR30

Control ID	Control Name	Control Definition	References	Failure Mode ID
MM	Memory Monitoring	The system shall provide operator visibility and appropriate alerting for <Role's host's> memory use, including available memory and memory use per <Role>.	SG.SI-4	FR29
MoC	Mobile Code	<Role|device> shall not accept mobile/active code technologies such as JavaScript, ActiveX, Flash, Java Applets, etc. The system shall actively detect and prevent any unauthorized code from executing on <role|device>. All use of mobile code shall be monitored.	SG.SC-16	FR5, FC12
MT	Message Timestamping	<Role> shall time stamp all configuration and management messages that it sends.		FR13
MV	Message Validation	<Role> shall validate all application protocol fields that it uses for logical and expected values including source, destination, time stamps, quality flags, and state indicators. <Role> shall use whitelisting of message types within a protocol along with message context and history when assessing the validity of the message.	SG.SI-8	FR15, FR24, FR25
NAE	Network Access Enforcement	All network infrastructure shall refuse all messages from unauthenticated and unauthorized devices, excepting requests for authentication and authorization.	SG.AC-16, SG.AC-17, SG.AC-19, SG.SC-5, SG.SC-18	FC5, FC9
NMP	Network Monitoring and Provisioning	The Network shall implement QoS monitoring to identify and alert instances of (and keep long-term records of) communications activity (e.g., one <Device> monopolizing bandwidth) that inhibit the function of any <Device>.		FC1
NOC	Network Operations Continuity	The system shall provide a means to compensate for loss of a single component of network infrastructure without loss of system functionality.	SG.CP-8	FC3
NSA	No Shared Accounts	The system shall assign unique identifiers to all individuals and connected systems or devices and associate each individual account (no duplication or sharing) with an account group/user group for proper auditing, management, and tracking. Wherever possible, globally privileged accounts (e.g., SuperUser accounts, Administrator, or Root) shall be disabled and/or removed.	SG.AC-3, SG.IA-4, SG.IA-5	FR4, FR11, FR21, FC12

Control ID	Control Name	Control Definition	References	Failure Mode ID
P	Prioritization	<Role> shall queue and schedule processing of messages using the following criteria: (1) Config messages shall be processed in the order in which they are received, (2) Operate messages shall be processed after all latency-constrained Config messages, and then in the order in which they are received, and (3) Inform messages shall be process after all latency-constrained Operate and Config messages, and then in the order in which they are received. Messages that may not wait for another message to be processed without violating their latency criteria shall be considered latency-constrained.	SG.SC-6	FR28
PaM	Password Management	<Role|device> enforces the use of strong user passwords, in accordance with FIPS 112, and protects user passwords from potential exposure. This includes: 1. Ensuring that passwords never cross component boundaries in the clear. 2. Ensuring that passwords are never stored in the clear and that stored password hashes use a cryptographic one-way hash function in accordance with FIPS 180-2. 3. Ensuring that passwords are never included in or allowed to be embedded into tools, source code, scripts, URLs, aliases, or shortcuts. 4. Enforcing password complexity policies (minimum length of at least 10 characters with a combination of lower/upper case, numerals, and special characters). 5. Changing passwords at defined intervals and minimizing reuse. 6. Expiring passwords after defined intervals of inactivity. 7. Protecting the password store from unauthorized modification.	SG.AC-21	FR20, FC12, FS3
PC	Processor Consumption	The <Role's host> shall implement process monitoring and control mechanisms to identify and mitigate processor consumption (e.g., runaway or starved processes) that inhibits the function of any <Role> resident on <Role's host>	SG.SC-6	FR28

Control ID	Control Name	Control Definition	References	Failure Mode ID
PDA	Portable Device Attachment	The system limits attachment of portable devices and media to allow only specifically authorized users to do so. The default state shall disable all access from portable devices and media. Attachment of portable devices and media shall be enabled only where it is necessary for operation and/or maintenance functions. The system prevents the automated execution of code located on portable media. Mobile devices traveling to high risk locations shall be appropriately labeled, hardened, and subsequently sanitized upon return; i.e., such mobile devices shall contain only minimal information required to conduct business during the use period.	SG.AC-17, SG.SC-4, SG.MP-3	FR6, FC12
PFP	Protection Function Preservation	Individual <Protection Applications> shall continue to provide functions designated by the organization as essential to operations in the face of the loss or compromise of any single device, communications link, or message in the overarching protection scheme.[7]	SG.SC-22	FZ2, FZ4
PrM	Processor Monitoring	The system shall provide operator visibility and appropriate alerting for <Role's host's> processor activity, including available CPU capacity and processor use per <Role>.	SG.SI-4	FR28

[7] Common mode failures (or "class breaks") are not covered by this control. If protection against common-mode failures is desired, the asset owner should consider heterogeneous solutions.

Control ID	Control Name	Control Definition	References	Failure Mode ID
PSI	Protection of Security Information	The system shall protect all sensitive information involved in the execution of security functions from unauthorized access or action. Sensitive information shall at a minimum include: • User Account Information • User and Device Privileges • Cryptographic Material (including keys, hashes, and certificates) • Non-Cryptographic Credential Data (including biologically-based credentials) • Audit Records • Configuration Files • System Backups Access to all sensitive information shall be controlled in accordance with Least Privilege (LP - defined herein). Storage of all sensitive information shall be controlled in accordance with Configuration File and Sensitive Data Integrity Check (CFSD) and Software and Firmware Authenticity (SFA). All cryptographic material shall be stored and managed in accordance with NIST 800-57 and FIPS 140-2. Additionally, storage of User Account Information and Non-Cryptographic Credential Data shall be encrypted using a FIPS 140-2 approved cryptographic module. Transmission of all sensitive information shall be controlled in accordance with Communications Confidentiality (CCf) and Communications Integrity (CI).	SG.SC-26, SG.AU-9	FS1, FS2, FS3
PW	Process Whitelisting	<Role> shall be configured with a process white list to restrict processes to only those necessary to support the <role's> function.		FR2, FR26
QSE	Quality of Service Enforcement	The network shall process all traffic in accordance with the QoS resource reservation identifier (i.e., IEEE 802.1Q Priority Tag).	SG.SC-6	FC1

