SECURITY PROFILE FOR WIDE-AREA MONITORING, PROTECTION, AND CONTROL

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
0.08

Revision History

Rev	Date	Summary	Marked
0.01	20110510	Outline established. Section 1 content complete.	N
0.02	20110510	Section 2 content complete.	N
0.03	20110511	Section 3 through failure definitions content complete.	N
0.04	20110512	Section 4 draft content and template tables	N
0.05	20110513	Content complete excepting Glossary, Acronyms, & References	N
0.06	20110515	Content complete + 1st team editing pass.	N
0.07	20110516	First public draft.	N
0.08	20110516	Table of Contents update.	N
	20110921	Incorporated comments	

Executive Summary

This document presents the security profile for wide-area monitoring, protection, and control (WAMPAC) of the electric grid, specifically leveraging synchrophasor technology. This profile addresses security concerns associated with the use of phasor measurements in electric system operational decisions, whether these decisions are made off-line, real-time but manually, or through automated processes. The recommendations made herein are based on stated system architectural and functional assumptions, and offer a singular security baseline for overall use of synchrophasor technology with tailored subsets of recommendations where variations in system deployment or usage occur.

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

The primary audience for this document is organizations that are developing or implementing solutions requiring or providing WAMPAC functionality through the use of synchrophasor technology. 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.

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 Pacific Gas & Electric and Southern California Edison.
2. Supporting organizations, including: The United States Department of Energy, the Electric Power Research Institute, and InGuardians.
3. The utility and vendor representatives that provided ASAP-SG with essential foundational knowledge and insight into the Wide Area Monitoring, Protection, and Control problem space, with a special thanks to the Grid Protection Alliance, Florida Power & Light, University of Illinois at Urbana/Champagne, Oncor, PJM, Pacific Northwest National Laboratory, SISCO, Southern California Edison, and WECC.

ASAP-SG would also like to thank the National Institute of Standards and Technology (NIST) Computer Security Division, the North American Reliability Corporation (NERC), and the North American Synchrophasor Initiative (NASPI) Data & Network Management Task Team (DNMTT) for the works that they have produced that served as reference material for the Security Profile for Wide Area Monitoring, Protection, and Control.

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

Authors

Glenn Allgood

Len Bass

Bobby Brown

Kevin Brown

Slade Griffin

James Ivers

Teja Kuruganti

Joe Lake

Howard Lipson

Jim Nutaro

Justin Searle

Brian Smith

Edited by: Darren Highfill

1 Introduction

This document presents the security profile for wide-area monitoring, protection, and control (WAMPAC) of the electric grid, specifically leveraging synchrophasor technology. System functions considered include the generation, transportation, aggregation, alignment, and processing of time-stamped electric system phase angle and magnitude ("phasor") measurements. This profile addresses security concerns associated with the use of phasor measurements in electric system operational decisions, whether these decisions are made off-line, real-time but manually, or through automated processes. The recommendations made herein are based on stated system architectural and functional assumptions, and offer a singular security baseline for overall use of synchrophasor technology with tailored subsets of recommendations where variations in system deployment or usage occur.

This document defines a reference architecture, a set of use cases to define system functionality, and a set of security controls for systems and components that implement the use cases. The security controls in this document are inspired by and intended to cover the application of technical requirements found in *NIST Interagency Report (IR) 7628: Guidelines for Smart Grid Cyber Security*[1] to synchrophasor systems and 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 synchrophasor technology and defining intrasystem-level security controls. The controls presented herein may then, in turn, be satisfied by communications protocol definition-level standards and manufacturing specifications. The underlying approach for developing this document was (1) to study real-world use of synchrophasor systems, (2) define the function of

[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.

these systems by presenting a reference architecture that defines abstract roles and use cases, (3) map the architecture's roles to real-world synchrophasor systems, (4) define broad security objectives for synchrophasor systems, (5) identify potential failures for each role in the context of the use cases, (6) define security controls to address the failures, and (7) assign controls to the roles.

An understanding of the concept of roles is essential to applying the security controls defined in this document. Roles have been designed abstractly to ensure applicability across a range of synchrophasor applications and products. The key roles for this document are those of a Phasor Measurement Unit (PMU), phasor Alignment, and an Application—each of which represents functionality that may be implemented by physical devices. A PMU makes time-stamped measurements of phase angle and magnitude (phasor) of voltage at a fixed point on the electric grid. Alignment continuously gathers phasor measurements from numerous PMUs, correlates measurements against fixed points in time, and provides a stream of aggregated sets of phasor measurements to an Application. Different types or classes of Applications are variously able to analyze data in an off-line or on-line fashion, integrate phasor data with other types of system data for a more complete picture of system state, and make and execute automated decisions regarding system protection and control. Not all Application functionality will be present in all systems, and this document takes this variation into account by assigning controls conditionally according to functionality where appropriate. To distinguish between different types of application functionality, this document leverages the classes of data as defined by the North American SynchroPhasor Initiative (NASPI) Data and Network Management Task Team (D&NMTT).[2] The roles mentioned above, and other supporting roles, are elaborated in Section 2.

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 functions involved in the use of synchrophasor data and applications for wide-area monitoring, protection, and control (WAMPAC). Specifically, this security profile addresses the transfer and delivery of time-synchronized, moderate resolution (i.e., 10-240 samples per ***second***), power-related waveform data across geographically diverse Transmission Operator and Reliability Coordinator locations. This security profile does not address the use of high resolution (i.e., 50-240 samples per ***cycle***[3])

[2] Quanta Technology LLC, *Phasor Gateway Technical Specification for North American Synchro-Phasor Initiative Network (NASPInet)*, May 29, 2009, page 1-4 (PDF page 11). Available at: http://www.naspi.org/naspinet.stm. Quanta Technology LLC, *Data Bus Technical Specification for North American Synchro-Phasor Initiative Network (NASPInet)*, May 29, 2009, page 1-4 (PDF page 11). Available at: http://www.naspi.org/naspinet.stm.

[3] Assuming 50-60 cycles per second, this equates to 2500-14400 samples per second.

waveform process bus data such as Sampled Values[4] inside a substation for purposes of high-speed automated protection functions, nor does it address processing requirements for synchrophasor data within a device or application beyond necessary security functions. This document also recognizes that some organizations will only implement a subset of the functions defined herein, and is therefore designed to accommodate different configurations and choices.

1.1.1 Equipment

From an equipment perspective, the scope of this security profile is bounded to devices that handle synchrophasor data as defined above or that directly support the functionality of synchrophasor applications.

Field Equipment

Equipment that produces phasor measurements used in wide-area applications is in scope. This will typically be a phasor measurement unit (PMU), however this functionality may also be implemented in a device performing other functions such as a relay, digital fault recorder, or meter. Other field devices implementing functions involved in synchrophasor measurement and applications such as time alignment, aggregation, caching, and/or storage are also in scope.

Perimeter Equipment

Equipment implementing functions that bridge organizational boundaries to facilitate synchrophasor applications is in scope. This includes phasor gateways as well as proxy servers used to bring in environmental data for correlation and/or overlay. External sources of environmental data are not explicitly in scope; however recommended controls for proxy servers may limit choices for acceptable external data sources.

Operations Center Equipment

Equipment in the operations center or control center that internalizes and processes phasor data in the course of performing synchrophasor application functionality is in scope. This includes Phasor Data Concentrators, Data Stores, and other central Applications as defined below.

Network Equipment

Equipment implementing any intermediary function specifically aimed at facilitating or brokering exchange of synchrophasor data between organizations is in scope. This includes devices that integrate configuration information, provide for long-term storage of time-series data (or other inter-organizational storage of phasor data), or any intermediary function required to establish communications between the phasor gateways of two or more organizations. Network equipment that supports the collection and handling of synchrophasor data within an organization or the functionality of the organization's synchrophasor applications is also in scope.

[4] IEC 61850

1.1.2 Processing

While determination of adequate business processing for synchrophasor data 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

Synchrophasor data may be used by Transmission Owners and Reliability Coordinators[5] to augment or in some cases solely supply applications that enable near and long-term decision-making, as well as advanced protection and control functions for certain organizations and scenarios. This security profile considers any application that takes synchrophasor data as direct input to be in scope. This includes both real-time (e.g., automated wide-area protection) and near-real-time (e.g., visualization and monitoring) applications, as well as tools for static and post-event analysis and forensics as performed by Transmission Owners and Reliability Coordinators. Analysis and research performed on static data by outside parties (e.g., academic institutions) is out of scope for this security profile. Regardless, transportation of data for this purpose must be secured in accordance with its sensitivity, and this document recommends against the indefinite exposure of any electronic interface for this purpose. Any electronic interface used to transport synchrophasor data for static analysis should be made available on a temporal basis, and only to explicitly defined recipients with assigned credentials. Specific functions that are considered in this security profile include:

Table 1 – NASPI Data Classes in Scope for this Security Profile

Function	NASPI Data Class	Purpose	Examples
Reliability Operations			
Wide-area adaptive protection	A	Grid stability response Planned power system separation	Centralized remedial action schemes Islanding and restoration Load response
Wide-area grid monitoring and visualization	B or C	Interconnection metrics Grid problem identification Oscillation detection System capacity	Monitoring and alarming Situational awareness tools State estimation Engineering analysis Dynamic line ratings
System Planning			
Benchmarking and validation	D	Understanding of system operations Identification of modeling errors	Power flow analysis Load flow analysis

[5] As defined by NERC in the Glossary of Terms Used in Reliability Standards. http://www.nerc.com/files/Glossary_12Feb08.pdf

		Power system model fine-tuning System behavior prediction	Modal frequency response Security assessment Short circuit analysis Dynamic model calibration
Forensics			
Post-event analysis	D	Root-cause determination Sequence of events	Transient analysis Validation of controller settings Procedure validation Line and equipment rating validation

Note: NASPI Data Service Class E is not considered in the scope of this document. Only PMUs owned and operated by utilities are considered.

1.1.4 Explicit Exclusions

As mentioned above, this security profile does not address the use of high resolution (i.e.: 50-240 samples per cycle) waveform process bus data such as Sampled Values inside the substation for purposes of high-speed automated protection functions, nor does it address the processing of synchrophasor data within a device or application beyond necessary security functions. While synchrophasor data may augment or enhance system monitoring for some organizations, this document explicitly considers the functions of system operation (i.e., manual oversight and control of system settings and behavior) and determination of necessary system protection (i.e., automated high-speed response to a fault condition) to be out of scope for this profile.

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 may in fact be iterative in nature.

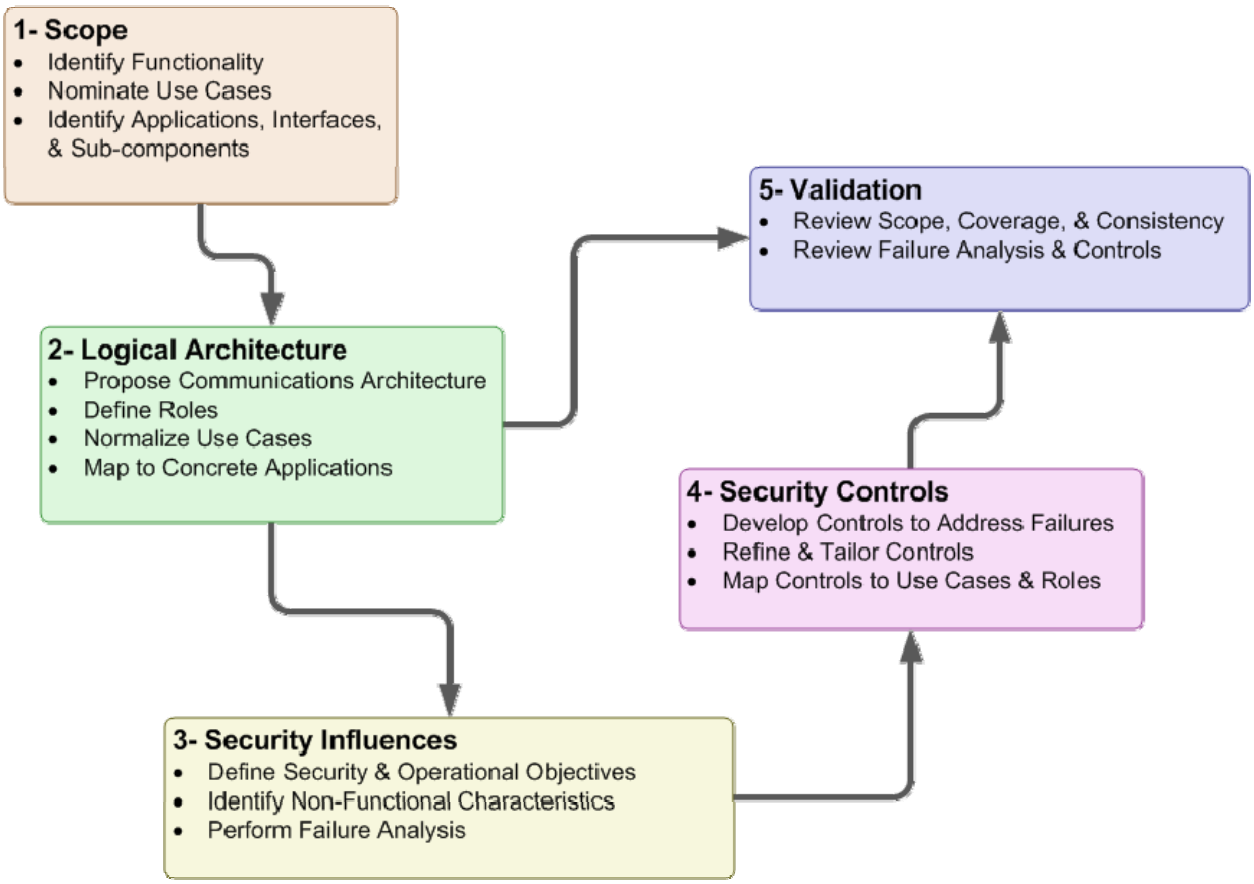

Figure 1 – Overview of Security Profile Development Approach

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:[6]

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 use cases that define what uses of the system are addressed by the security profile and identifies the roles within those use cases that are the targets of the security guidance to be developed.

2. *Construct a logical architecture showing the relationships between roles in the use cases.* The logical architecture ties the conceptual model developed in step 1 above to

[6] For a more detailed description of this process, please see the ASAP-SG Security Profile Blueprint. http://www.smartgridipedia.org/images/4/43/Security_Profile_Blueprint_-_v1_0_-_20101006.pdf

architectures and concrete applications familiar to stakeholders. The logical architecture shows which roles and relationships fall within the scope of the profile and which, though appearing in the use cases, may nonetheless fall outside the scope of the profile.

3. *Identify security influences and objectives.* The specific aims of the security profile are defined here in terms of the logical architecture from step 2. These aims include high-level security guidance that the profile will refine, related security guidance that will be tailored for the security profile, and characteristics of the system that must be preserved as security controls are put into place. This step also includes identification of security related failures that may inhibit the operation of the system.
4. *Define the security controls.* New security controls are defined, existing controls from other security documents are referenced, or both to meet the security objectives defined in step 3. Each role is associated with the set of roles it is expected to implement.
5. *Validation.* This step encompasses a collection of validation checks, such as ensuring that the selected controls are complete with respect to the identified failures (i.e., that there is at least one control for each failure) and that there are no superfluous controls (i.e., for each recommended control, there is a failure that it addresses).

The products of these steps are shown in Figure 2.

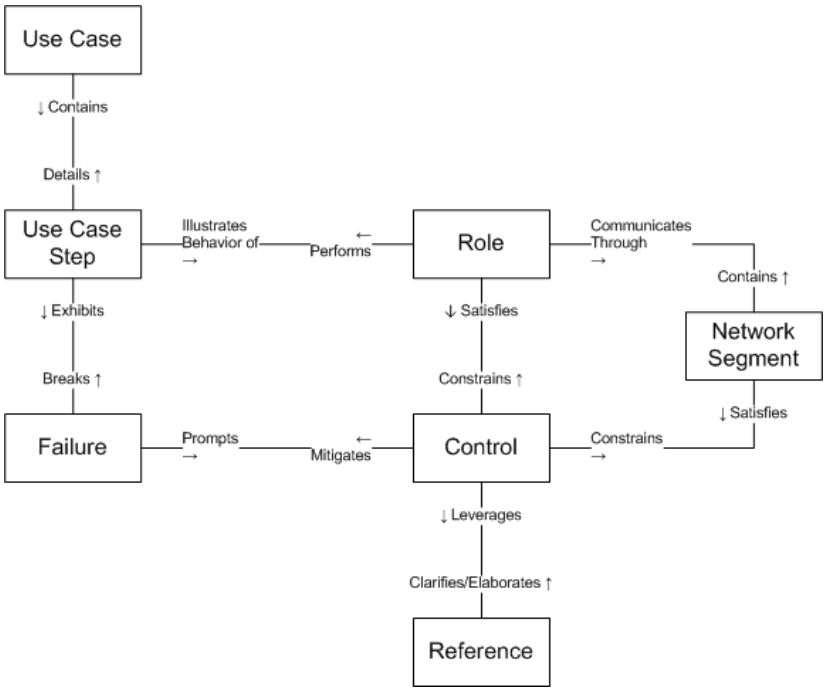

Figure 2 – WAMPAC SP Artifact Relationships

The individual use case steps within each use case provide a detailed view of the activities that are considered within the scope of the profile. Each step is carried out by a specific role, and that role is responsible for the security controls that mitigate potential failures of the step. These potential failures are identified in step 3 above by considering of how each step in these use cases may fail and, consequently, how the failure might prevent the system or role from

successfully carrying out the use case. Each identified potential failure of a step in a use case prompts the development of one or more controls to mitigate it.