Control ID	Control Name	Control Definition	References	Failure Mode ID
QSS	Quality of Service Specification	<Role> shall specify the IEEE 802.1Q priority tag in accordance with IEC 62351-6 Section 7 on all outgoing messages. All protection-related traffic originating in the protection zone shall be tagged with priority 4-7. All traffic not essential to power system operations (e.g., enterprise visibility data) shall be tagged with priority 0. All other substation traffic shall be tagged with priority 1-3.	SG.SC-6	FC1
RD	Replacement of Data	<Role> shall provide a mechanism for the user to select a replacement policy for data in its store. By default, the policy gives priority to newer data, which will replace older data when storage is exhausted. <Role> shall also provide mechanism to indicate which data should never be deleted.		FR17, FR27
RIS	Remote Interactive Sessions	All remote user-interactive sessions to <role> shall be encrypted using FIPS 140-2 compliant mechanisms, including all administrative and maintenance activities.	SG.AC-1, SG.AC-15, SG.SC-9	FR22, FC3, FC5, FC12
SCP	Secure Coding Practices	Software components shall be developed in accordance with secure coding standards (e.g., the CERT Secure Coding Standards or OWASP Development Guide) for avoidance of cataloged coding flaws and weaknesses (e.g., the NIST SAMATE Reference Dataset or the MITRE Common Weakness Enumeration). Compliance can be demonstrated through code inspections or use of static analysis tools.	SG.SA-8, SG.SC-4, SG.SI-3	FR8, FR10, FC12
SD	Session Duration	The system: 1. Prevents further user access to the system by expiring or terminating the session after no more than 15 minutes of inactivity with appropriate safety considerations. 2. Sessions must be reestablished using identification and authentication procedures specified herein. 3. The existing information on the display shall be obfuscated during session lock.	SG.AC-12, SG.AC-13	FR22, FC3, FC5, FC12
SFA	Software and Firmware Authenticity	<Role> shall not accept software or firmware updates that do not have cryptographically signed message payloads, nor shall a system execute any software or firmware before validating its cryptographic signature. Acceptable technologies shall be specified by FIPS 186.	SG.SI-7	FR3, FR26, FC12

Control ID	Control Name	Control Definition	References	Failure Mode ID
SIC	Storage Integrity Check	<Role> shall perform automated checks to validate the integrity of the logical and physical media on a periodic basis as defined by the organization, in no cases exceeding 1 week between checks. Integrity checks shall verify the media is in adequate condition to perform the functions assigned to <role>, and shall immediately report any abnormalities or problems discovered during the scan to the administrator of <role>.	SG.SI-7	FR27
SId	Self-Identification	The <role> shall be able to report identifying information of the software and hardware upon request, consistent with Access Controls identified in this document. This shall at a minimum include unique identifiers for device hardware and instance of the software responding to the request, and shall include at least one element that is uniquely dependent on the component contents such as a FIPS 186 compliant hash value for the component.		FR25
SIn	Systems Inventory	The system shall create and maintain (on at least a daily basis) an inventory of applications and devices that includes information that uniquely identifies each component, such as manufacturer, type, serial number, version number, and location (logical and physical).	SG.CM-8	FC4
SKS	Startup in Known State	<Role> shall start up in a known state that is safe and secure in accordance with system requirements set by the organization.		FR9
SM	Storage Monitoring	The <Role's host> shall implement data storage monitoring and control mechanisms to identify and mitigate storage consumption (e.g., unbounded log file growth) that inhibits the function of any <Role> resident on <Role's host>. The system shall also provide operator visibility and appropriate alerting for <Role's host's> available storage and activity, including available disk space and disk use per <Role>.	SG.AU-3, SG.AU-4, SG.SC-6, SG.SI-4	FR17

Control ID	Control Name	Control Definition	References	Failure Mode ID
SNAR	Secure Name / Address Resolution	The network infrastructure signs data that it returns in response to name/address resolution queries using a FIPS 186 compliant mechanism. Before using this data, the recipient shall use the digital signature to determine the authenticity and integrity of the host/service name to network address resolution information. The name / address resolution service shall reside logically within the substation network and the host of this service shall reside physically within the substation.	SG.SC-5, SG.SC-21	FC8
SR	System Restoration	The system shall have the ability to recover <role|device> from securely maintained backups, images, and configurations in the event of compromised device(s) or network (exception: hardware changes).	SG.CP-10	FS1, FS2
TCF	Traffic Control and Filtering	The system shall enforce the flow of information into, out of, and within the network by placing boundary protection devices (e.g., proxies, gateways, firewalls, and routers) at designated network segment boundaries. These firewalls shall control (i.e., filter) all traffic passing between network segments, using “deny unless specifically permitted” policies. The system shall restrict "permit" rules to the smallest number of endpoints, workstations, devices, and services possible.	SG.AC-5, SG.AC-19, SG.CA-4, SG.SC-5, SG.SC-7, SG.SC-18, SG.SC-30, SG.SI-3	FC1, FC6, FC7, FC8, FC10
TFA	Two-Factor Authentication	<Role> shall require a minimum of two independent types of authentication for human interaction. Valid types of authentication include known information (e.g., passwords and passphrases), physical possession (e.g., physical security tokens), and inherent characteristics (e.g., biometrics).	SG.AC-21	FR20, FC12
TU	Testing Updates	The system shall include an isolated environment that replicates the configuration and behavior (including being afforded the same protections) of the actual architecture and environment for testing and scanning of updates to firmware, software, and configuration prior to deployment to determine effectiveness and potential side effects.	SG.SA-10	FR7, FR33

Control ID	Control Name	Control Definition	References	Failure Mode ID
ULA	Unsuccessful Login Attempts	The system: 1. Enforces a limit of an organization-defined number of consecutive invalid access attempts (i.e., user logins and system-to-system connections) during an organization-defined time period. 2. When the maximum number of unsuccessful attempts is exceeded, automatically locks the account/node for an organization-defined, exponentially increasing time period or until released by an administrator with appropriate safety considerations (e.g., emergency override). 3. When automatic locks are triggered, alerts shall be raised to the administrator. 4. Notifies the user of the previous successful logon date/time and the number of unsuccessful logon attempts since that date/time upon successful login.	SG.AC-3, SG.AC-8, SG.AC-9	FR23, FC3, FC5, FC12
VE	VLAN Enforcement	The network shall segment traffic in accordance with the Virtual Local Area Network identifier (i.e., IEEE 802.1Q VLAN Tag).	SG.AC-5, SG.SC-30	FZ1

4.2 Security Controls Mapping

Table 11 presents the recommended allocation of the security controls from Section **Error! Reference source not found.** to elements of a substation automation system. In the event that a control cannot be implemented on the indicated elements, the organization should implement mitigating controls addressing the same failure modes (as noted in Table 10), note the exception, and provide the rationale (e.g., a risk analysis) that demonstrates why the alternative control is sufficient to mitigate the risk.

The first two columns identify each security control with its ID and name; the corresponding control definition can be found in Table 10. The remaining columns identify different elements of a substation automation system that could implement a security control.

- The first nine columns correspond to the roles of the logical architecture, as defined in Sections 2.1 and 2.2. In some cases, a control that is allocated to a role should be implemented by the role itself; in other cases, the control should be implemented on the role's host. These differences are noted in the definition of the individual security controls in Table 10. An "X" in a cell means that the identified role should implement the identified security control.
- The final column represents the various elements of network infrastructure, such as routers and firewalls. An "X" in a cell means that SA network infrastructure should implement the identified security control. Instances where not all network infrastructure must satisfy the control are annotated by footnotes.

Table 11 – Control Mapping

Control ID	Control Name	Actuator	Sensor	Protection Application	Control Application	Monitoring Application	Substation Information Repository	Proxy	Substation Control Authority	Substation User Interface	Network Infrastructure
AAM	Automated Account Management		x	x	x	x	x	x	x	x	x
AE	Access Enforcement		x	x	x	x	x	x	x	x	x
AF	Authenticator Feedback									x	
AVC	Alternate Value Comparison	x	x	x	x	x	x	x	x	x	
BPR	Backup Power Requirement	x	x	x	x	x		x			x
CAR	Content of Audit Records	x	x	x	x	x	x	x	x	x	x
CCf	Communication Confidentiality	x	x	x	x	x	x	x	x	x	
CCp	Communications Consumption		x	x	x	x	x	x	x	x	
CFA	Configuration File Authenticity	x	x	x	x	x	x	x	x	x	
CFSD	Configuration File and Sensitive Data Integrity Check	x	x	x	x	x	x	x	x	x	
CI	Communication Integrity	x	x	x	x	x	x	x	x	x	
CKIM	Cryptographic Key Implementation and Management	x	x	x	x	x	x	x	x	x	
CMA	Cryptographic Module Authentication	x	x	x	x	x	x	x	x	x	x
CoM	Communications Monitoring		x	x	x	x	x	x	x	x	
CRDI	Clock Record and Discrepancy Identification	x	x	x	x	x	x	x	x	x	
CrM	Credential Management		x	x	x	x	x	x	x	x	x
CSM	Concurrent Session Management	x	x	x	x	x	x	x	x	x	x
CSW	Configured Size Warnings						x				
CuC	Current Configuration	x	x	x	x	x	x	x	x	x	x
DUF	Disabling Unnecessary Functions	x	x	x	x	x	x	x	x	x	
EI	Endpoint Isolation	x	x	x	x	x	x	x	x	x	x
ENS	Emergency Network Segmentation	x	x	x	x	x	x	x	x	x	x[8]
ES	Endpoint Security	x	x	x	x	x	x	x	x	x	
ESP	EMI/Surge Protection										x

[8] The system must implement at least one instance

Control ID	Control Name	Actuator	Sensor	Protection Application	Control Application	Monitoring Application	Substation Information Repository	Proxy	Substation Control Authority	Substation User Interface	Network Infrastructure
FDC	Factory Default Credentials	x	x	x	x	x	x	x	x	x	x
GD	Graceful Degradation	x	x	x	x	x	x	x	x	x	x
GSRP	GOOSE and SMV Replay Protection	x	x	x							
HM	Health Monitoring	x	x	x	x	x	x	x	x	x	
ID	Intrusion Detection										x
IPC	Isolation of Protection Communications	x	x	x							
IUA	Inappropriate User Activity	x	x	x	x	x	x	x	x	x	x
IW	Interaction Whitelisting	x	x	x	x	x	x	x	x	x	
LFCA	Limited Field Component Access	x	x	x	x	x	x	x	x	x	x
LP	Least Privilege	x	x	x	x	x	x	x	x	x	x
MeC	Memory Consumption		x	x	x	x	x	x	x	x	
MIC	Manual Input Checking									x	
MId	Message Identities	x	x	x	x	x	x	x	x	x	
MIs	Memory Isolation		x	x	x	x	x	x	x	x	
MM	Memory Monitoring		x	x	x	x	x	x	x	x	
MoC	Mobile Code		x	x	x	x	x	x	x	x	x
MT	Message Timestamping	x	x	x	x	x	x	x	x	x	
MV	Message Validation	x	x	x	x	x	x	x	x	x	
NAE	Network Access Enforcement										x
NMP	Network Monitoring and Provisioning										x
NOC	Network Operations Continuity										x
NSA	No Shared Accounts	x	x	x	x	x	x	x	x	x	x
P	Prioritization		x	x	x	x		x	x		
PaM	Password Management							x		x	x
PC	Processor Consumption		x	x	x	x		x	x		
PDA	Portable Device Attachment	x	x	x	x	x	x	x	x	x	x
PFP	Protection Function Preservation			x							
PrM	Processor Monitoring		x	x	x	x		x	x		
PSI	Protection of Security Information	x	x	x	x	x	x	x	x	x	x

Control ID	Control Name	Actuator	Sensor	Protection Application	Control Application	Monitoring Application	Substation Information Repository	Proxy	Substation Control Authority	Substation User Interface	Network Infrastructure
PW	Process Whitelisting	x	x	x	x	x	x	x	x	x	
QSE	Quality of Service Enforcement										x
QSS	Quality of Service Specification	x	x	x	x	x	x	x	x	x	
RD	Replacement of Data						x				
RIS	Remote Interactive Sessions	x	x	x	x	x	x	x	x	x	x
SCP	Secure Coding Practices	x	x	x	x	x	x	x	x	x	x
SD	Session Duration	x	x	x	x	x	x	x	x	x	x
SFA	Software and Firmware Authenticity		x	x	x	x	x	x	x	x	x
SIC	Storage Integrity Check						x				
SId	Self-Identification	x	x	x	x	x	x	x	x	x	
SIn	Systems Inventory	x	x	x	x	x	x	x	x	x	x
SKS	Startup in Known State	x	x	x	x	x	x	x	x	x	
SM	Storage Monitoring						x				
SNAR	Secure Name / Address Resolution[9]	x	x	x	x	x	x	x	x	x	x
SR	System Restoration	x	x	x	x	x	x	x	x	x	x
TCF	Traffic Control and Filtering										x
TFA	Two-Factor Authentication	x	x	x	x	x	x	x	x	x	x
TU	Testing Updates	x	x	x	x	x	x	x	x	x	
ULA	Unsuccessful Login Attempts	x	x	x	x	x	x	x	x	x	x
VE	VLAN Enforcement										x[10]

4.3 Security Control Coverage

The following tables provide controls for each of the failure mode identified in Section **Error! Reference source not found.**. Each table is organized by failure mode, clearly identifying the set of security controls that collectively address each failure mode. All of the information found in this table is found elsewhere in this document, primarily in Table 11. Where Table 11 shows

[9] Only applies to roles and network infrastructure that use an address resolution service.