Though most controls are assigned to specific roles, some failures 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 failures are mitigated by network controls that focus specifically on protecting the movement of information within the use case. In the WAMPAC profile, these controls take the form of recommended network segmentation (see Section 4.1).

Whenever a control is derived from sources identified in step 4, that source (e.g., reference to a specific NIST IR 7628 requirement number) is noted.

1.3 Audience & Recommended Use

The primary audience of this document is organizations that are developing or implementing solutions requiring or providing WAMPAC functionality through the use of synchrophasor technology. 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 synchrophasor 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 4.2 and Appendix E:.

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 for given failures (impacts) for roles and the functionality they implement (use cases), 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 synchrophasor technology procurement activities
2. configuring and operating synchrophasor systems, and systems built on synchrophasor technology
3. evaluating planned or deployed WAMPAC solutions (see Appendix C: for more information)

In some cases, a utility will not make use of all functionality described in the included use cases, 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 it addresses all the same failures and should perform a risk analysis to confirm the adequacy of the alternative control.

1.3.2 Reliability Coordinator

Reliability Coordinators set direction and establish policy and procedure within the utility and may use this document in a similar fashion to electric utilities, notably with the exception that they will not have any PMUs of their own or any automated connection to system protection and control functions. However, this profile is constructed such that the roles that satisfy these pieces of functionality are considered and analyzed in a modular fashion with respect to the remainder of the reference architecture.

Guidance for all applicable roles and controls may be used with no loss of integrity, as this document provides clear qualifiers where recommendations are conditionally based on underlying functionality. Reliability Coordinators may assume that they do not implement any Class A Applications as defined in Section 1.1.3 above, and follow all recommendations in this document that do not explicitly state an association with Class A functionality.

1.3.3 Synchrophasor (and Derivative Technology) Vendors

Vendors may use this document to incorporate security controls needed for the development of synchrophasor products as well as solutions built upon or derived from synchrophasor 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 use cases also offer tools for understanding synchrophasor applications in an abstract sense.

2 Functional Analysis

The purpose of the functional analysis is to define a clear picture of the scope, architecture, and functionality of wide-area monitoring, protection, and control (WAMPAC) systems, as addressed by this security profile. The real-world specific performance of WAMPAC 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 Alignment role may be performed by a stand-alone component, or rolled into a platform that also performs many of the analysis and presentation functions as defined in the Application role. Conversely, some implementations may have the automated decision-making functionality of the Application role deployed in a central server as well as on hardened platforms out in the field. Regardless, this profile defines roles in such a way that the logical architecture and use case functionality 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 WAMPAC systems and functions.
2. Define abstract roles that characterize elements of WAMPAC systems concisely. Roles are neutral to implementation and vendor, and capture the essence of common functionality without the details of particular applications. The resulting roles are presented in Section 2.2. Their relationships with each other (topologically) are presented in Section 2.1.
3. Define use cases describing how the roles interact to implement WAMPAC functionality. The use cases are modular in nature, which allows organizations to determine which use

cases 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 use cases are presented in Section 2.4.

4. Validate the roles and use cases by ensuring that they are adequate to describe common real-world implementations. The mapping between roles and real world implementations are presented in Section 2.2.13 (this is presented before the use cases to reinforce the meaning of the roles).

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 WAMPAC systems in important ways and so are included as context. Specifically, the following roles are in-scope for this profile, and security recommendations are provided for each in Section 4.3:

- Alignment
- Application
- Data Store
- Environmental Data Interface
- Field Alignment
- Field Application
- Phasor Gateway
- Phasor Manager
- Phasor Measurement Unit
- Registry

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 2.2.13 for more information).

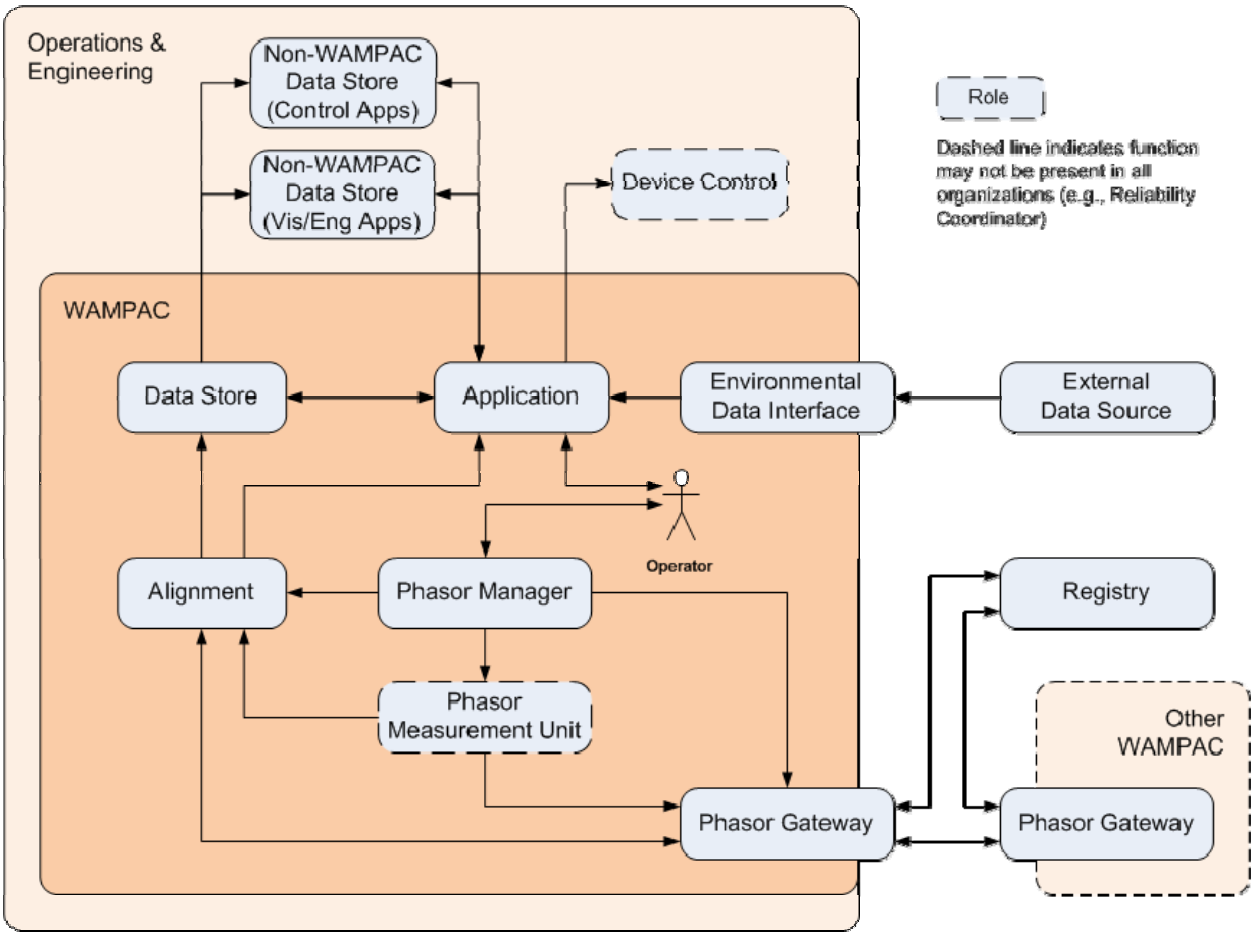

Figure 3 – WAMPAC Logical Architecture

The essential roles involved in WAMPAC systems are shown in Figure 3. This diagram presents several ideas:

- Human and software/hardware roles are distinguished by shape. Roles that are implemented in software and/or hardware are shown as rounded rectangles and roles representing people are shown as stick figures.
- Roles that have a dashed outline may not be present in all implementations. For example, a Reliability Coordinator (RC) will not have any form of Device Control or any of their own PMUs. Transmission Owners (TO) may or may not have implemented the system in such a way as to have an electronic link to Device Control (e.g., a SCADA system or an RTU) for automated protection and control functionality.
- Large, rounded, shaded regions represent different areas in which the roles are typically deployed. The principal distinction is between roles that are deployed within an organization vs. external to the organization, and between roles that are explicitly part of a WAMPAC system vs. those in other parts of the same organization.

- Lines between roles represent interactions; arrows indicate the direction of *primary* interaction.[7]
- Multiplicities between roles are not depicted, but are generally many-to-many. That is, a device serving the Alignment role may receive data from multiple PMUs and may also interact with multiple Applications.

All software/hardware roles are assumed to have some inherent communications ability (i.e., there is no need to model a distinct communications element associated with each software/hardware role).

2.2 Role Definitions

All roles are defined in the following sub-sections.

2.2.1 Alignment

This describes the version of the Alignment role that executes in the control center, and aggregates multiple PMU samples with equal timestamps into a single time-aligned packet. Alignment does not function as a persistent repository, and data is retained (or buffered) only until it is transmitted, discarded, or stored persistently (e.g., if data arrives too late to be collected in a super packet). Note that this role describes many, but not all of the functions performed by many Phasor Data Concentrators (PDCs) found on the market. Specifically, this role separates alignment functionality from management functions. Please see Section 4.3 on mapping to real-world functionality for a more in-depth explanation.

The responsibilities of the Alignment role are:

- Aggregate incoming data for the current time period into a super-packet
- Buffer incoming data until all data has been received
- Monitor the clock (GPS) and determine when data has reached maximum allowable time lag
- Send data to the Data Store as appropriate
- Interact with other roles to ensure that the synchrophasor information is correctly configured end-to-end and that the Alignment is correctly configured to receive the time-series data from PMUs
- Interact with PMUs to control their data streams

[7] For example, the Environmental Data Interface most often sends new data to an Application, but this could take place through either a push or pull arrangement. In the figure, the mechanics of negotiating and managing the information flow are not represented, while the general flow of information is depicted using an arrow from the Environmental Data Interface to the Application.

2.2.2 Field Alignment

This is the version of Alignment that executes in the field. Its functional description is the same as for the version of Alignment that executes in a control center, but because it is in the field some of its logical and physical control requirements will be different. This is true not only for the Field Alignment software itself, but also for the software and hardware platforms that support it. The differences in control requirements are present throughout the engineering life cycle (including design, implementation, acquisition, deployment, operations, maintenance, and decommissioning). Specifically, system resources may be more constrained in a field-deployed device than a centrally-deployed platform, and/or connectivity may or may not be available to central servers.

The Field Alignment role is not shown separately in the logical architecture (Figure 3) or the use cases (Section 2.4) as it performs and interacts just as the Alignment role does.

2.2.3 Application

This is a program that executes in a control center. It depends critically on time-synchronized phasor measurements for its primary task. Examples include decision making applicable for wide area monitoring; real time dynamics and stability monitoring; dynamic system ratings for operating power systems closer to the margin to reduce congestion costs and increasing asset utilization; and improvements in state estimation, protection, and controls. The responsibilities of the Application role are:

- Interact with the Data Store and Alignment as appropriate to gather and save data used to determine appropriate actions
- Send commands to Device Control if necessary

2.2.4 Field Application

This is a program that executes in the field. Its functional description is the same as for Application, but because it executes in the field some of its logical and physical control requirements will be different. This is true not only for the Field Application itself, but also for the software and hardware platforms that support it. The differences in control requirements are present throughout the engineering life cycle (including design, implementation, acquisition, deployment, operations, maintenance, and decommissioning).

The Field Application role is not shown separately in the logical architecture (Figure 3) or the use cases (Section 2.4) as it performs and interacts just as the Application role does.

2.2.5 Data Store

A Data Store is a persistent repository of time-series data typically used for purposes of off-line analysis by WAMPAC and Non-WAMPAC applications. The responsibilities of the Data Store are:

- Store information received
- forward full-resolution or down sampled data information to Non-WAMPAC Data Stores as appropriate

- Return data as requested in response to queries

2.2.6 Environmental Data Interface

This is an interface or proxy that bridges the network used by Applications and other networks that provide access to sources of external data, including but not limited to weather, traffic, fire, and other relevant regionally-specific data. Data accessed via this interface is provided by one or more External Data Sources. The responsibilities of the Environmental Data Interface are:

- Request environmental data from External Data Sources
- Forward environmental data to all relevant Applications

2.2.7 External Data Source

This is a source of data that does not originate with the electric utility, but that is used by one or more WAMPAC Applications as an overlay or to provide additional context information to the Operator. This data is always accessed through an Environmental Data Interface.

2.2.8 Non-WAMPAC Data Store

This is a utility operated data store that supports other operational, but non-WAMPAC applications that do not rely critically on time-synchronized phasor measurements for their primary tasks. Non-WAMPAC Data Stores are classified in this document as supporting either control applications or visualization/engineering applications.

2.2.9 Phasor Gateway

This is software that bridges one or more utility networks for the purpose of exchanging phasor measurement data. A Local Phasor Gateway is owned by the utility in question and is used to provide data to other utilities. A Remote Phasor Gateway is owned by another utility and provides data to the utility in question. The specific responsibilities of a Phasor Gateway are:

- Forward PMU data to all Remote Phasor Gateways with verified access to that PMUs data
- Forward PMU data received from a remote PMU to Alignment
- Interact with the Phasor Manager to ensure that PMUs are appropriately configured so that the Phasor Gateway can process PMU data
- Sends description of local PMU to Registry and/or Remote Phasor Gateway(s) as appropriate and maintains association between Registry ID and local PMU ID
- Forwards changes in status of remote PMUs to the local Phasor Manager, and changes in status of local PMUs to the Registry, and/or Remote Phasor Gateway(s) as appropriate
- Forwards PMU search query to the Registry and forwards responses to the local Phasor Manager
- Interacts with the Registry and/or Remote Phasor Gateway(s) to terminate data streams from either a local PMU or a remote PMU

2.2.10 Phasor Measurement Unit (PMU)

This is a sensing and reporting device that measures magnitude and phase angle of a voltage signal at fixed points in time. All PMUs take their measurements at the same instant, and coordination for this purpose is achieved by using a common clock (e.g., via GPS time). A PMU may be a standalone device or embedded within a multi-function Intelligent Electronic Device (IED) such as a protective relay, meter, or digital fault recorder. A PMU also contains a communication sub-system for reporting its measurements. The specific responsibilities of a PMU are:

- Monitor an external high resolution clock
- Compute phasor measurement and add a time stamp
- Send phasor data to Alignment and possibly the Phasor Gateway
- Interact with the Phasor Manager, Alignment, and Phasor Gateway to ensure that configuration information is consistent across these roles
- Process commands to start or stop data streams to particular clients

2.2.11 Registry

A registry is standalone software or a module within some other software that often resides outside the utility's organizational boundaries, and serves to facilitate lookup of metadata for PMUs within other organizations. It maintains a list of all PMUs known to the registry, and all information necessary to communicate with those PMUs for any purpose. The specific responsibilities of the Registry are:

- Assign a unique ID to each registered PMU
- Remove PMUs from the Registry as requested
- Notify appropriate Remote Phasor Gateways of PMUs that have been registered or whose status has been modified
- Update PMU status information as informed by Phasor Gateways
- Return PMU identification information and other permitted metadata in response to search queries

2.2.12 Phasor Manager

This is standalone software or a module within other software that permits the management of one or more PMUs. Management tasks performed by the Phasor Manager include enabling and disabling PMUs, providing information about its managed PMUs to other roles, and forwarding requests to reconfigure a PMU on behalf of another role. The specific responsibilities of the Phasor Manager are:

- Coordinate configuration data between PMU, Alignment, and the Operator as appropriate

- Interact with the Operator to initiate, modify, or terminate a PMU's data stream to Alignment or the Phasor Gateway and to inform the Operator of appropriate PMU status information
- Send PMU identity and description to the Local Phasor Gateway for dissemination to other organizations as appropriate (i.e., to a Registry or Remote Phasor Gateway)
- Forward commands from an operator to a PMU as appropriate
- Forward PMU search queries (e.g., from a local operator) or search results (e.g., in response to a query from an operator in an external organization) to the Phasor Gateway.

2.2.13 Device Control

This is an abstract role that provides a service to a WAMPAC Application for advanced protection and control functions. The Device Control role brokers changes in power system devices that affect circuit configuration or voltage attributes. This role interacts with the Utility SCADA system to execute actuator commands.

2.3 Role Mappings

This section demonstrates several examples of how the logical architecture presented in Section 0 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 Application of Logical Architecture: Wide Area Stability and Voltage Control

Transmission of power on today's electric grid often requires reactive power compensation for voltage control, transient stability, and power quality improvement. To provide dynamic reactive compensation a utility will typically use a static VAR compensator (SVC) comprised of advanced power electronics devices with software-based information and control systems. The utility will then use phasor measurements (providing instantaneous voltage and phase angles at various points of the grid) to intelligently control the oscillations within the power system by coordinating the control of compensation devices to vary the capacitance, reactance, and transformer tap changers, ultimately improving overall system operation. The application uses advanced algorithms to process the phasor measurements to derive control inputs to capacitor/reactor banks for swing stabilization.