[10] Only applies to network infrastructure in the Protection Zone.

the mapping from security control to failure modes, these tables show the mapping from failure mode to security controls.

No new information is presented in this section; this organization is for the convenience of a reader wishing to examine the manner and degree to which the recommended security controls address each failure mode.

4.3.1 Role-Based Failures and Controls

Table 12 shows the set of security controls that are recommended to address each role-based failure mode identified in Section **Error! Reference source not found.**. The first two columns correspond to the ID and textual description of each role-based failure mode from Table 6. The last two columns correspond to the ID and name of security controls from Table 11. Each failure mode is mapped to one or more security controls; the combination of controls is recommended to mitigate the failure mode (i.e., it does not identify a set of options).

Table 12 – Role-Based Failure Modes and Controls

Failure Mode ID	Failure Mode	Control ID	Control Name
FR01	User loads unauthorized code on [Role]	EI	Endpoint Isolation
		IUA	Inappropriate User Activity
		LP	Least Privilege
FR02	[Role] executes existing code that should never be executed	ES	Endpoint Security
		PW	Process Whitelisting
FR03	Authorized user loads/accepts unauthorized code on [Role]	SFA	Software and Firmware Authenticity
FR04	Improperly identified user (incorrect or elevated privileges) loads unauthorized code on [Role]	CMA	Cryptographic Module Authentication
		NSA	No Shared Accounts
FR05	[Role] executes unauthorized mobile/active code	MoC	Mobile Code
FR06	[Role] executes unauthorized code from mobile device	PDA	Portable Device Attachment
FR07	[Role] executes unreliable (authorized, but not tested) code	TU	Testing Updates
FR08	[Role] is poorly implemented, allowing instruction pointer compromise (e.g., buffer overflow)	SCP	Secure Coding Practices
FR09	[Role] is poorly implemented and starts/restarts in an unknown state	SKS	Startup in Known State
FR10	[Role] does not adequately manage memory (i.e., capacity and integrity) (e.g., memory leaks, bad initialization)	SCP	Secure Coding Practices

Failure Mode ID	Failure Mode	Control ID	Control Name
FR11	[Role] receives message from unknown sender (includes unauthenticated sender)	CMA	Cryptographic Module Authentication
		Mid	Message Identities
		NSA	No Shared Accounts
FR12	[Role] receives message from unexpected sender	IW	Interaction Whitelisting
FR13	[Role] incorrectly acts on, interprets, or discards data not synchronized with [Role]'s clock	CRDI	Clock Record and Discrepancy Identification
		MT	Message Timestamping
FR14	[Role] processes user input without sufficient validation (e.g., syntactic, semantic; timing...)	MIC	Manual Input Checking
FR15	[Role] processes message input without sufficient validation (e.g., syntactic, semantic; timing...)	MV	Message Validation
FR16	[Role] uses incorrect or corrupt corroboration data for validation of message sender	CFSD	Configuration File and Sensitive Data Integrity Check
		CrM	Credential Management
FR17	[Role] does not have access to sufficient storage to perform its functions	CSW	Configured Size Warnings
		RD	Replacement of Data
		SM	Store Monitoring
FR18	[Role] Improperly manipulates data	AE	Access Enforcement
		CFSD	Configuration File and Sensitive Data Integrity Check
		CuC	Current Configuration
		IUA	Inappropriate User Activity
		LP	Least Privilege
FR19	Authenticated user performs unauthorized action on [Role]	EI	Endpoint Isolation
		IUA	Inappropriate User Activity
		LP	Least Privilege
FR20	Unauthorized user successfully guesses credentials to account	PaM	Password Management
		TFA	Two-Factor Authentication
FR21	Role does not sufficiently distinguish between users	AAM	Automated Account Management
		CMA	Cryptographic Module Authentication

Failure Mode ID	Failure Mode	Control ID	Control Name
		FDC	Factory Default Credentials
		NSA	No Shared Accounts
FR22	[Role] enables improper use of authorized session / enables session hijacking	RIS	Remote Interactive Sessions
		SD	Session Duration
FR23	[Role]'s login interface enables unauthorized account access	AF	Authenticator Feedback
		ULA	Unsuccessful Login Attempts
FR24	[Role] experiences unexpected process restart or shutdown	BPR	Backup Power Requirement
		DUF	Disabling Unnecessary Functions
		HM	Health Monitoring
		MV	Message Validation
FR25	[Role] uses incorrect / improper data for evaluation during processing	AVC	Alternate Value Comparison
		CFSD	Configuration File and Sensitive Data Integrity Check
		CuC	Current Configuration
		SId	Self-Identification
		MV	Message Validation
FR26	[Role's host] supplies data to application that is false	PW	Process Whitelisting
		SFA	Software and Firmware Authenticity
FR27	[Role] improperly manages its data store (e.g., unneccessarily overwriting data)	RD	Replacement of Data
		SIC	Storage Integrity Check
FR28	[Role] does not have access to sufficient processing resources to perform its functions on time	CSM	Concurrent Session Management
		DUF	Disabling Unnecessary Functions
		P	Prioritization
		PC	Processor Consumption
		PrM	Processor Monitoring
FR29	[Role] does not have access to sufficient memory to perform its functions	MeC	Memory Consumption
		MM	Memory Monitoring
FR30	[Role's host] does not adequately manage memory	Mis	Memory Isolation

Failure Mode ID	Failure Mode	Control ID	Control Name
	integrity		
FR31	[Role] does not have access to sufficient communications resources (e.g., NIC) to perform its functions on time	CCp	Communications Consumption
		CoM	Communications Monitoring
FR32	[Role] sends spurious message	ID	Intrusion Detection
		IW	Interaction Whitelisting
FR33	Authorized user misconfigures [Role] settings	CFA	Configuration File Authenticity
		CFSD	Configuration File and Sensitive Data Integrity Check
		TU	Testing Updates

4.3.2 Communication-Based Failures and Controls

Table 13 shows the set of security controls that are recommended to address each communication-based failure mode identified in Section 3.3.2. The first three columns correspond to the ID, textual description, and examples of each communication-based failure mode from Table 7. The last two columns correspond to the ID and name of security controls from Table 11. Each failure mode is mapped to one or more security controls; the combination of controls is recommended to mitigate the failure mode (i.e., it does not identify a set of options).

Table 13 – Communication-Based Failure Modes and Controls

Failure Mode ID	Failure Mode	Example	Control ID	Control Name
FC1	Message to or from [Role] is blocked, dropped, or delayed because the network is saturated	DDoS, Spurious message generation, Authorized network device consuming network resources	QSE	Quality of Service Enforcement
			QSS	Quality of Service Specification
			TCF	Traffic Control and Filtering
			ENS	Emergency Network Segmentation
			EI	Endpoint Isolation
		Network underprovisioned; network over-allocated (e.g., addition of devices/functionality over time)	NM	Network Monitoring

Failure Mode ID	Failure Mode	Example	Control ID	Control Name
FC2	Message to or from [Role] is blocked, dropped, or delayed because of interference on the network medium	Insufficient signal-to-noise ratio, electromagnetic interference	ESP	EMI/Surge Protection
FC3	Message to or from [Role] is blocked, dropped, or delayed because a device or service in the network infrastructure is not available or functional	Incorrect firmware update, DNS not available	CSM	Concurrent Session Management
			RIS	Remote Interactive Sessions
			SD	Session Duration
			ULA	Unsuccessful Login Attempts
			NOC	Network Operations Continuity
			BPR	Backup Power Requirement
FC4	Message to or from [Role] is inappropriately blocked by a network device	Incorrect configuration. Traffic is getting to a router or switch, but protocol parameters are incorrect (e.g., frame size, baud rate, data rate).	SIn	Systems Inventory
			CuC	Current Configuration
			AAM	Automated Account Management
			AE	Access Enforcement
			LP	Least Privilege
			CrM	Credential Management
FC5	Unauthorized device views messages through unauthorized access to transmission medium (logical or physical access)	Wiretap, wireless snooping, incorrect network configuration, unauthorized use of communication port	CCf	Communication Confidentiality
			RIS	Remote Interactive Sessions
			SD	Session Duration
			ULA	Unsuccessful Login Attempts
			NAE	Network Access Enforcement
			LFCA	Limited Field Component Access
			CrM	Credential Management
FC6	Message delivered to unintended (additional) recipients due to misuse of broadcast or multicast protocol	Incorrect network configuration	TCF	Traffic Control and Filtering
			CuC	Current Configuration
FC7	Inappropriate connection between networks allows information to leak between domains	Unauthorized bridge between networks established in end device, cable inadvertently installed between switches in separate networks.	TCF	Traffic Control and Filtering

Failure Mode ID	Failure Mode	Example	Control ID	Control Name
FC8	Message is delayed or exposed to unintended recipients because network infrastructure routes traffic over inappropriate path	Network device advertising incorrect network, duplicate IP address, network device sends message to wrong interface, incorrect metrics in router configuration	TCF	Traffic Control and Filtering
			CuC	Current Configuration
			SNAR	Secure Name / Address Resolution
FC9	Network accepts a message from an unauthorized source	Rogue device attaches to network	NAE	Network Access Enforcement
			EI	Endpoint Isolation
			ID	Intrusion Detection
			IW	Interaction Whitelisting
			CrM	Credential Management
FC10	Network accepts an unauthorized message type	Device sends message using unauthorized protocol	TCF	Traffic Control and Filtering
			IW	Interaction Whitelisting
FC11	Message attributes (header or payload) are corrupt or manipulated	Unauthorized/erroneous modification of message header	CI	Communication Integrity
			CKIM	Cryptographic Key Implementation and Management
			ID	Intrusion Detection
FC12	Network device is subverted to mis-handle (e.g., block, delay, mis-route, inject, or manipulate) communications.		LP	Least Privilege
			AE	Access Enforcement
			IUA	Inappropriate User Activity
			RIS	Remote Interactive Sessions
			SD	Session Duration
			ULA	Unsuccessful Login Attempts
			CrM	Credential Management
			EI	Endpoint Isolation
			SFA	Software and Firmware Authenticity
			NSA	No Shared Accounts
			CMA	Cryptographic Module Authentication
			MoC	Mobile Code
			PDA	Portable Device Attachment
			SCP	Secure Coding Practices
			PaM	Password Management

Failure Mode ID	Failure Mode	Example	Control ID	Control Name
			TFA	Two-Factor Authentication
			FDC	Factory Default Credentials
			AAM	Automated Account Management

4.3.3 Zone-Based Failures and Controls

Table 14 shows the set of security controls that are recommended to address each zone-based failure mode identified in Section **Error! Reference source not found.**. The first three columns correspond to the ID, textual description, and examples of each zone-based failure mode from Table 8. The last two columns correspond to the ID and name of security controls from Table 11. Each failure mode is mapped to one or more security controls; the combination of controls is recommended to mitigate the failure mode (i.e., it does not identify a set of options).

Table 14 – Zone-Based Failure Modes and Controls

Failure Mode ID	Failure Mode	Example	Control ID	Control Name
FZ1	Messages required for system protection do not arrive in a timely manner	Overloaded network or device (throughput)	IPC	Isolation of Protection Communications
			VE	VLAN Enforcement
FZ2	Coordination among replicated, redundant, and/or independent roles within protection zone (i.e., coordinated protection scheme) produces incorrect result.	Compromise of 1 out of 1+ redundant devices;	PFP	Protection Function Preservation
FZ3	Protection function misoperates due to incorrect data.	Interception/injection of specific protection messages (due to rogue device on protection network);	GSRP	GOOSE and SMV Replay Protection[11]
FZ4	Protection function not available or deficient due to device failure or compromise.	Protective relay compromised, removing it from service – no redundant device; multiple devices of same type disabled by class break; failover switch compromised, preventing backup device from providing coverage;	PFP	Protection Function Preservation

[11] Special control required because the standard means of preventing interception/injection would violate Protection Zone Operational Principle #2.