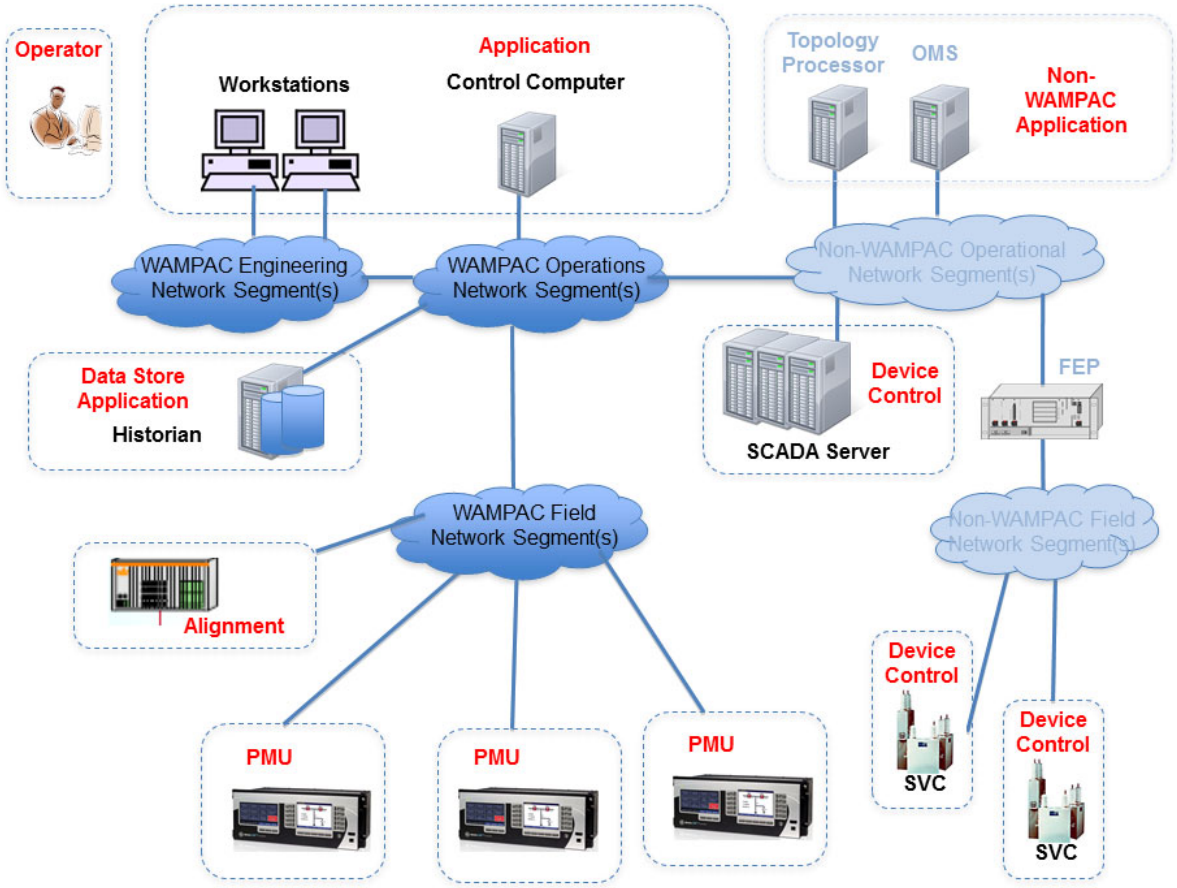

Figure 4 – Wide Area Stability and Voltage Control

Figure 4 shows how the logical architecture may be applied in a wide area stability and voltage control application with the centrally deployed control computer acting as a WAMPAC Application. Icons of various devices represent equipment and systems deployed in a utility network. Red text denotes the roles as implemented by each device or devices. The clouds denote the network segments (see Section 4.1) on which the devices are deployed.

This WAMPAC Application typically uses utility-owned PMU data to compute the control signals for reactive power compensation with the workstations provide the human-machine interface for the Application. The PMUs are located in the field and are connected via the WAMPAC Field Network Segment(s), providing the phasor measurements for the WAMPAC Application. The Alignment role temporally correlates various PMU data before the Application processes the data. The Historian acts as the WAMPAC Data Store to archive the time-series phasor data, and also acts as a WAMPAC application by performing specific time-series data archiving and retrieval. The Historian along with the WAMPAC Application that computes control signals for reactive power compensation are centrally located in the operations center and connected to the WAMPAC Operations Network Segment(s), along with operator workstations that provide situational awareness for grid operators. Engineering workstations are typically connected to the WAMPAC Engineering Network Segment(s), and facilitate additional management and oversight of field-deployed equipment. Once the control outputs are generated,

the WAMPAC Applications communicate control settings to the SCADA Server and hand off control execution to the SCADA system in the utility network. The SCADA Server and the SVC are the actual control dispatch and actuator elements, and assume the role of Device Control.

2.3.2 Application of Logical Architecture: Post-event Analysis

Phasor measurements provide high-resolution situational understanding of the state of the power system; however in the absence of phasor data, the state estimator uses voltage at each bus along with reactive and real power measurements to compute phase angles across the network. The process of calculating an estimate of system state in this manner is time consuming and provides only periodic snapshots of the system operation. In contrast, phasor measurements provide more information at high-speed and accurately time-stamped, and can reveal the actual line loading, power flow, and other early indications of system disturbances. While advanced applications can utilize this high-speed, high-resolution data to perform real-time system protection, this data can also be used for effective post-event analysis. Archived time-series phasor data can reveal the propagation of adverse events allowing for future system planning and improved provisioning. In many implementations, the capability to perform analyses with phasor measurements will reveal insights that could not feasibly be calculated using only traditional voltage and current measurements. Specifically, phasor measurements will provide the ability to determine precise power system conditions such as power flow on a continual basis.

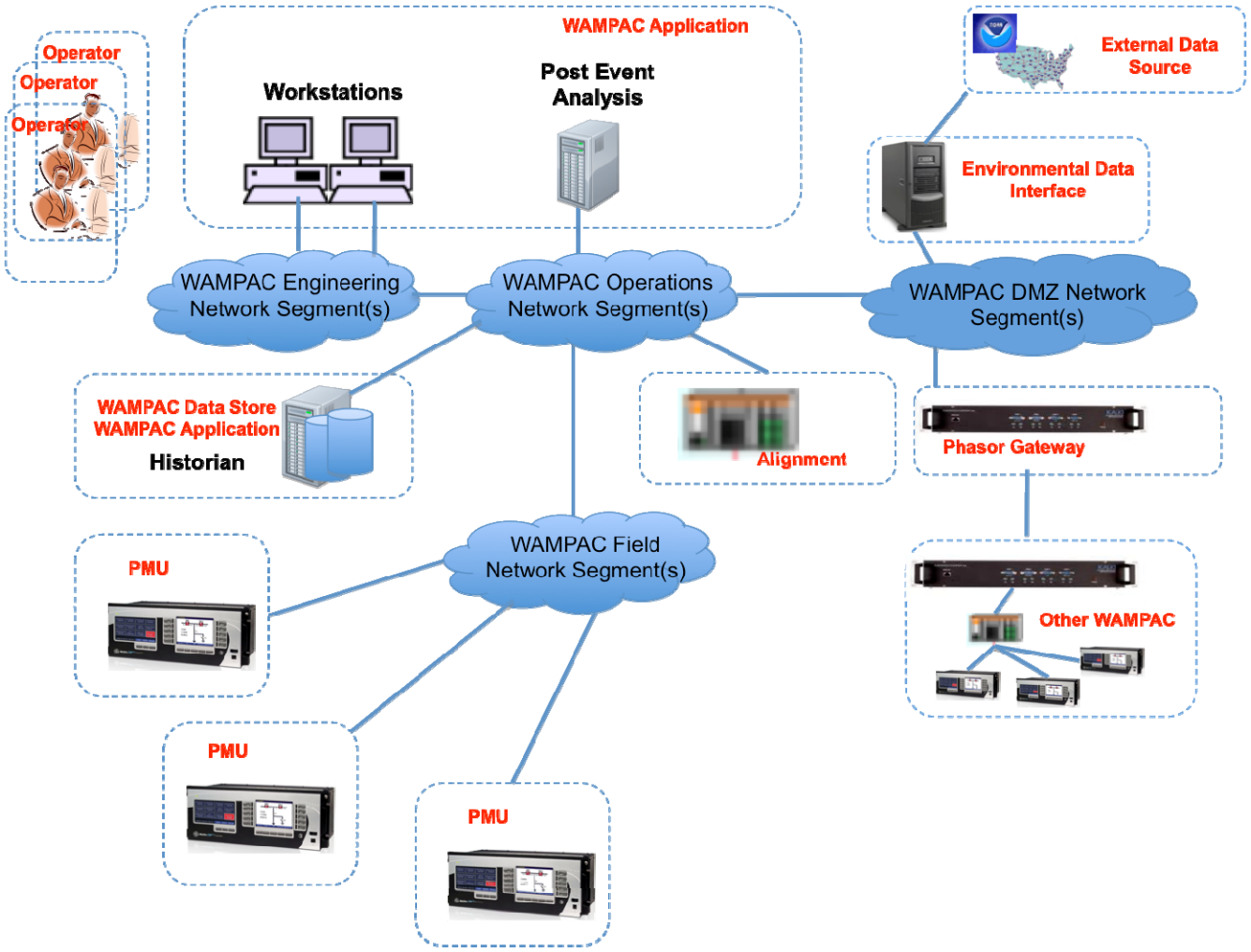

Figure 5 – Post-event Analysis

Figure 5 shows how the logical architecture could be applied with post-event analysis as a centrally deployed WAMPAC Application. This WAMPAC application will retrieve the relevant data from the archive and process system variables as they correspond to the progress of a disturbance across the system. The workstations provide the human-machine interface to the operator for analysis and engineering planning activities. Post-event analysis also often requires environmental data for performing root-cause analysis, particularly in the events of unusual loading (e.g., severe weather patterns) and system faults (e.g., line to ground due to lightning strikes). The Historian acts as the WAMPAC Data Store and WAMPAC Application for archiving and retrieving spatially and temporally correlated phasor and environmental data. The web-proxy serves as the Environmental Data Interface to access the External Data Source for weather, traffic, fire, and other contextually relevant information. Often phasor data from neighboring utilities is also required for effective post-event analysis, in which case the Phasor Gateway provides access. Both the Environmental Data Interface and Phasor Gateway are connected through WAMPAC DMZ Network Segment(s). In this example, the Alignment role is centrally located and performs the correlated time-series alignment of the data from PMUs internal and external to the utility. The PMUs are located in the field and reside in the WAMPAC Field Network Segment(s).

2.3.3 *Application of Logical Architecture: Distributed Voltage Stability Control*

Wide Area Control and Voltage Stability functionality can also be deployed in a distributed manner by using intelligent synchronous vector processor (SVP) devices. Power flow across a line can be controlled using static VAR compensators (the SVC) devices and, in many instances, optimal local operation can be achieved by coordinated and distributed control of these devices using SVPs. Control decisions can be made in the field with a subset of phasor measurements and a locally-deployed situational awareness application performing supervisory control of the SVP devices. The following application demonstrates one such implementation across a line with two source buses with PMUs and an SVC device for implementing the control signals.

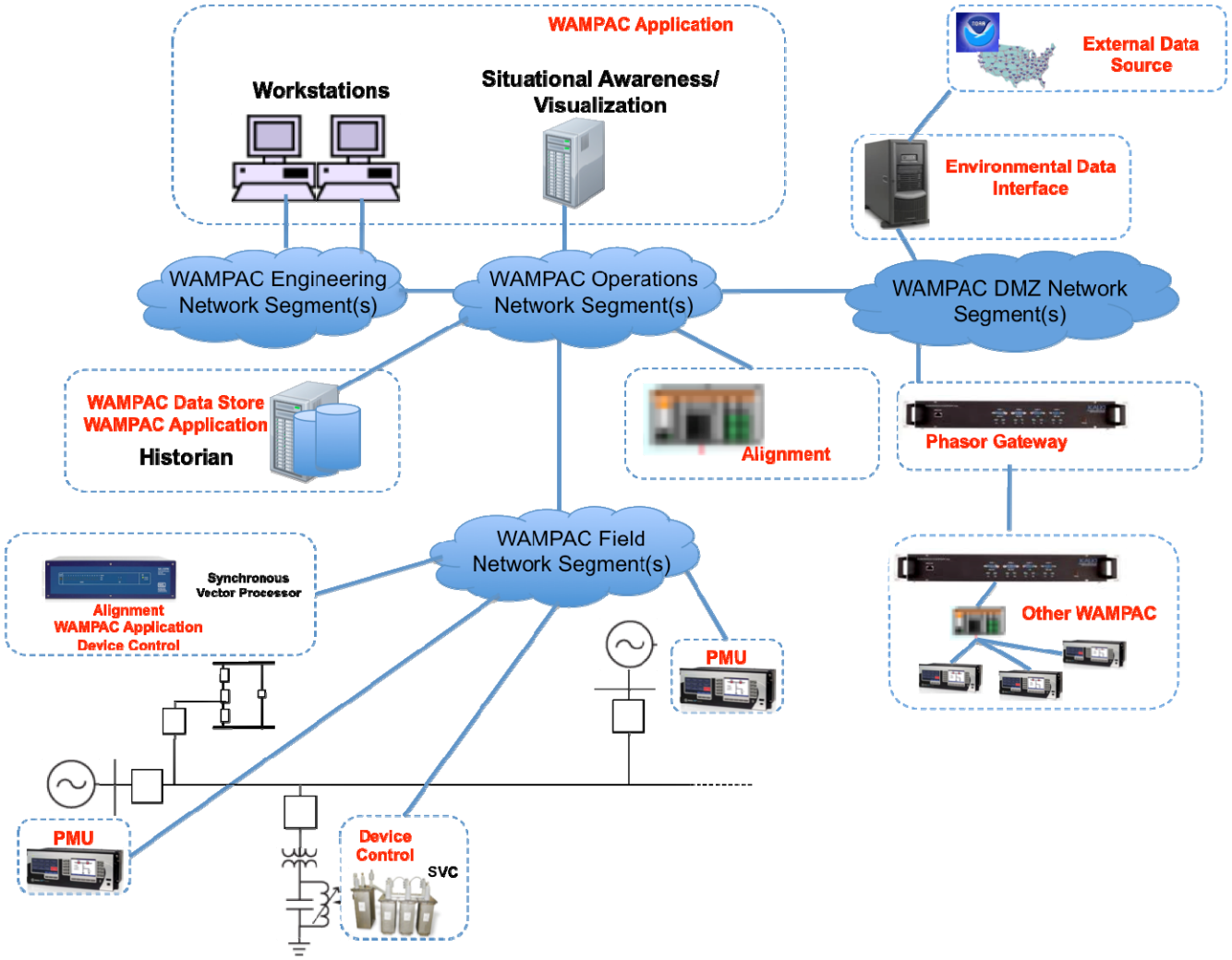

Figure 6 – Distributed Voltage Stability Control

Figure 6 shows how the logical architecture may be applied in a distributed voltage stability control application with the field-deployed SVPs serving the roles of a WAMPAC Field Application, Alignment, and Device Control. The PMUs are deployed in the field at the source buses, and reside along with the SVPs in the WAMPAC Field Network Segment(s). The workstations provide the human-machine interface for the centrally-deployed, situational awareness WAMPAC Application, which in turn performs supervisory coordination of the SVP

devices in the field. The Historian acts as the WAMPAC Data Store to archive the time-series phasor data. Both the Historian and the situational-awareness WAMPAC Application are centrally located in the operations center and connected to the WAMPAC Operations Network Segment(s), along with operator workstations that provide situational awareness for grid operators. Engineering workstations are typically connected to the WAMPAC Engineering Network Segment(s), and facilitate additional management and oversight of field-deployed equipment.

2.4 Use Cases

This section presents a superset of the use cases that are needed to realize a WAMPAC system. A given WAMPAC system may only implement a subset of these use cases.

The use cases are designed to be composable. For example, a particular activity may be the result of several different actions; and in such cases the common activity is called out as a separate use case that is then linked to other use cases that precede it or follow it. The result is that a single, long thread of activity may be represented by the composition of several related use cases. Future versions of this Security Policy we will add additional use cases including one specifically will covering Environmental data transportation to the internal environment.

This security profile defines WAMPAC functionality using the following use cases:

- Use Cases 1-6 deal with steady-state operations assuming all communication channels have been established. This covers:
    - Generation of measurements
    - Distribution of phasor data to local applications & other organizations
    - Access to non-PMU data
    - Application processing
- Use Cases 7 and 8 deal with the establishment and control of data streams within an organization (i.e., control of data streams from one's own PMUs).
- Use Cases 9-13 deal with sharing information about PMUs with other organizations.
- Use Cases 14-16 deal with the establishment and termination of data streams extending to and coming from other organizations.

These use cases do *not* include security controls, such as the use of authentication or encryption. Security controls and their mapping to the roles performing these use cases are found in Section 4.

Each use case contains the following elements:

- Use Case Description: This is a summary of the use case, describing the overall flow and steps.
- Preconditions: These are conditions that must be true for the use case to be successfully executed.

- Minimal Guarantees: These are properties that must remain true any time the use case is initiated, regardless of whether it terminates successfully.
- Success Guarantees: These are properties that will be true only if the use case terminates successfully. This requires that all preconditions and all condition checks (e.g., for validity of a request) be satisfied during execution of the use case.
- Trigger: This is the stimulus that initiates execution of the use case.
- Main Success Scenario: This defines the series of steps undertaken by each role during successful execution of the use case. The scenario is depicted graphically in an activity diagram (the notation used in these diagrams is explained in Appendix B) and each step is summarized in text.

Use Case 1: PMU Generates New Data

Use Case Description: This use case describes how a PMU monitors local power system parameters, such as current and/or voltage inputs, and generates time stamped phasor measurements. The use case assumes that the PMU is either configured for spontaneous transmission or that a data start command has been received to start the data stream if the system utilizes commanded mode.

Preconditions:

- The PMU is installed, operating correctly, and has all of the necessary network connections available.
- The PMU is synchronized with a time source of sufficient accuracy.
- The PMU has been initialized and received a start data command if system utilizes commanded mode.
- The PMU has been initialized and data is being sent continuously if the system utilizes spontaneous mode.

Minimal Guarantees:

- The PMU sends data to the Phasor Gateway and Alignment in a timely manner.

Success Guarantees:

- All data sent from the PMU has a correct and accurate time stamp.

Trigger:

The trigger for this use case is the PMU beginning the transmission of the data stream(s).

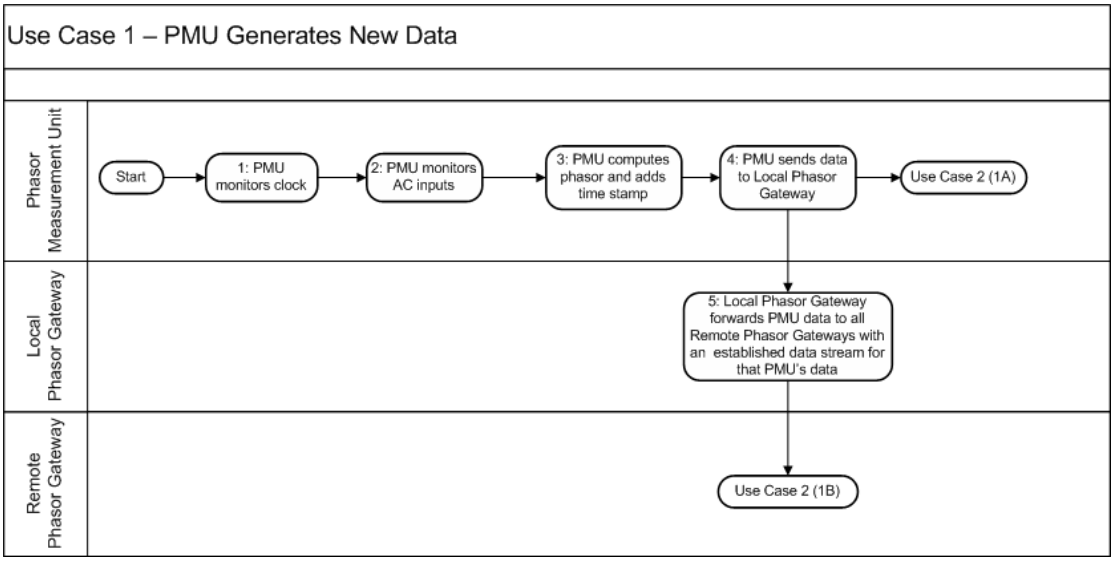

Diagram: Use Case 1: PMU Generates New Data

Main Success Scenario:

1: The PMU monitors its assigned external clock source. The PMU synchronizes its internal clock to the external clock source.

2: The PMU monitors AC inputs (one or more) derived from instrument transformers connected to the power grid. Each AC input is then converted to digital quantities representing magnitude and phase angle (i.e., phasor).

3: The PMU assembles all phasor measurements into a data frame adding time stamp, status, quality, and other diagnostic data.

4: The PMU sends the data frame to the Local Phasor Gateway. This triggers Use Case 2 (1A), in which the PMU sends the same information to Alignment.

5: The Local Phasor Gateway receives the data frame and forwards to all Remote Phasor Gateways that have valid subscriptions to data from the PMU. This triggers Use Case 2 (1B), in which the Remote Phasor Gateway brings the PMU data into its organization's WAMPAC system.

Use Case 2: Alignment Processes PMU Data

Use Case Description: This use case describes how Alignment receives and processes a data frame from a Phasor Gateway (indicating data from another organization) or directly from a PMU (indicating data from the same organization). The use case assumes that Alignment and all associated PMUs are configured and initiated.

Preconditions:

- Alignment is installed, operating correctly, and has all of the necessary network connections available.
- Alignment is synchronized with a time source of sufficient accuracy.

Minimal Guarantees:

- Alignment only processes valid data.
- Alignment only buffers data which does not exceed the maximum lag time.
- Alignment sends data frames to the Data Store unaltered.

Success Guarantees:

- Alignment reaches the maximum lag time or receives all expected data, then proceeds to Use Case 3 where Alignment aggregates the buffered data.

Trigger:

There are two possible triggers for this use case.

- Alignment receives a data frame from a PMU.
- Alignment receives a data frame from a Phasor Gateway.

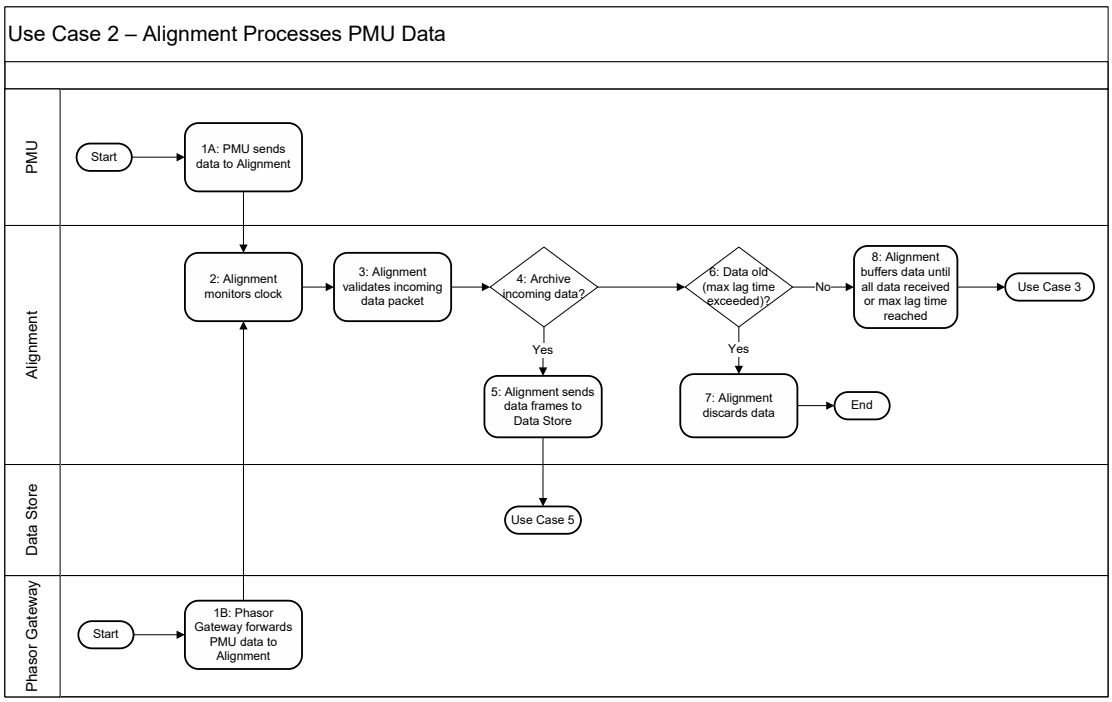

Diagram: Use Case 2: Alignment Processes PMU Data

Main Success Scenario:

1A: A PMU sends a data frame directly to Alignment.

1B: A Phasor Gateway forwards data from a remote PMU to Alignment.

2: Alignment monitors its assigned external clock source. Alignment synchronizes its internal clock to the external clock source.

3: Alignment validates the received data. Examples include simple range validation based on data type (e.g., $-180 \leq$ angle < 180 or $59.90 \leq$ frequency ≤ 60.10).

4: Some set of incoming data frames is usually archived. For example, Alignment could archive all validated data frames or only late data frames (i.e., those that are too late to be included in a super packet). The appropriate check is made in this step.

5: Alignment sends a copy of the incoming data frame to the Data Store. This is the store of record, and Use Case 5 shows how the data frames are processed at the Data Store.

6: Alignment determines whether the incoming data frame has exceeded the maximum lag time.

7: Data that exceeds the maximum lag time is discarded.

8: If the maximum lag time has not been exceeded, Alignment buffers the data frame. This triggers Use Case 3, in which Alignment determines whether it is time to assemble and send a super packet.

Use Case 3: Alignment Aggregates Data and Sends Super Packet

Use Case Description: This use case describes how Alignment assembles a super packet from multiple data streams. The use case assumes that Alignment is initiated and configured to send data to a WAMPAC Application.

Preconditions:

- Alignment is installed, operating correctly, and has all of the necessary network connections available.

Minimal Guarantees:

- Data from individual data streams shall not be altered when assembled into a super packet.

Success Guarantees:

- All relevant Applications receive the super packet.
- The super packet is archived in the Data Store.

Trigger:

This use case is triggered when the maximum lag time had been reached or all expected data has been received by the Alignment.

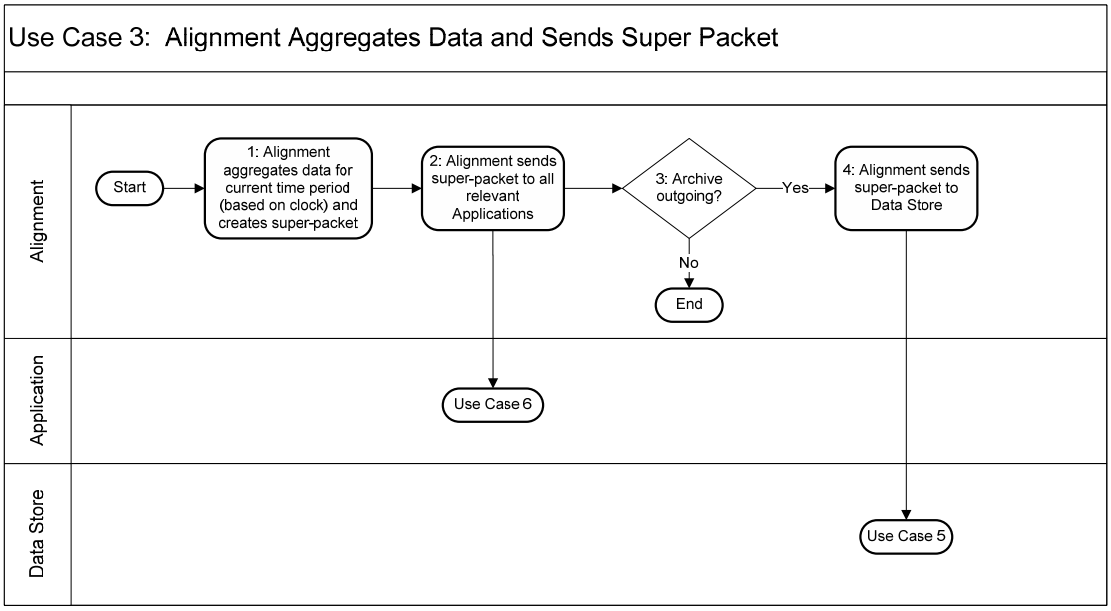

Diagram: Use Case 3: Alignment Aggregates Data and Sends Super Packet

Main Success Scenario:

1: When the clock indicates that it is time to send a new super packet, Alignment aggregates time aligned data from individual incoming data streams to create a super packet.

2: Alignment sends the super packet to all relevant Applications. This triggers Use Case 6, in which an Application processes the super packet.

3: In some system architectures, historical data is archived at this point (as opposed to when data arrives, in Use Case 2). Alignment decides whether to archive the outgoing super packet in this step.

4: If the outgoing super packet is to be archived, Alignment sends the super packet to the Data Store. This triggers Use Case 5, in which the Data Store processes the super packet.

Use Case 4: Environmental Data Interface Forwards Data to an Application

Use Case Description: This use case describes how an Application obtains data concerning weather, traffic, or other events and phenomena relevant to the operation of a power system that are used by the Application to augment its PMU dependent functions. The source of the external data is an entity not part of the utility, nor necessarily responsive to the utility's needs (e.g., weather data provided by NOAA). Data obtained via this use case is distinguished from other types of external data (e.g., an external source of time such as provided by GPS or an atomic clock) in that environmental data is not critical to the operation of the Application (i.e., the environmental data somehow improves or augments the Application's PMU-related functions, but is not necessary to perform them).

Preconditions:

- The Environmental Data Interface is installed, operating correctly, and has all of the necessary network connections available.
- The data to be forwarded is accessible by the Environmental Data Interface.
- The Application is ready and able to receive data from the Environmental Data Interface.

Minimal Guarantees:

- The Environmental Data Interface will forward data only to Applications that expect to receive it.
- Only the expected data will be forwarded by the Environmental Data Interface to an Application.

Success Guarantees:

- The Applications have the data that they expected to receive from the Environmental Data Interface.

Trigger:

There are two possible triggers for this use case.

- An External Data Source sends an update of its data to the Environmental Data Interface.
- The Environmental Data Interface retrieves an update from an External Data Source. This could be a periodic request or based on a change in interested Applications, their interests, or both.

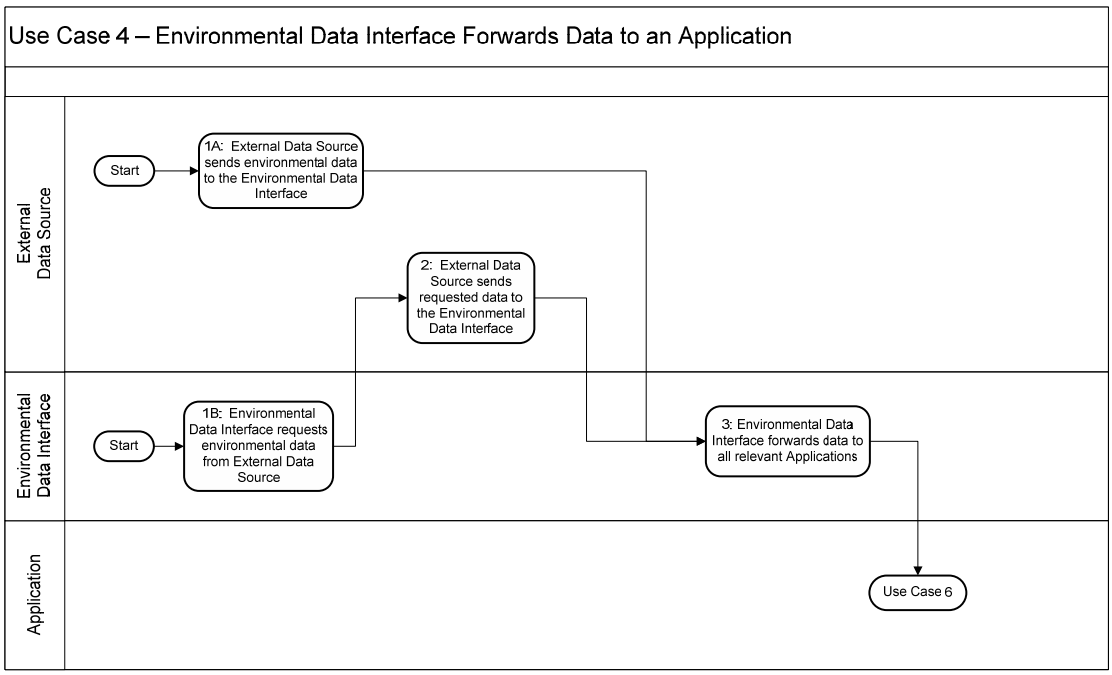

Diagram: Use Case 4: Environmental Data Interface Forwards Data to an Application

Main Success Scenarios:

1A: The External Data Source sends data to the Environmental Data Interface. The data push may occur at any time: triggered periodically, by set conditions (which could be determined by the source of data, the Environmental Data Interface, or both), or any combination.

1B: The Environmental Data Interface requests data from an External Data Source. This request may occur periodically or in response to conditions determined by the Environmental Data Interface, its potential recipients, or both.

2: The External Data Source receives the request, identifies data relevant to the request, and transmits that data to the Environmental Data Interface.

3: The Environmental Data Interface matches the incoming data or aspects of it with interested Applications and then forwards to the appropriate Application(s). This triggers Use Case 6, in which an Application processes the new data.

Use Case 5: Data Store Records Information

Use Case Description: When the Data Store receives information, it stores the information for later retrieval. In some cases, the information being stored may also be mirrored at other Non-WAMPAC Data Stores to allow Non-WAMPAC Applications to access the data without interfering with the WAMPAC system.

Preconditions:

- The sender is permitted to store data in the Data Store.
- Appropriate connections have been made between the Data Store and any Non-WAMPAC Data Stores in which information is to be mirrored.

Minimal Guarantees:

- No data is removed from the Data Store.

Success Guarantees:

- Newly received data is correctly stored and available for access at a later point in time (presuming there is no subsequent removal of the data).
- If the data is to be mirrored to a Non-WAMPAC Data Store, the same information (without change) is sent to the appropriate Non-WAMPAC Data Store(s).

Trigger:

This use case is triggered whenever another role stores information in the Data Store. Alignment may store super-packets or individual PMU data frames in the Data Store. An Application may store or append additional information, such as tagging data when it fails a validation check.