Failure Mode ID	Failure Mode	Example	Control ID	Control Name
FZ5	Loss of communication with roles outside the zone or subzone prevents Role from performing core functionality	Core functionality fails due to data disruption or delay caused by comm failures to/from outside the zone or subzone; A process gets hung waiting for a response from outside the zone or subzone. (Does not have appropriate timeout.)	GD	Graceful Degradation

4.3.4 Security-Control-Based Failures and Controls

Table 15 shows the set of security controls that are recommended to address each security-control-based failure mode identified in Section 3.3.4. The first three columns correspond to the ID, textual description, and examples of each security-control-based failure mode from Table 9. The last two columns correspond to the ID and name of security controls from Table 10. Each failure mode is mapped to one or more security controls; the combination of controls is recommended to mitigate the failure mode (i.e., it does not identify a set of options).

Table 15 - Security-Control-Based Failure Modes and Controls

Failure Mode ID	Failure Mode	Example	Control ID	Control Name
FS1	Integrity of security information is compromised.	Password files are tampered with. Log files are corrupted.	PSI	Protection of Security Information
			SR	System Restoration
FS2	Security information is not available.	Forensic information is deleted by an unauthorized user or never collected.	AAM	Automated Account Management
			CAR	Content of Audit Records
			PSI	Protection of Security Information
			SR	System Restoration
FS3	Confidentiality of security information is violated.	Passwords are stored, or transmitted, in clear text.	AF	Authenticator Feedback
			PaM	Password Management
			PSI	Protection of Security Information

Appendix A: NIST IR 7628 Requirements Mapped To ASAP-SG SA SP Controls

A goal of this profile is to support and align with the NIST IR 7628. Therefore Table 16 below provides a list of requirements from the NIST IR 7628 that are covered by controls in this profile.

Table 16 – NIST IR 7628 Requirements Mapped to SA SP Controls

NIST IR 7628 Requirement ID	NIST IR 7628 Requirement Name	ASAP-SG SA SP Control ID	ASAP-SG SA SP Control Name
SG.AC-1	Access Control Policy and Procedures	LP	Least Privilege
		RIS	Remote Interactive Sessions
SG.AC-3	Account Management	AAM	Automated Account Management
		LP	Least Privilege
		NSA	No Shared Accounts
		ULA	Unsuccessful Login Attempts
SG.AC-4	Access Enforcement	AE	Access Enforcement
SG.AC-5	Information Flow Enforcement	ENS	Emergency Network Segmentation

NIST IR 7628 Requirement ID	NIST IR 7628 Requirement Name	ASAP-SG SA SP Control ID	ASAP-SG SA SP Control Name
		IPC	Isolation of Protection Communications
		IW	Interaction Whitelisting
		TCF	Traffic Control and Filtering
		VE	VLAN Enforcement
SG.AC-6	Separation of Duties	LP	Least Privilege
SG.AC-7	Least Privilege	LP	Least Privilege
SG.AC-8	Unsuccessful Login Attempts	ULA	Unsuccessful Login Attempts
SG.AC-9	Smart Grid Information System Use Notification	ULA	Unsuccessful Login Attempts
SG.AC-10	Previous Logon Notification	CSM	Concurrent Session Management
SG.AC-11	Concurrent Session Control	CSM	Concurrent Session Management
SG.AC-12	Session Lock	SD	Session Duration
SG.AC-13	Remote Session Termination	SD	Session Duration
SG.AC-15	Remote Access	AE	Access Enforcement
		CoM	Communications Monitoring
		CrM	Credential Management
		RIS	Remote Interactive Sessions
SG.AC-16	Wireless Access Restrictions	DUF	Disabling Uneccessary Functions
		NAE	Network Access Enforcement
SG.AC-17	Access Control for Portable and Mobile Devices	NAE	Network Access Enforcement
		PDA	Portable Device Attachment
SG.AC-19	Control System Access Restrictions	IW	Interaction Whitelisting
		LP	Least Privilege
		NAE	Network Access Enforcement
		TCF	Traffic Control and Filtering
SG.AC-21	Passwords	PaM	[P] Password Management
		TFA	Two-Factor Authentication

NIST IR 7628 Requirement ID	NIST IR 7628 Requirement Name	ASAP-SG SA SP Control ID	ASAP-SG SA SP Control Name
SG.AU-3	Content of Audit Records	SM	Storage Monitoring
		CAR	Content of Audit Records
SG.AU-4	Audit Storage Capacity	SC	Storage Consumption
SG.AU-8	Time Stamps	CRDI	Clock Record and Discrepancy Identification
SG.AU-9	Protection of Audit Information	PSI	Protection of Security Information
SG.AU-15	Audit Generation	CAR	Content of Audit Records
SG.AU-16	Non-Repudiation	CAR	Content of Audit Records
		PSI	Protection of Security Information
SG.CA-4	Smart Grid Information System Connections	TCF	Traffic Control and Filtering
SG.CM-2	Baseline Configuration	CFA	Configuration File Authenticity
		CFSD	Configuration File and Sensitive Data Integrity Check
		CuC	Current Configuration
SG.CM-3	Configuration Change Control	CFA	Configuration File Authenticity
		CFSD	Configuration File and Sensitive Data Integrity Check
		CuC	Current Configuration
SG.CM-5	Access Restrictions for Configuration Change	LP	Least Privilege
SG.CM-6	Configuration Settings	CuC	Current Configuration
SG.CM-7	Configuration for Least Functionality	DUF	Disabling Uneccessary Functions
SG.CM-8	Component Inventory	CuC	Current Configuration
		SIn	Systems Inventory
SG.CM-10	Factory Default Settings Management	FDC	Factory Default Credentials
SG.CP-8	Alternate Telecommunications Services	NOC	Network Operations Continuity
SG.CP-10	Smart Grid Information System Recovery and Reconstitution	SR	System Restoration