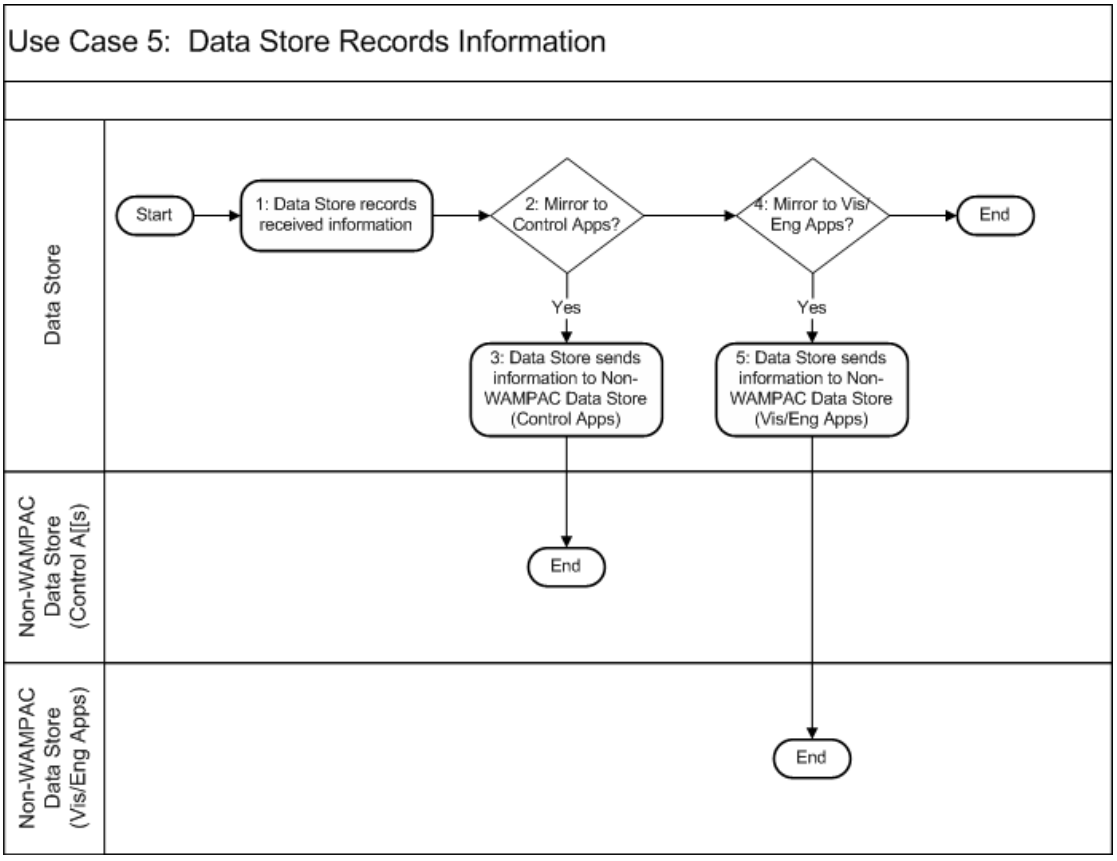

Diagram: Use Case 5: Data Store Records Information

Main Success Scenario:

1: The Data Store receives information and stores it unaltered for later recall.

2: The Data Store examines its configured set of rules and parameters to determine if some or all information received should be mirrored to a Non-WAMPAC Data Store supporting control applications. This would typically be the same PMU data found in super-packets.

3: If the data is to be mirrored to a Non-WAMPAC Data Store supporting control application, the Data Store sends the information to a Non-WAMPAC Data Store (Control Apps).

4: The Data Store examines its configured set of rules and parameters to determine if some or all information received should be mirrored to a Non-WAMPAC Data Store supporting visualization and engineering applications outside of WAMPAC. This would typically be the same PMU data found in super-packets.

5: If the data is to be mirrored to a Non-WAMPAC Data Store supporting visualization and engineering applications, the Data Store sends the information to a Non-WAMPAC Data Store (Visualization/Engineering Applications) for storage.

Use Case 6: An Application Processes New Data

Use Case Description: Applications process new data as it arrives. The most common form of new data is super packets received from Alignment. Other forms of new data include various types of data from the Environmental Data Interface.

Each Application will execute its own specific behavior. This use case depicts an abstraction of the superset of behaviors and interactions that an Application could execute on reception of new data. A particular Application may execute separate portions of the use case based on the type of data that arrives. These differences are represented by the sequence of choice blocks in the diagram.

Preconditions:

- The Application has been configured to expect the arriving data (e.g., if the arriving data is a super packet, then the Application is aware of all included PMUs).

Minimal Guarantees:

- The Application takes no undue action.
- The Application does not corrupt or destroy any existing data.

Success Guarantees:

- The Application takes all appropriate actions given the new data and current state of the system.

Trigger:

The Application receives new data or a signal from Alignment or Environmental Data Interface.

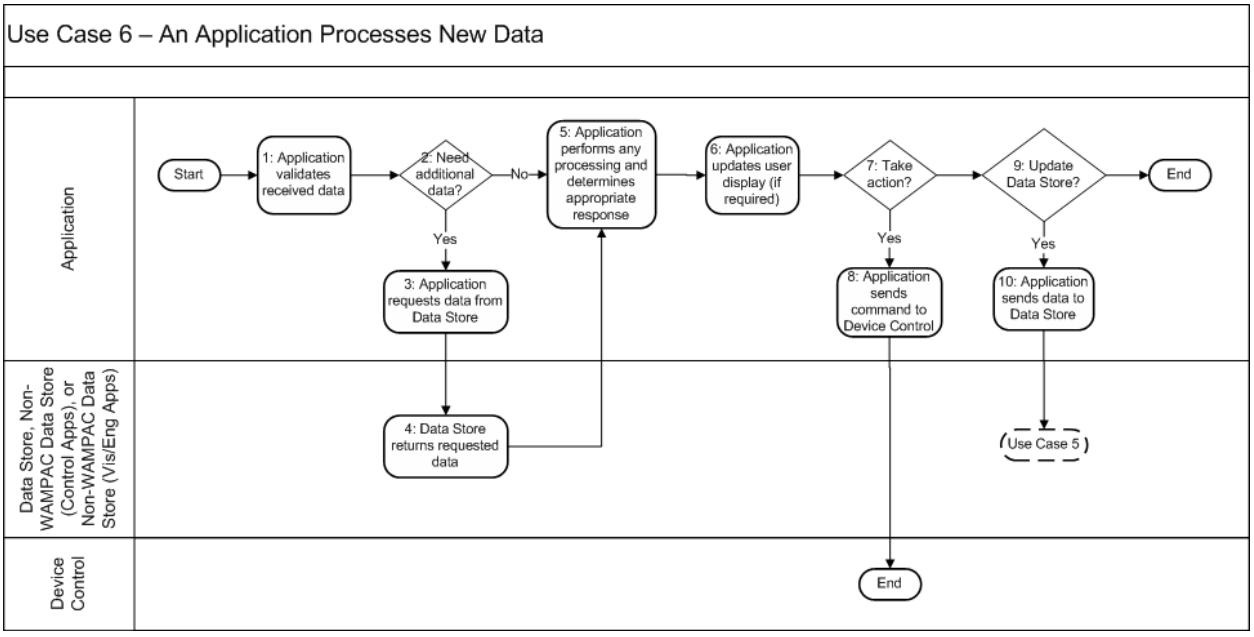

Diagram: Use Case 6: An Application Processes New Data

Main Success Scenario:

1: The Application validates the data it has received. If the received data is a super packet, validation could include range checks on PMU data, that all PMUs identified in the packet are known to the application, or that the time on the packet is within an allowable interval from the current time.

2: Some types of Applications need to retrieve additional data from a Data Store or Non-WAMPAC Data Store to complete their processing. For example, historical PMU data from the Data Store and historical switch positions from a Non-WAMPAC Data Store would be used for a post-event analysis Application. In this step, the Application determines if it needs such information.

3: If the Application needs additional data, it requests the needed data from the appropriate Data Store or a Non-WAMPAC Data Store.

4: The Data Store or Non-WAMPAC Data Store retrieves the requested data and sends it to the requesting Application.

5: The Application next determines what to do in response to the new data. The type of decision making varies among different types of Applications. For example, Class A Applications may send out control commands to Device Control, Class B Applications will integrate data into Non-WAMPAC Applications such as a state estimator, Class C Applications will present visualization of the data in a format useful for the Operator to make decisions, and Class D Applications will run off-line analyses.

6: If the Application includes a user interface and an update is required, the user interface is updated to reflect the new data and any decisions that have been made.

7: Some types of Applications are able to take action on physical devices without Operator supervision. In this step, such Applications determine whether the calculations and decisions made in step 5 call for commands to be sent to physical devices.

8: If a command needs to be sent, the Application sends the appropriate command for one or more physical devices to Device Control.

9: Some types of Applications generate new data during their processing. In this step, such Applications determine whether this data should be sent to the Data Store or a Non-WAMPAC Data Store to make it available to other roles. Marking data as suspect because of a failed validation check would be one example of data stored in the Data Store. Environmental data is one example of data stored in the Non-WAMPAC Data Store.

10: If data needs to be stored, the Application sends the new data to the appropriate Data Store (or a Non-WAMPAC Data Store). This is followed by Use Case 5 if the destination is the Data Store, in which the Data Store processes the new data.

Use Case 7: Operator Configures Alignment (or Phasor Gateway) for a Data Stream

Use Case Description: In order for the client (either Alignment or Phasor Gateway) to process a data frame received from a PMU, it must first acquire the configuration information for the associated PMU. This configuration information includes data such as the time base utilized by the PMU, number of PMUs in the data frame, station name, PMU ID, and the number of phasors. There are two scenarios for this exchange of configuration information. The first scenario is referred to in this use case as "online access." In this scenario the client sends the configuration request directly to the PMU. The PMU then sends the configuration data to the requesting client. In the second scenario, the operator configures the client independently of the PMU (e.g., importing an IEC-61850 Substation Configuration Language (SCL) file) and is referred to in this use case as "offline access."

Preconditions:

- The PMU has been installed, tested, and has all of the necessary network connections available.

Minimal Guarantees:

- The PMU provides a valid response to a configuration request command for online access to configuration data.
- The current PMU configuration is available in a format suitable to the client for offline access to configuration data.

Success Guarantees:

- The PMU configuration data in the client (Alignment or Phasor Gateway) matches the current PMU configuration.

Trigger:

This use case is triggered when the client (Alignment or Phasor Gateway) requires the PMU configuration information to process a new or re-configured PMU data frame.

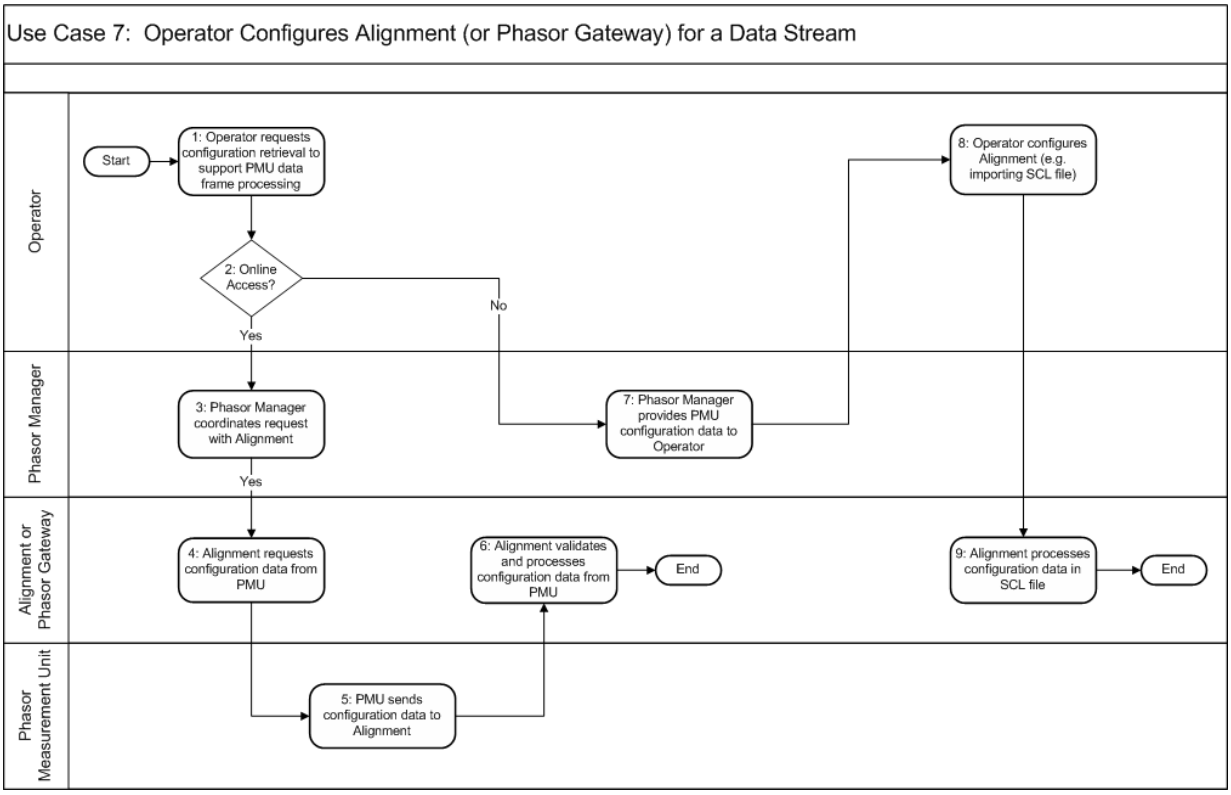

Diagram: Use Case 7: Operator Configures Alignment (or Phasor Gateway) for a Data Stream

Main Success Scenario:

1: An Operator initiates a request via the Phasor Manager to provide the current configuration data from a specific PMU to a client which subscribes to its data stream. This request may be the result of a data stream being available from a new PMU or an existing PMU which has been reconfigured and thus requires new configuration information to be provided to the client (Alignment or Phasor Gateway).

2: Some systems use online access of the configuration information directly from the PMU and some systems use an offline access mechanism. In this step, the Phasor Manager determines how to satisfy the Operator's request (i.e., whether an offline or online process must be used).

3: In the online access scenario, the Phasor Manager forwards the request from the Operator to the client (Alignment or Phasor Gateway). In this context, the request from the Operator is for the client (Alignment or Phasor Gateway) to update its configuration data for a particular PMU.

4: The client (Alignment or Phasor Gateway) receives the request from the Phasor Manager and sends a request to the PMU for its current configuration data. For implementations utilizing the C37.118 standard, this would consist of a "configuration request" command. For implementations utilizing the IEC-61850-90-5 standard, this consists of the client (Alignment or Phasor Gateway) reading the appropriate control block or other mechanism.

5: The PMU receives the request from the client (Alignment or Phasor Gateway) and returns the appropriate configuration data.

6: The client (Alignment or Phasor Gateway) receives the configuration data from the PMU. It processes the configuration data to prepare for receipt of the specific PMUs data stream. Some validation, such as if the expected PMU responded, may be done as part of this processing. Once the client has processed the PMU configuration data, it is now ready to receive the specific PMU's data stream. This ends the Use Case for the online access scenario.

7: In the offline access scenario, the Phasor Manager processes the request by providing configuration data relating to the current configuration of the specified PMU to the Operator. For implementations utilizing the IEC 61850-90-5 standard, this involves the Phasor Manager exporting a version of a SCL file. For implementations utilizing the C37.118 standard, this may be done in a proprietary or non-standard method (e.g., manually).

8: The Operator inputs the PMU configuration information into the client (Alignment or Phasor Gateway). For implementations utilizing the IEC 61850-90-5 standard, this involves the client importing the SCL file generated by the Phasor Manager. For implementations utilizing the C37.118 standard, this may be done in a proprietary or non-standard method (e.g., manually utilizing information provided by the Phasor Manager).

9: The client (Alignment or Phasor Gateway) processes the configuration data to prepare for receipt of the specific PMUs data stream. Once the client has processed the PMU configuration data, it is now ready to receive the specific PMU's data stream. This ends the Use Case for the offline access scenario.

Use Case 8: Operator Sends Command Affecting Data Stream to Alignment (or Phasor Gateway)

Use Case Description: Data transmission from a PMU can be categorized in one of two modes of operation: commanded or spontaneous. This use case covers the commanded mode in which the PMU data stream is stopped or started from a remote client. This use case only covers PMUs within the same organization as the Operator.

Preconditions:

- The PMU has been installed, tested, and has all of the necessary network connections available.
- The client (Alignment or Phasor Gateway) has received and processed the PMU's configuration information.

Minimal Guarantees:

- The PMU does not start or intentionally stop its data stream unless a command is received from a client.

Success Guarantees:

- The PMU processes the command from the client (Alignment or Phasor gateway) and starts or stops the data stream as requested.

Trigger:

This use case is triggered by an operator initiating a request for a PMU to either start or stop its data stream.

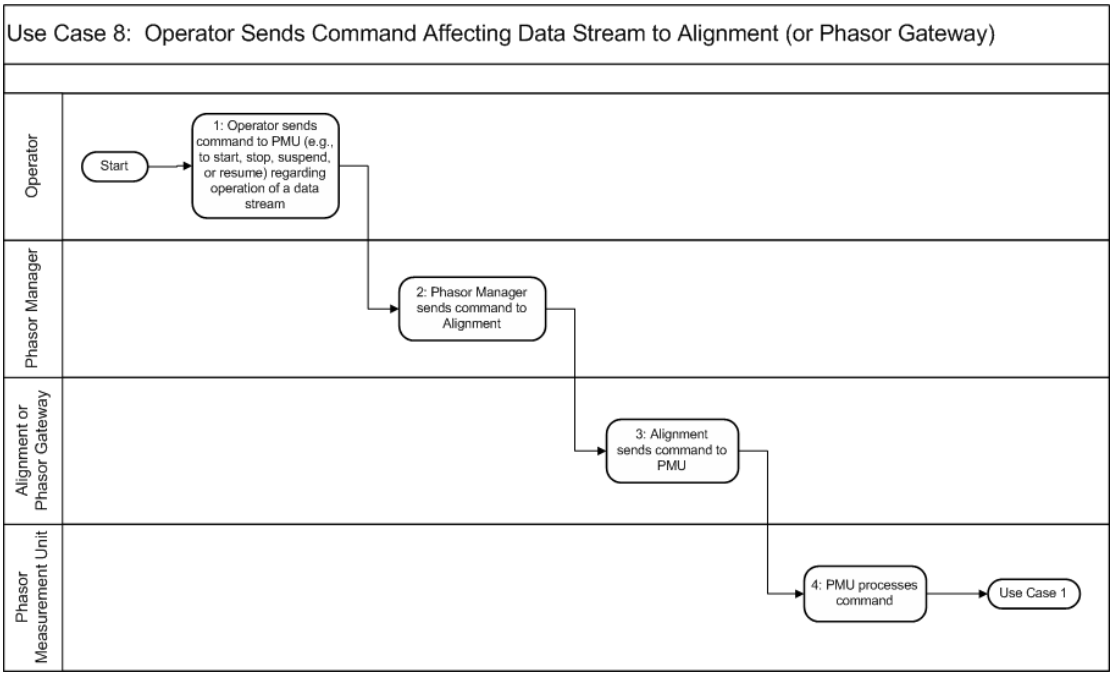

Diagram: Use Case 8: Operator Sends Command Affecting Data Stream to Alignment (or Phasor Gateway)

Main Success Scenario:

1: An Operator initiates a request via an interface to the Phasor Manager to send a command (e.g., start, stop, suspend, or resume a data stream) to a PMU.

2: The Phasor Manager receives the request from the Operator and forwards it to the appropriate client (Alignment or Phasor Gateway).

3: The client (Alignment or Phasor Gateway) receives the request and sends the corresponding command to the PMU.

4: The PMU processes the command. If the command was to start or resume the data stream, this use case then triggers Use Case 1 in which the PMU generates new data.

Use Case 9: Operator Advertises Initial Availability of Data from Local PMU via Registry

Use Case Description: In order for PMU data to be available to remote Applications which access the data through a Phasor Gateway, the PMU and its available measurement points are registered with a PMU Registry. This registration includes the PMU's identity, environmental information relevant to the PMU (e.g., location), as well as specific characteristics of the data it produces (e.g., phase, frequency of data reporting, and equipment).

Preconditions:

- The PMU has been installed, tested, and has all of the necessary network connections available.

Minimal Guarantees:

- No incorrect information is stored in the Registry.
- No unintended modifications or deletions are made to information in the Registry.

Success Guarantees:

- The PMU is registered in the PMU Registry, including all relevant data another organization needs to evaluate whether they are interested in the PMU's data and all identifier information required for another organization to request establishment of a data stream.
- The Registry provides the Phasor Manager with a GUID for the PMU, which the Phasor Manager retains for later reference.
- The Registry notifies other organizations of the availability of new PMU data.

Trigger:

There are two possible triggers for this use case.

- The organization decides to make a PMU's data available to other organizations for the first time.
- The organization had previously registered a PMU in the Registry, subsequently unregistered the PMU, and now it is to be re-registered. The prior credentials are no longer valid and so a new registration must be made.

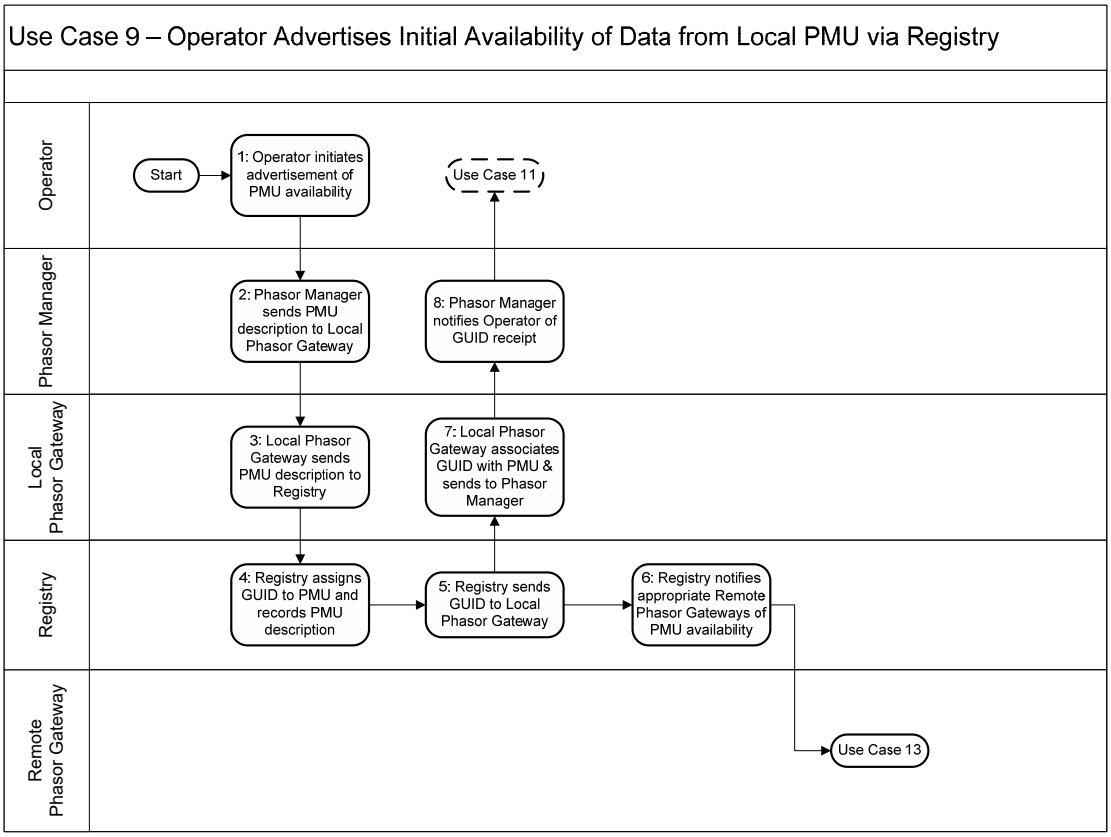

Diagram: Use Case 9: Operator Advertises Initial Availability of Data from Local PMU via Registry

Main Success Scenario:

1: The PMU's operating organization decides to register the PMU based on criteria outside of the scope of this use case. The actual registration is initiated by an Operator within the operating organization through a Phasor Manager.

2: The Phasor Manager receives the request from the Operator to register the PMU with the Registry. The Phasor Manager retrieves the PMU description and sends that information to the Phasor Gateway with a request to register the PMU.

3: The Phasor Gateway, in turn, sends the PMU description to the Registry.

4: The Registry assigns a globally unique identifier (GUID) to the PMU. The GUID is guaranteed to be unique across all PMUs whether currently registered or not. The Registry records the PMU description along with the assigned GUID.

5: The Registry passes the GUID associated with the PMU back to the Phasor Gateway.

6. The Registry also notifies the appropriate Remote Phasor Gateways of PMU availability. This triggers Use Case 13, in which the Remote Phasor Gateway makes an Operator within its organization aware of the PMU's availability.

7: The Phasor Gateway sends the GUID and its association with the PMU back to the Phasor Manager. The Phasor Manager stores this information for later reference.

8. The Phasor Manager notifies the operator of successful registration and the receipt of the GUID. Optionally, this may trigger Use case 13, in which an Operator could look up the PMU's information on the Registry to ensure it was recorded correctly.

Use Case 10: Operator Modifies Registry Information for a PMU

Use Case Description: Some of the relevant metadata (e.g., identity, environmental information, or measurement characteristics) for a previously-registered PMU has changed. This change is reported to the Registry.

Preconditions:

- The PMU has been installed, tested, has all of the necessary network connections available, and has already been registered with the Registry.

Minimal Guarantees:

- No unintended modifications or deletions are made to information in the Registry.

Success Guarantees:

- The PMU is registered in the PMU Registry, with all (and only) relevant data updated.

Trigger:

Information that was previously stored in the PMU Registry has changed for a PMU.

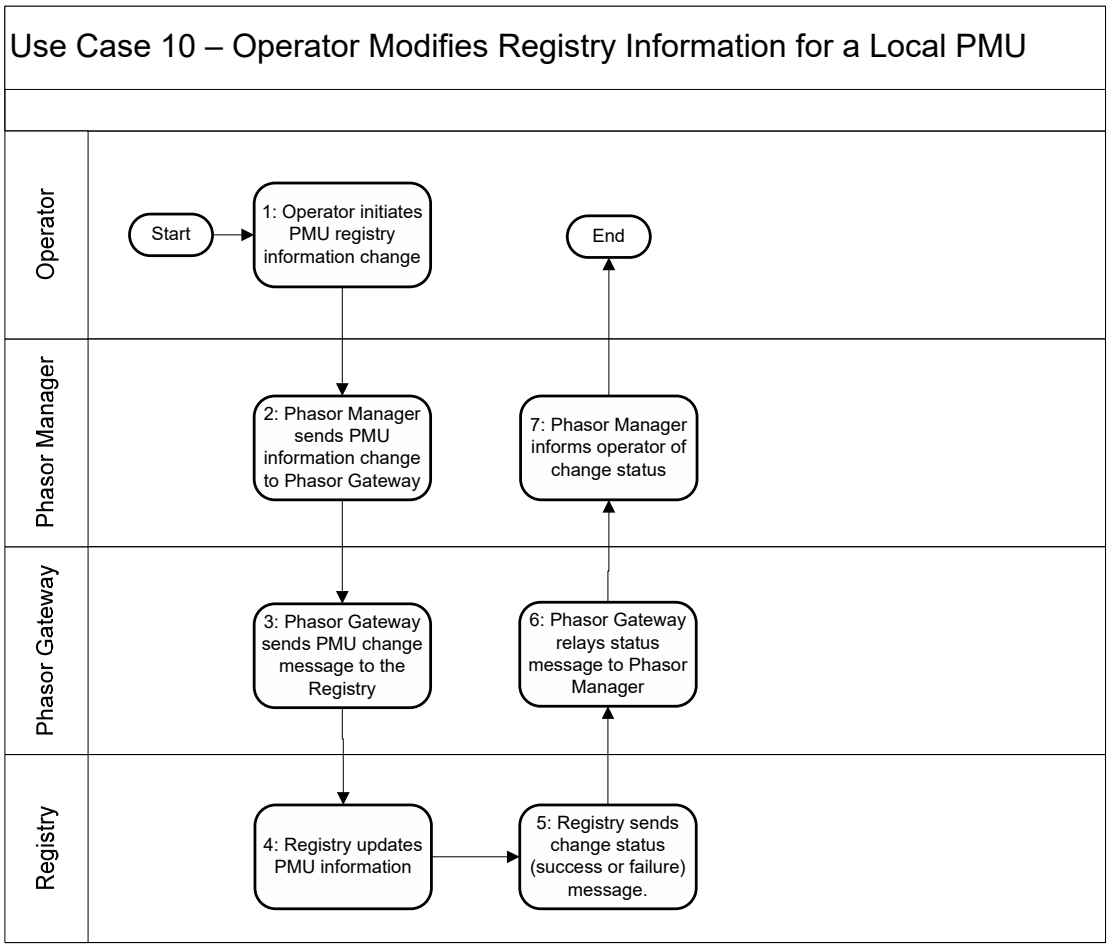

Diagram: Use Case 10: Operator Modifies Registry Information for a PMU

Main Success Scenario:

1: Some of the relevant metadata (e.g., identity, environmental information, or measurement characteristics) for a previously-registered PMU has changed. An Operator within the operating organization initiates a modification of the registered data through the Phasor Manager.

2: The Phasor Manager receives the request from the Operator to modify the registered data for the PMU. The Phasor Manager forwards the new information about the PMU information to the Phasor Gateway with a request to modify the PMU's registration.

3: The Phasor Gateway, in turn, sends the request and modified information to the Registry.

4: The Registry updates the specified PMU information.

5: The Registry sends the result of the update operation (success or failure) back to the Phasor Gateway.

6: The Phasor Gateway relays this information to the Phasor Manager.

7: The Phasor Manager notifies the Operator of the results of the modification.

Use Case 11: Operator Searches for PMU in Registry

Use Case Description: An Operator wishes to determine whether a remote PMU that meets desired criteria has been registered with the Registry and is accessible to the operator's organization. The Operator searches the Registry for the corresponding PMU parameters, and subsequently evaluates whether a found PMU can meet the organization's needs. If a match is found, the organization would request access to the PMU's data stream from the PMU's operating organization. This access request takes place through other channels and is outside the scope of this profile.

Preconditions:

- The Operator knows the desired characteristics of the remote PMU.

Minimal Guarantees:

- The Operator is not falsely informed of a PMU's availability.
- The Operator does not receive information about PMU's for which they are not supposed to have access.

Success Guarantees:

- The Operator receives sufficient information to determine if a remote PMU is available that meets the organization's needs.

Trigger:

The Operator wishes to determine the availability of a remote PMU that meets desired criteria.

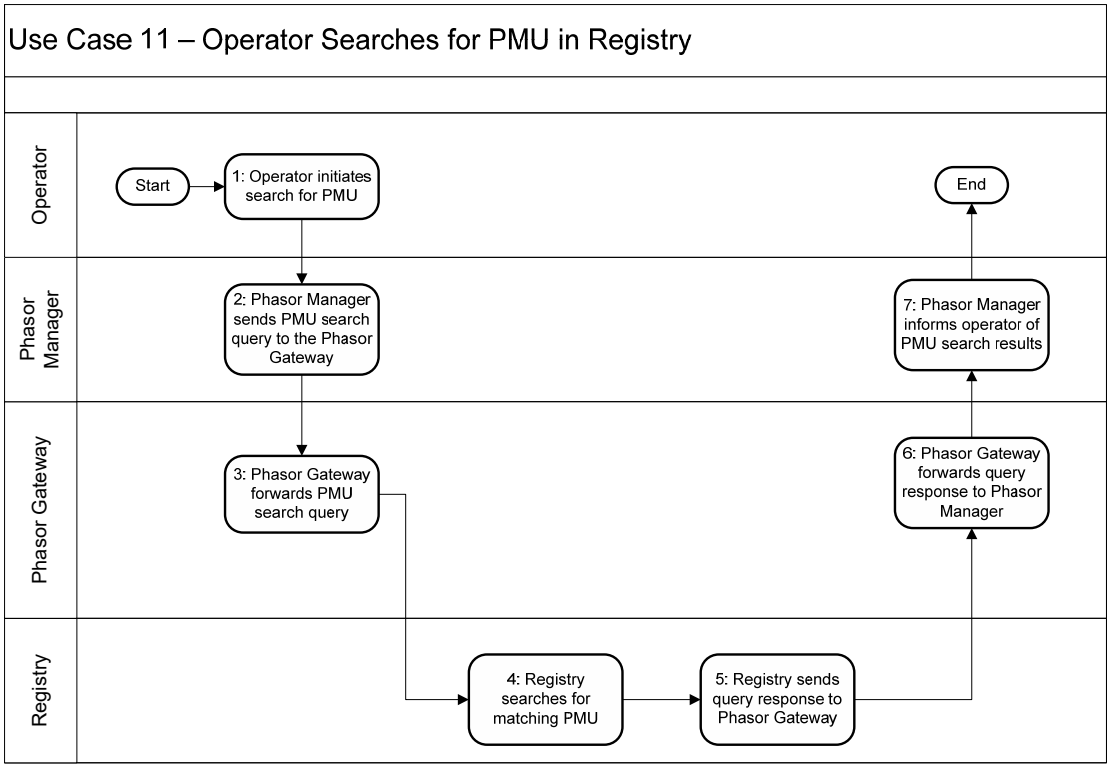

Diagram: Use Case 11: Operator Searches for PMU in Registry

Main Success Scenario:

1: An Operator configures a query regarding the availability of a remote PMU that meets desired criteria using the Phasor Manager.

2: The Phasor Manager forwards the query to the Phasor Gateway.

3: The Phasor Gateway, in turn, sends the request to the Registry.

4: The Registry evaluates the query against the list of registered PMUs available to the requesting organization.

5: The Registry sends the result of the query back to the requesting Phasor Gateway.

6: The Phasor Gateway relays this information back to the Phasor Manager.

7: The Phasor Manager communicates query results back to the Operator.

Use Case 12: Operator Advertises Initial Availability of Data from Local PMU via Point-to-Point

Use Case Description: In order for local PMU data to be available to remote Applications that access the data through a Phasor Gateway, the Operator provides metadata about the PMU and its available measurement points to the remote organization. This metadata includes the PMU's identity, environmental information relevant to the PMU (e.g., location), as well as specific characteristics of the data it produces (e.g., phase, frequency of data reporting, equipment, etc.). This use case differs from Use Case 9 in that a Registry is not used.

Preconditions:

- The PMU has been installed, tested, and has all of the necessary network connections available.
- Network connections necessary to send and receive configuration data between Phasor Gateways are available and operating correctly.
- The organization has decided to make phasor data from the PMU available to another (remote) organization.

Minimal Guarantees:

- No incorrect PMU metadata is provided to the remote organization.
- No PMU metadata for other PMUs is provided to the remote organization.

Success Guarantees:

- The remote organization receives correct metadata about the local PMU.

Trigger:

The operating organization decides to share data from a local PMU with another organization.