NIST IR 7628 Requirement ID	NIST IR 7628 Requirement Name	ASAP-SG SA SP Control ID	ASAP-SG SA SP Control Name
SG.CP-11	Fail-Safe Response	GD	Graceful Degradation
SG.IA-4	User Identification and Authentication	CMA	Cryptographic Module Authentication
		NSA	No Shared Accounts
SG.IA-5	Device Identification and Authentication	CMA	Cryptographic Module Authentication
		NSA	No Shared Accounts
SG.IA-6	Authenticator Feedback	AF	Authenticator Feedback
SG.MP-3	Media Marking	PDA	Portable Device Attachment
SG.PE-3	Physical Access	CrM	Credential Management
		LFCA	Limited Field Component Access
SG.PE-9	Emergency Power	BPR	Backup Power Requirement
SG.SA-7	User Installed Software	DUF	Disabling Uneccessary Functions
SG.SA-8	Security Engineering Principles	SCP	Secure Coding Practices
SG.SA-10	Developer Security Testing	TU	Testing Updates
SG.SC-2	Communications Partitioning	VE	VLAN Enforcement
SG.SC-3	Security Function Isolation	CMA	Cryptographic Module Authentication
SG.SC-4	Information Remnants	PDA	Portable Device Attachment
		SCP	Secure Coding Practices
SG.SC-5	Denial-of-Service Protection	EI	Endpoint Isolation
		ENS	Emergency Network Segmentation
		IW	Interaction Whitelisting
		NAE	Network Access Enforcement
		SNAR	Secure Name / Address Resolution
		TCF	Traffic Control and Filtering
SG.SC-6	Resource Priority	CCp	Communications Consumption
		MeC	Memory Consumption
		P	Prioritization

NIST IR 7628 Requirement ID	NIST IR 7628 Requirement Name	ASAP-SG SA SP Control ID	ASAP-SG SA SP Control Name
		PC	Processor Consumption
		QSE	Quaility of Service Enforcement
		QSS	Quality of Service Specification
		SC	Storage Consumption
SG.SC-7	Boundary Protection	TCF	Traffic Control and Filtering
SG.SC-8	Communication Integrity	CI	Communication Integrity
SG.SC-9	Communication Confidentiality	CCf	Communication Confidentiality
		RIS	Remote Interactive Sessions
SG.SC-11	Cryptographic Key Establishment and Management	CKIM	Cryptographic Key Implementation and Management
SG.SC-12	Use of Validated Cryptography	CMA	Cryptographic Module Authentication
SG.SC-13	Collaborative Computing	DUF	Disabling Uneccessary Functions
SG.SC-15	Public Key Infrastructure Certificates	CKIM	Cryptographic Key Implementation and Management
SG.SC-16	Mobile Code	MoC	Mobile Code
SG.SC-17	Voice-Over Internet Protocol	DUF	Disabling Uneccessary Functions
SG.SC-18	System Connections	NAE	Network Access Enforcement
		TCF	Traffic Control and Filtering
SG.SC-19	Security Roles	LP	Least Privilege
SG.SC-20	Message Authenticity	CI	Communication Integrity
		CMA	Cryptographic Module Authentication
		MId	Message Identities
SG.SC-21	Secure Name/Address Resolution Service	SNAR	Secure Name / Address Resolution
SG.SC-22	Fail in Known State	GD	Graceful Degradation
		PFP	Protection Function Preservation
SG.SC-23	Thin Nodes	DUF	Disabling Uneccessary

NIST IR 7628 Requirement ID	NIST IR 7628 Requirement Name	ASAP-SG SA SP Control ID	ASAP-SG SA SP Control Name
			Functions
SG.SC-26	Confidentiality of Information at Rest	PSI	Protection of Security Information
SG.SC-29	Application Partitioning	MIs	Memory Isolation
SG.SC-30	Smart Grid Information System Partitioning	ENS	Emergency Network Segmentation
		GD	Graceful Degradation
		IPC	Isolation of Protection Communications
		TCF	Traffic Control and Filtering
		VE	VLAN Enforcement
		EI	Endpoint Isolation
SG.SI-3	Malicious Code and Spam Protection	ES	Endpoint Security
		IW	Interaction Whitelisting
		SCP	Secure Coding Practices
		TCF	Traffic Control and Filtering
SG.SI-4	Smart Grid Information System Monitoring Tools and Techniques	CoM	Communications Monitoring
		ES	Endpoint Security
		HM	Health Monitoring
		ID	Intrusion Detection
		IUA	Inappropriate User Activity
		MM	Memory Monitoring
		PrM	Processor Monitoring
		SM	Storage Monitoring
SG.SI-7	Software and Information Integrity	CFA	Configuration File Authenticity
		CFSD	Configuration File and Sensitive Data Integrity Check
		CuC	Current Configuration
		SFA	Software and Firmware Authenticity
		SIC	Storage Integrity Check
SG.SI-8	Information Input Validation	MIC	Manual Input Checking
		MV	Message Validation

Table 17 provides list of NIST IR 7628 requirements for which the controls in this profile provide only partial or no coverage, along with the level of coverage and reasons for the gaps.

Table 17 - NIST IR 7628 Requirement Gaps

NISTIR Category	NIST IR 7628 Requirement ID	NIST IR 7628 Requirement Name	Notes
SG.AC	SG.AC-2	Remote Access Policy and Procedures	Policy
SG.AC	SG.AC-14	Permitted Actions without Identification or Authentication	Not needed in SA
SG.AC	SG.AC-18	Use of External Information Control Systems	Organizational
SG.AC	SG.AC-20	Publicly Accessible Content	
SG.AT	All	Awareness and Training	Organizational
SG.AU	SG.AU-1	Audit and Accountability Policy and Procedures	Policy
	SG.AU-2	Auditable Events	Organizational
	SG.AU-4	Audit Storage Capacity	Organizational
	SG.AU-5	Response to Audit Processing Failures	Audit processing not in-scope
	SG.AU-6	Audit Monitoring, Analysis, and Reporting	Organizational
	SG.AU-7	Audit Reduction and Report Generation	Business need, no specific SA implications
	SG.AU-10	Audit Record Retention	Organizational
	SG.AU-11	Conduct and Frequency of Audits	Organizational
	SG.AU-12	Auditor Qualification	Organizational
	SG.AU-13	Audit Tools	Organizational
	SG.AU-14	Security Policy Compliance	Organizational
SG.CA	SG.CA-1	Security Assessment and Authorization Policy and Procedures	Organizational
	SG.CA-2	Security Assessments	Organizational
	SG.CA-3	Continuous Improvement	Organizational
	SG.CA-5	Security Authorization to Operate	Organizational
	SG.CA-6	Continuous Monitoring	Organizational
SG.CM	SG.CM-1	Configuration Management Policy and Procedures	Organizational
	SG.CM-4	Monitoring Configuration Changes	Organizational (NOTE: CFSD facilitates coverage)
	SG.CM-9	Addition, Removal, and Disposal of Equipment	Organizational