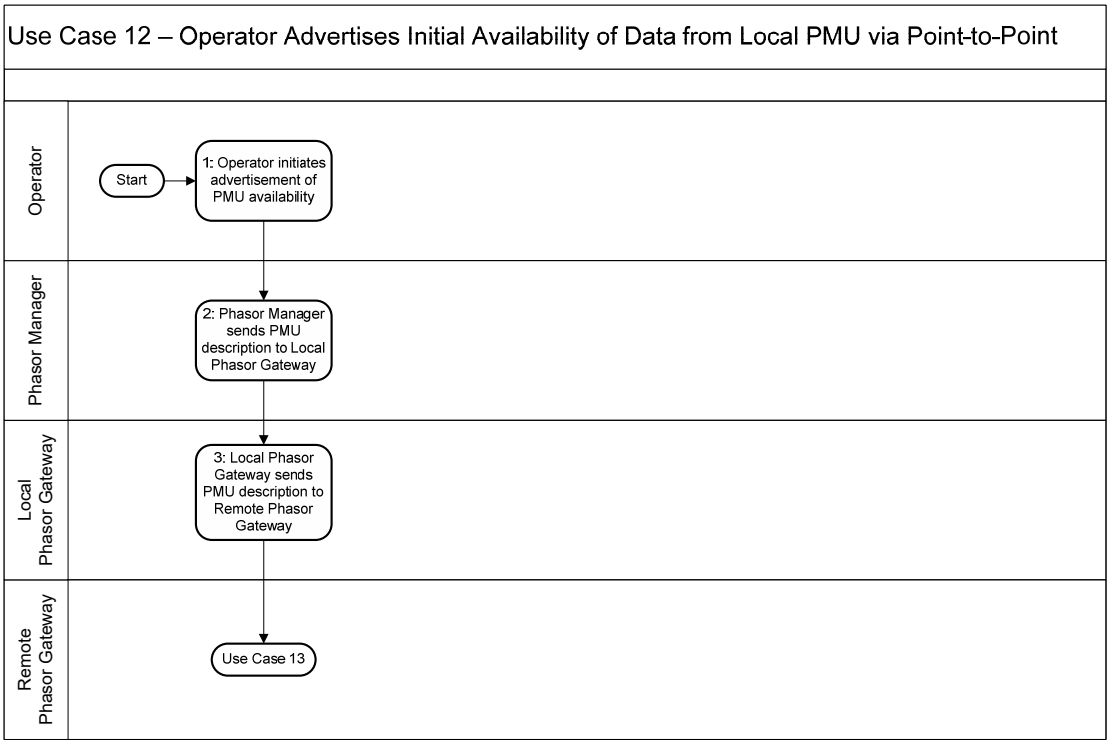

Diagram: Use Case 12: Operator Advertises Initial Availability of Data from Local PMU via Point-to-Point

Main Success Scenario:

1: The data from a local PMU is to be shared with a remote organization. The decision to share the data generated by the PMU is made by the operating organization based on criteria outside of the scope of this use case. The advertisement of this information is initiated by an Operator within the operating organization selecting the data to be shared in the Phasor Manager.

2: The Phasor Manager receives the request from the Operator to send the PMU's information to a remote organization. The Phasor Manager retrieves the addressing/connection information for the remote organization's Phasor Gateway, and sends the PMU information to the Local Phasor Gateway with a request to forward the information to the Remote Phasor Gateway.

3: The Local Phasor Gateway, in turn, sends the PMU information to the Remote Phasor Gateway. This triggers Use Case 13, in which the remote organization's Phasor Gateway processes information about the PMU.

Use Case 13: Operator Receives Notification of Availability of a Remote PMU (Push)

Use Case Description: An Operator receives notification that data from a remote PMU is accessible to the Operator's organization.

Preconditions:

- The organization operating the remote PMU has agreed to make data from the remote PMU available to the local organization.
- The Remote Phasor Gateway knows the connection/addressing information for the Local Phasor Gateway.

Minimal Guarantees:

- The Operator receives no false information regarding a remote PMU.

Success Guarantees:

- The operator is informed that data from the remote PMU is available.

Trigger:

A Remote Phasor Gateway (from another organization) sends notification of the availability of data from a specific remote PMU to the Local Phasor Gateway.

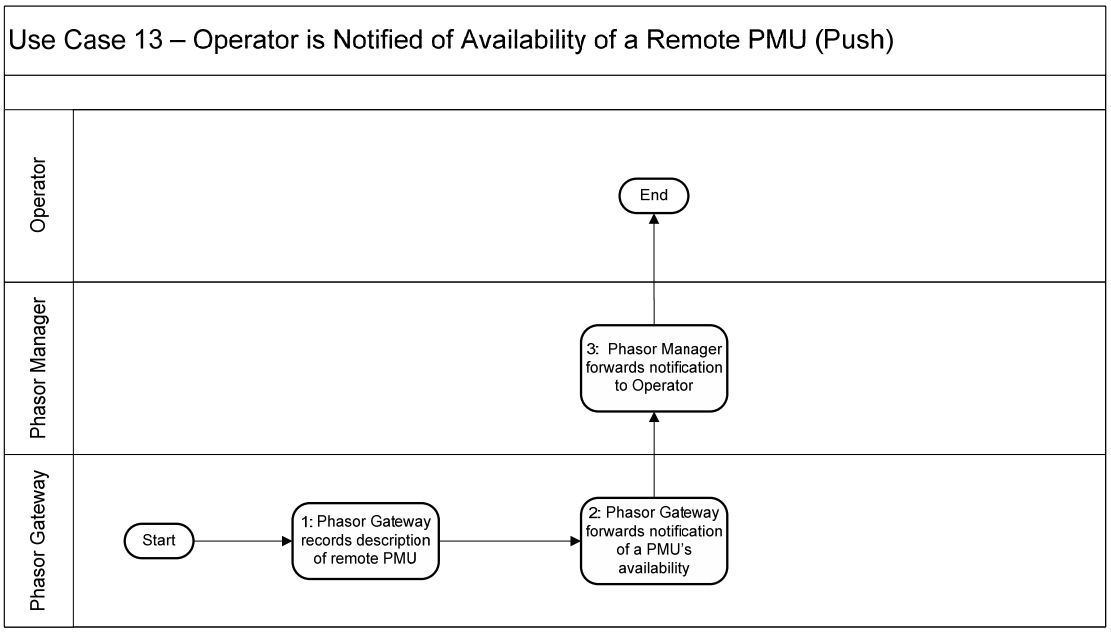

Diagram: Use Case 13: Operator is Notified of Availability of a Remote PMU (Push)

Main Success Scenario:

1: The (local) Phasor Gateway receives indication of the availability of a remote PMU from a Remote Phasor Gateway.

2. The Phasor Gateway forwards the notification of the remote PMU's availability to the Phasor Manager.

3. The Phasor Manager informs the Operator of the availability of data from a remote PMU.

Use Case 14: Operator Initiates a Data Stream to a Remote Organization

Use Case Description: This use case describes how the Operator of a local PMU creates a data stream from that PMU to a remote organization.

Preconditions:

- Network connections necessary to send and receive configuration data between Phasor Gateways are available and operating correctly.
- The receiving organization has configured its Phasor Gateway to accept and process data originating from the PMU in question.

Minimal Guarantees:

- Data from the local PMU does not go to any unintended recipients.

Success Guarantees:

- All intermediate systems responsible for streaming data from the local PMU to the remote organization are ready to manage data originating from the local PMU.

Trigger:

- The receiving organization requests, via a phone call or other mechanism outside the scope of the use case, data from organization that owns the PMU in question.
- The organization owning the PMU offers to provide its data to the recipient and the recipient agrees.

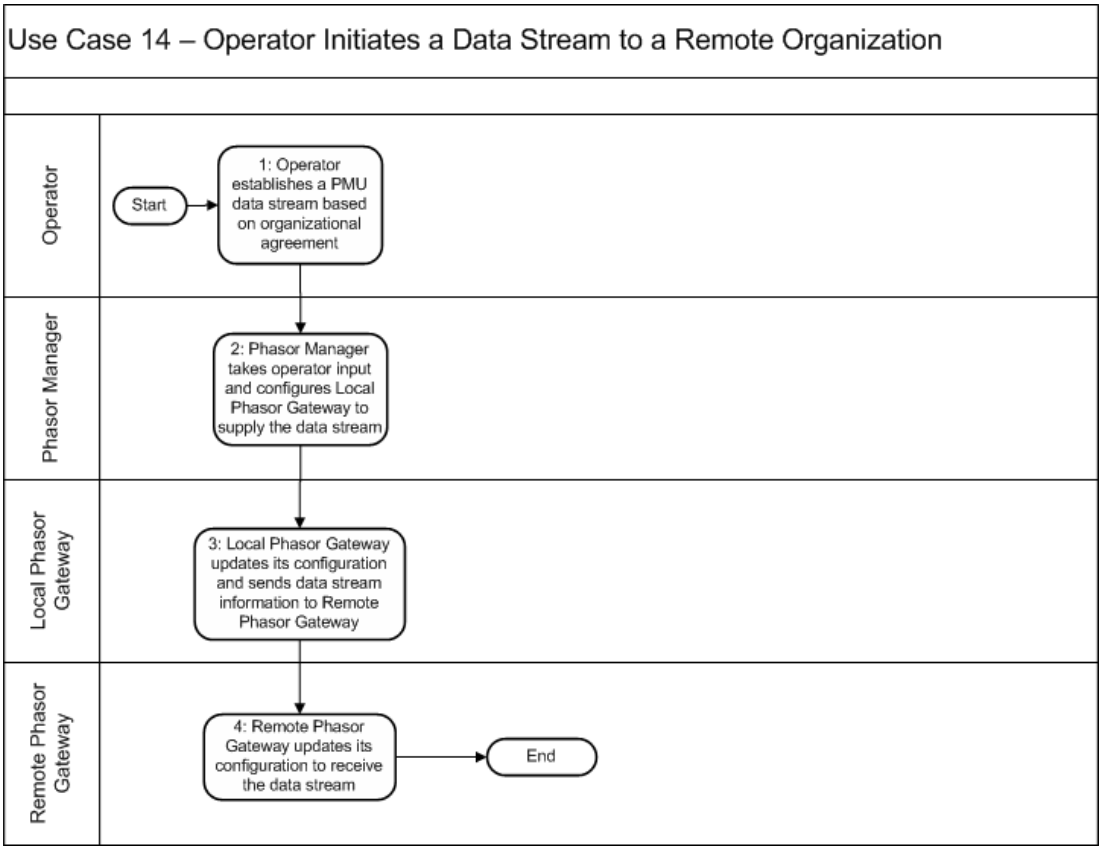

Diagram: Use Case 14: Operator Initiates a Data Stream to a Remote Organization

Main Success Scenario:

1: An Operator in the organization that operates the local PMU instructs the Phasor Manager to export data generated by the PMU to the remote organization.

2: The Phasor Manager assembles configuration data and any relevant metadata concerning the PMU in question. This information and the operator's request to export that PMU's data are sent by the Phasor Manager to the Local Phasor Gateway.

3: The Local Phasor Gateway configures itself to forward data from the PMU to the remote organization. The Local Phasor Gateway then sends relevant information about itself and the PMU to the Remote Phasor Gateway. The Local Phasor Gateway is now prepared to forward the PMU's data to the Remote Phasor Gateway.

4: The Remote Phasor Gateway receives information about the PMU and Local Phasor Gateway, and uses this information to configure itself to receive data from the PMU that is forwarded to it by the Local Phasor Gateway. The Remote Phasor Gateway is now prepared to receive and process the PMU's data from the Local Phasor Gateway.

Use Case 15: Operator Terminates a Data Stream to Remote Organization(s)

Use Case Description: This use case describes how the operator of a local PMU stops a data stream from that PMU to a remote organization.

Preconditions:

- The Remote Phasor Gateway is aware of the local PMU data stream.
- Network connections necessary to send and receive configuration data between Phasor Gateways (and the Registry, if involved) are available and operating correctly.
- The local PMU is registered in the PMU Registry (if Registry is involved).

Minimal Guarantees:

- The Local Phasor Gateway no longer forwards information from the local PMU.

Success Guarantees:

- The Remote Phasor Gateway no longer accepts information from the local PMU.
- The Registry (if involved) no longer retains an active record of the local PMU.

Trigger:

- The remote organization requests, via a phone call or other mechanism outside the scope of the use case, that the owner of the local PMU terminate the relevant data stream.
- The organization owning the local PMU decides to terminate the data stream for any reason.

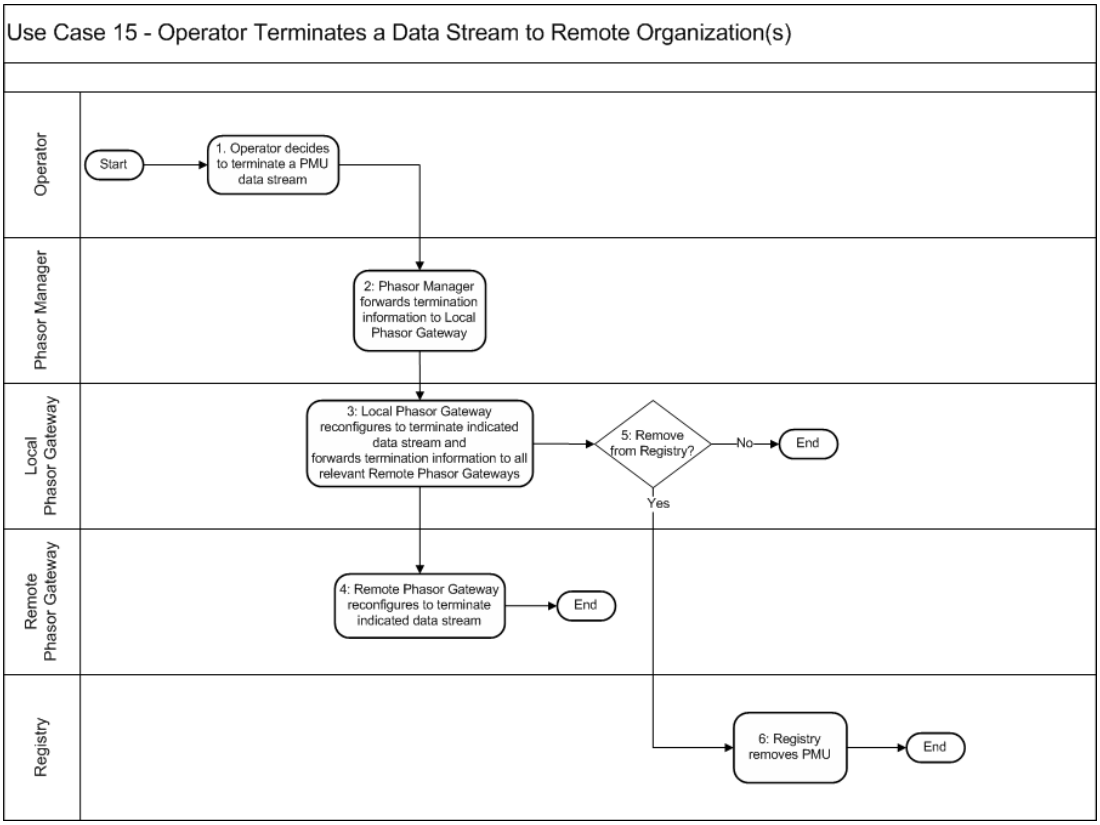

Diagram: Use Case 15: Operator Terminates a Data Stream to Remote Organization(s)

Main Success Scenario:

1: An operator in the organization that owns the local PMU instructs the Phasor Manager to stop exporting data generated by a PMU to one or more remote organizations.

2: The Phasor Manager extracts from its PMU configuration data any relevant information concerning the PMU in question. This information and the operator's request to stop exporting that PMU's data are sent by the Phasor Manager to the Local Phasor Gateway.

3: The Local Phasor Gateway configures itself to stop forwarding data from the PMU to each selected external organization. The Local Phasor Gateway sends relevant information about itself and the PMU to the appropriate Remote Phasor Gateway(s) and, possibly, the Registry.

4: Each remote Phasor Gateway receives information about the PMU and Local Phasor Gateway, and uses this information to configure itself to stop accepting data from the PMU that is forwarded to it by the Local Phasor Gateway.

5: The Local Phasor Gateway determines whether a Registry has a record of the PMU and if so, whether the PMU's record should be removed from the Registry.

6: If instructed to remove its record of the PMU, the Registry does so.

Use Case 16: Operator Terminates a Data Stream from a Remote Organization

Use Case Description: In this use case, an operator ends a subscription to a PMU that is operated by a remote organization. This ends the reception of data from the PMU to all Applications, etc. within the local organization.

Preconditions:

- The Remote Phasor Gateway is publishing data to the receiving organization.
- Network connections necessary to send and receive configuration data between Phasor Gateways are available and operating correctly.

Minimal Guarantees:

- The Local Phasor Gateway no longer accepts information from the PMU.

Success Guarantees:

- The Remote Phasor Gateway no longer forwards information from the PMU.

Trigger:

- The organization subscribed to the data decides that it no longer wants to receive it.