NISTIR Category	NIST IR 7628 Requirement ID	NIST IR 7628 Requirement Name	Notes
	SG.CM-11	Configuration Management Plan	Organizational
SG.CP	SG.CP-1	Continuity of Operations Policy and Procedures	Organizational
	SG.CP-2	Continuity of Operations Plan	Organizational
	SG.CP-3	Continuity of Operations Roles and Responsibilities	Organizational
	SG.CP-4	Continuity of Operations Training	Organizational
	SG.CP-5	Continuity of Operations Plan Testing	Organizational
	SG.CP-6	Continuity of Operations Plan Update	Organizational
	SG.CP-7	Alternate Storage Sites	Organizational
	SG.CP-9	Alternate Control Center	Organizational
SG.IA	SG.IA-1	Identification and Authentication Policy and Procedures	Organizational
	SG.IA-2	Identifier Management	Organizational
	SG.IA-3	Authenticator Management	Organizational
SG.ID	SG.ID-1	Information and Document Management Policy and Procedures	Organizational
	SG.ID-2	Information and Document Retention	Organizational
	SG.ID-3	Information Handling	Organizational
	SG.ID-4	Information Exchange	Organizational
	SG.ID-5	Automated Labeling	Low value for SA, Not selected in NISTIR
SG.IR-1	SG.IR-1	Incident Response Policy and Procedures	Organizational
	SG.IR-2	Incident Response Roles and Responsibilities	Organizational
	SG.IR-3	Incident Response Training	Organizational
	SG.IR-4	Incident Response Testing and Exercises	Organizational
	SG.IR-5	Incident Handling	Organizational
	SG.IR-6	Incident Monitoring	Organizational
	SG.IR-7	Incident Reporting	Organizational
	SG.IR-8	Incident Response Investigation and Analysis	Organizational
	SG.IR-9	Corrective Action	Organizational

NISTIR Category	NIST IR 7628 Requirement ID	NIST IR 7628 Requirement Name	Notes
	SG.IR-10	Smart Grid Information System Backup	Organizational (NOTE: CKIM, SR, and PSI facilitate technical capabilities here)
	SG.IR-11	Coordination of Emergency Response	Organizational
SG.MA	SG.MA-1	Smart Grid Information System Maintenance Policy and Procedures	Organizational
	SG.MA-2	Legacy Smart Grid Information System Upgrades	Organizational
	SG.MA-3	Smart Grid Information System Maintenance	Organizational
	SG.MA-4	Maintenance Tools	Organizational
	SG.MA-5	Maintenance Personnel	Organizational
	SG.MA-6	Remote Maintenance	Organizational (NOTE: Not recommended and not in scope for SA)
	SG.MA-7	Timely Maintenance	Organizational
SG.MP	SG.MP-1	Media Protection Polcy and Procedures	Organizational
	SG.MP-2	Media Sensitivity Level	N/A
	SG.MP-3	Media Marking	N/A
	SG.MP-4	Media Storage	N/A
	SG.MP-5	Media Transport	N/A
	SG.MP-6	Media Sanitization and Disposal	Organizational
SG.PE	SG.PE-1	Physical and Environmental Security Policy and Procedures	Organizational
	SG.PE-2	Physical Access Authorizations	Organizational
	SG.PE-4	Monitoring Physical Access	Organizational
	SG.PE-5	Visitor Control	Organizational
	SG.PE-6	Visitor Records	Organizational
	SG.PE-7	Physical Access Log Retention	Organizational
	SG.PE-8	Emergency Shutoff Protection	Organizational
	SG.PE-10	Delivery and Removal	Organizational
	SG.PE-11	Alternate Work Site	Organizational
	SG.PE-12	Location of Smart Grid Information System Assets	Organizational + N/A
SG.PL	All	Planning	Organizational
SG.PM	All	Security Program Management	Organizational

NISTIR Category	NIST IR 7628 Requirement ID	NIST IR 7628 Requirement Name	Notes
SG.PS	All	Personnel Security	Organizational
SG.RA	All	Risk Management and Assessment	Organizational
SG.SA	SG.SA-1	Smart Grid Information System and Services Acquisition Policy and Procedures	Organizational
	SG.SA-2	Security Policies for Contractors and Third Parties	Organizational
	SG.SA-3	Life-Cycle Support	Organizational
	SG.SA-4	Acquisitions	Organizational
	SG.SA-5	Smart Grid Information System Documentation	Organizational
	SG.SA-6	Software License Usage Restrictions	Organizational
	SG.SA-9	Developer Configuration Management	Organizational
	SG.SA-11	Supply Chain Protection	Organizational
SG.SC	SG.SC-1	Smart Grid Information System and Communication Protection Policy and Procedures	Organizational
	SG.SC-3	Security Function Isolation	Unclear how to implement for SA
	SG.SC-10	Trusted Path	N/A
	SG.SC-14	Transmission of Security Parameters	N/A
	SG.SC-24	Honeypots	Inappropriate for SA
	SG.SC-25	Operating System-Independent Applications	N/A
	SG.SC-27	Heterogeneity	Inappropriate for SA
	SG.SC-28	Virtualization Techniques	Inappropriate for SA
SG.SI	SG.SI-1	Smart Grid Information System and Information Integrity Policy and Procedures	Organizational
	SG.SI-2	Flaw Remediation	Organizational
	SG.SI-5	Security Alerts and Advisories	Organizational
	SG.SI-6	Security Function Verification	Unclear how this would be handled for SA. Supporting controls include AAM, CAR, CFSD, ID, HM, and IUA.
	SG.SI-9	Error Handling	Not specific to SA

Table 18 identifies controls in this profile that do not map to a requirement in the NIST IR 7628:

Table 18 - SA Controls Not Covered by NIST IR 7628

ASAP-SG Control ID	ASAP-SG Control Name
AVC	Alternate Value Comparison
CSW	Configured Size Warnings
ESP	EMI/Surge Protection
GSRP	GOOSE and SMV Replay Protection
MT	Message Timestamping
NMP	Network Monitoring and Provisioning
PW	Process Whitelisting
RD	Replacement of Data
SId	Self-Identification
SKS	Startup in Known State
TQF	Timestamps and Quality Flags