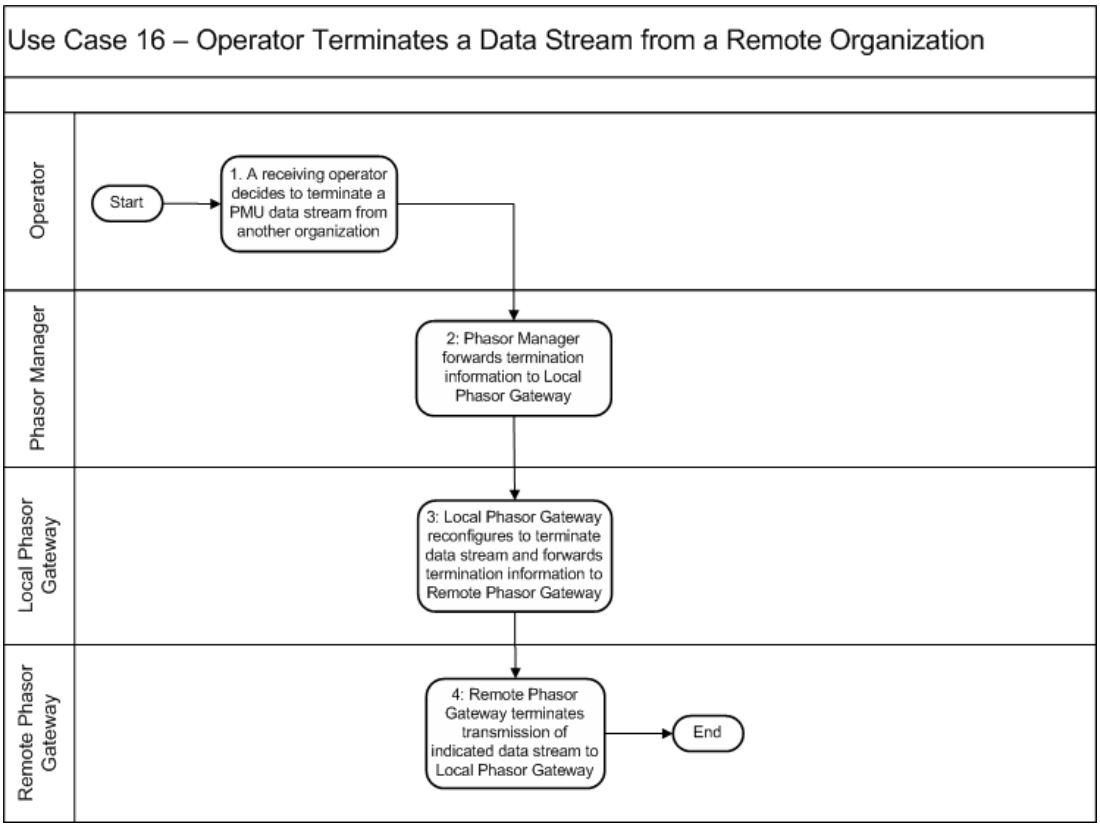

Diagram: Use Case 16: Operator Terminates a Data Stream to a Remote Organization

Main Success Scenario:

1: An Operator in the organization subscribed to the PMU data stream instructs its Phasor Manager to stop importing data generated by this PMU from the external organization.

2: The Phasor Manager extracts from its PMU configuration data any relevant information concerning the PMU in question. This information and the operator's request to stop importing that PMU's data are sent by the Phasor Manager to the Local Phasor Gateway.

3: The Local Phasor Gateway configures itself to stop importing data relating to the PMU in question. The Local Phasor Gateway sends relevant information about itself and the PMU to the Remote Phasor Gateway with a request for the Remote Phasor Gateway to stop forwarding data generated by the PMU.

4: The Remote Phasor Gateway receives information about the PMU and Local Phasor Gateway, and it uses this information to configure itself to stop forwarding data from the PMU to the Local Phasor Gateway.

3 Failure Analysis

The underlying approach used to create this security profile began with defining the functions of the WAMPAC system through abstract roles and use cases. The development of the use cases and the definition of roles took 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 of the process for identifying failures in Section 3.1 below. A brief overview of the foundational security and operational objectives is presented in Section 3.2 and a more detailed view of the identified failures is presented in Section 3.3.

3.1 Failure Analysis Process

The failure identification and analysis process is loosely based on conducting a Failure Modes and Effects Analysis (FMEA) on the WAMPAC logical architecture presented in Section 2, however the analysis was performed with a security bias to failure identification. A FMEA is a qualitative procedure for analyzing potential system failures and their associated modes as a function of assemblies, subassemblies, components, subcomponents, and so forth. This process leads to a quantification of the number and severity of failures and to an understanding of their impact on system stability and operations. With this information, a cost-benefits analysis can then be conducted to eliminate those risks that are considered catastrophic and accept those risks that are considered acceptable/manageable during operations. In general, the protocol for conducting a FMEA includes:

1. Establish a comprehensive 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 responsibilities.

3. At an appropriate level of abstraction, identify all failures, effects, consequences, and initiating events associated with each role.
4. Identify and analyze controls for each failure, its effects and consequences, or both.
5. Qualitatively assign a risk for each failure pairing 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 the WAMPAC security profile, the failure analysis process centers on steps 1-4. Steps 5-6 must account for 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.

This document begins the FMEA procedure by developing a WAMPAC architectural model that identifies the primary relationships and data flows among the elements of a WAMPAC system.

Given the system elements and their roles (Section 2.2) and relationships (Section 0), the set of role/failure pairings are applied to a finite set of use cases (Section 2.4) to provide a descriptive analysis of how the WAMPAC system may fail. The resulting list of failures serves as a basis for (1) justifying the set of selected controls, as each control must address an identified failure, and (2) identifying and remediating gaps in the selected controls, as each failure must be addressed by at least one control.

For this security profile, failure analysis centers on the roles and use cases defined in Sections 2.2 and 2.4 and the impact of potential failures on a WAMPAC system. This process is used to identify WAMPAC system issues, which are in turn used as inputs to assign failure incidents for the pairing of each role with each step of each use case. Each step of each use case is examined for potential failures against the security and operational objectives with respect to each role. All of the identified failures are then aggregated and generalized across all use cases.

3.2 Security and Operational Objectives

The goal of this document is to establish a cyber environment in which a WAMPAC 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 WAMPAC systems will be deployed:

1. Available bandwidth and connection quality vary greatly throughout the heterogeneous networks where PMUs will be deployed.
2. Computing resources will vary greatly from one installation to another.

3. Regulation and legal agreements require a separation between electric system operations and market functions (i.e., sale of bulk electricity).
4. Historical synchrophasor data is valuable for system event forensics, and therefore may have legal and financial implications with respect to liability or regulatory fines and penalties.
5. Real-time synchrophasor data can help facilitate market manipulation if available to a bad actor for misuse. Specifically, a bad actor could observe transmission system constraints and manipulate spot-market prices to take unfair advantage of limited power buying options.

3.2.2 Core Operational Assumptions

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

1. Grid Operators and Reliability Coordinators will use phasor data to make operational decisions. In some cases these will be automated decisions.
2. WAMPAC applications built on phasor data typically reside in close physical and logical proximity to central systems essential to the operation and control of the grid.
    a. Physical connection: Applications using phasor data are often deployed in central utility networks that also host operation and control functions
    b. Logical connection: Applications using phasor data may interact with central utility operation and control functions
3. Different applications will have different needs for phasor data. These differing needs include latency, availability, sample rate, time coordination, retention, etc.
    a. Class A Application: Phasor data used in automated, high-speed protection and control functions
    b. Class B Application: Phasor data used as input to real-time system analysis and in manual operational decisions (e.g., state estimator enhancement)
    c. Class C Application: Visualization of phasor data
    d. Class D Application: Use of phasor data in post-event analysis
    e. Class E Application: Research, development, and testing (NOTE: Class E applications are not covered in this profile)
4. Utilities typically deploy PMU's in field environments alongside or as parts of equipment used to control the grid.
5. Phasor data will be shared across organizational boundaries.
6. Once a phasor data stream has been established, there are no normal conditions that will prompt the curtailment of a stream.
7. All phasor data must go through alignment prior to use by applications.

3.2.3 Security Principles

Fourteen objectives for the WAMPAC system were identified and utilized throughout the profile development process. These objectives served as the "ground rules" for the WAMPAC systems and helped with use case development and failure identification. The 14 objectives are as follows:

1. Security controls should have minimal impact on, and in no way prevent, the primary mission of the WAMPAC system.
2. Security controls should minimize the impact of adverse events on the quality of service for WAMPAC communications and functions.
3. All WAMPAC systems and components should restrict logical and physical access to authenticated and authorized systems and personnel.
4. Only authenticated and authorized configuration changes (e.g., firmware, settings, etc.) should be processed by WAMPAC systems.
5. All configuration changes and access requests to WAMPAC systems should be auditable.
6. WAMPAC applications should validate the authenticity and integrity of all data acquired.
7. Asset owners should not rely exclusively on security measures outside their direct observation and control.
8. The introduction or integration of WAMPAC systems should not expose other utility systems to unauthorized access or attack (i.e., don't increase the attack surface).
9. Utility systems should be able to continue essential functions in the absence of PMU data.
10. Authorized operators should have the ability to disable automated protection and control associated with WAMPAC systems while maintaining monitoring functionality.
11. Essential WAMPAC functionality should not have single points of failure.
12. WAMPAC systems should protect synchrophasor and other system data from unauthorized disclosure.
13. WAMPAC systems should at all times be able to determine who has access to synchrophasor and other system data.

3.3 Failures

Failure analysis was performed by first analyzing each step of each use case against the security and operational objectives in Section 3.2.3. Failures that could result from security issues and that could lead to a violation of the objectives or interfere with the functional goal of the step were captured. After the initial failure identification step, the list of failures were grouped and generalized across the entire collection of use cases and their constituent roles.

Table 2 through Table 4 below define the generalized failures that apply across all of the roles. Each table includes a unique failure ID, a short definition of the failure, and a more elaborate

explanation. It should be noted that the failure ID number does not imply any kind of priority assignment. In each table, a <Role> can be one of the 12 essential roles (see Section 2.2) involved in WAMPAC systems, though a given failure may not be applicable to some roles. The failure analysis for this security profile resulted in the identification of 32 distinct failures.

3.3.1 Generic Failures

GF1-GF18 are generic failures that apply to all the roles with in the WAMPAC system or to a subset of the roles based on location (central or field).

Table 2 – WAMPAC Failures

Failure ID	Definition	Explanation	Examples
GF1	<Role> sends a message to an incorrect recipient	The role addresses a message to recipients that do not require the message, are incapable of processing the message, or both.	Transposing bytes in the recipients IP address Retrieving incorrect entries from a host lookup table
GF2	<Role> sends incorrect type of message	The role sends a message containing information other than what is required or expected by the recipient.	Sending a health and status report when a sensor data is required Returning an incorrect object type from remote procedure call.
GF3	<Role> sends corrupted or incorrectly formatted message	The role sends a message that is ill-formed by the sender and therefore cannot be processed by the recipient.	Using little-endian encoding when big-endian is expected Using wide characters when ASCII characters are expected.
GF4	<Role> sends a spurious message	The role transmits a message that is not required or expected by a legitimate recipient.	Broadcasting health and status information that should only be provided upon request Transmitting a flood of repeated or randomly varying messages.
GF5	<Role> sends an unauthorized message	The role transmits a message in spite of a prohibition against doing so or in violation of limits on the sender's use of network resources.	Sending sensor data when only configuration data is allowed to be transmitted

Failure ID	Definition	Explanation	Examples
GF6	<Role> does not send a message in a timely manner	The transmission of a message must occur within a particular span of time but the role fails to start the transmission within that span. This can cause a deadline for receipt of the message to be missed.	Writing the message to an invalid socket descriptor Missing a transmit deadline due to a task-scheduling failure
GF7	<Role> receives a message from an unauthorized/wrong source	The role accepts a message that comes from a source that is not authorized to send information to the role.	Role responds to a health and status request that arrives from an unknown source Role changes its operational settings on receiving a message from a public access computer (e.g., in a public library)
GF8	<Role> receives incorrect type of message	The role receives a message that is unexpected, incorrect, or containing inappropriate information, but processes that message regardless.	Processing an instruction to reconfigure when only requests for health and status are expected Responding to a request for status when in a state that disallows these messages.
GF9	<Role> receives corrupted or incorrectly formatted data	The role receives a message with an expected type from a legitimate source but that is ill formed. This can include data that has been manipulated in transit.	The role processes a message that fails its CRC check The role processes a command to change a control set point to some value that is outside of its valid range

Failure ID	Definition	Explanation	Examples
GF10	<Role> receives a spurious message	The role receives a message that is not expected and the processes the information in the message.	The role expects new data every minute, but upon receiving data every second processes the unexpected data The role extracts and processes a broadcasted command when no commands are expected on the broadcast channel Receiving a flood of unexpected data renders the role non-responsive to subsequent legitimate messages
GF11	<Role> does not receive a message in a timely manner	The transmission of a message must occur within a particular span of time, but the role fails to initiate reception of the message in that time.	A message is discarded due to insufficient space in the receive buffer Deadline for acting on the message is missed due to a task-scheduler failure
GF12	<Role> inappropriately rejects an authorized and valid message	The role fails to recognize the credentials of a device or individual, improperly marks the message as erroneous, or both, and thereby improperly disregards messages from that device or individual.	A corrupted password file prevents authorized users from accessing the role Software errors in the message validation software incorrectly classifies a well-formed message as invalid
GF13	<Role> fails to protect against unauthorized access and manipulation	The role allows a user or device to read or modify data without regard for their credential and access rights.	A file that should be read-only is marked as read-write Data that should be encrypted is stored as plain text
GF14	<Role> fails to protect data storage from being corrupted	The role fails to protect against data being modified or destroyed and the modification or destruction is not detected, is irreversible, or both.	Improper integrity checks in disk storage irreversibly corrupts data New data overwrites existing data without warning

Failure ID	Definition	Explanation	Examples
GF15	<Role> fails to prevent exhaustion of storage space	The role fails to provide sufficient resources for storing data and the exhaustion of storage goes unnoticed.	Disk space in a data store approaches storage limits without warning A user or process is granted access to storage space that exceeds a specified quota, without notification to administrators
GF16	<Role> fails to execute action in a timely fashion (resource starvation)	The role fails to execute a command within the required span of time due to insufficient resources or inappropriate use of resources.	Failure of the task-scheduler to execute the command as required Execution of the command is delayed due to software or hardware failures
GF17	<Role> accepts and applies corrupted configuration settings	The role applies new configuration settings regardless of their integrity or appropriateness in the context of the device's mission or operational state.	A secure shell server loads and processes a configuration file that contains unrecognized instructions A device silently uses default settings when provided with incorrect configuration data
GF18	<Role> is subverted to execute wrong action based on changes to its operational parameters, its data, or its internal state	The role is made to take action or inaction that is inappropriate to its mission or operation state. This can occur when software is corrupted prior to being placed into a particular device.	A sensor is instructed to raise its reporting threshold, but lowers it instead The role is instructed to delete a user's account, but instead resets the account password to a default value

3.3.2 Clock Failures

Clock1-Clock6 are clock-related failures within the WAMPAC system that affect the roles that contain and rely upon a clock.

Table 3 – Clock Failures

Failure ID	Definition	Explanation	Examples
Clock1	External source of time is unavailable to <role> for synchronization	Time originates from an external source such as GPS or NTP, but that source is not accessible or unavailable.	Loss of GPS signal due to improper antenna placement Unavailability of network time source due to communication mis-configuration
Clock2	External source of time is corrupted or spoofed providing wrong time to <role> for synchronization	Time is provided by an inappropriate source or the source is corrupted providing inaccurate time.	Sporadic jamming of GPS or other time signal Compromised time distribution resulting in wrong time propagated across devices
Clock3	<Role> has an internal source of time that is corrupted or unavailable	The role provides incorrect time to an application because of a failure or subversion of the internal mechanism for accessing the clock.	Software faults and/or subversive replacement of software Inaccurate local hardware causes excessive clock drift
Clock4	<Role> fails to obtain acceptable time quality	The role has access to a time source but its accuracy, precision, or both are not adequate to support the application.	Precision of the network time source is unacceptable for measuring phase angle deviation
Clock5	<Role> synchronizes to a wrong time source	The role that has access to more than one clock (e.g., GPS and NTP) selects the wrong one for the application requirements.	Selecting a stratum two time source when stratum one time source is required causing timing errors with application
Clock6	<Role> fails to provide power to the local clock	The role fails to provide backup power to the local clock causing the local clock to drift between synchronizations providing inaccurate time to the application.	Discharged battery in a field device resets the time value

3.3.3 Specific Failures

SF1-SF8 are failures associated with specific WAMPAC roles that are critical to the mission or operational state of the system.

Table 4 – Specific Failures

Failure ID	Definition	Explanation	Examples
SF1	<Role> contains sensors that are not calibrated correctly	The role contains sensor that has drifted out of calibration or has been mis-calibrated and fails to notify the application.	Current transformer is out of calibration due to inherent phase-shift
SF2	<Role> is physically tampered with or accessed by unauthorized personnel	The locks, protection force, or other mechanism for preventing physical access to a device or facility fails and allows access by unauthorized personnel.	
SF3	<Role> is maliciously modified in supply chain	Hardware vendor/manufacturer with malicious intent inserts hardware or software into device. The organization responsible fails to identify untrustworthy components in its supply chain.	
SF4	<Role> fails to identify and protect against unauthorized attempts to read or alter the contents of its memory (buffer)	The role fails to implement correct handling of memory management in a shared environment.	Shared memory space in devices implementing multiple roles provides access to data by unauthorized agents
SF6	<Role> fails to implement valid authentication mechanisms	The role fails to implement adequate trust verification mechanisms resulting in incorrect or absent verification of credentials.	Use of digital certificates from third-party requires system-wide trust verification mechanism for that particular third-party
SF7	<Role> contains supporting subsystems that are functioning improperly	The role contains or interacts with supporting subsystems that operate incorrectly or stops operating which impacts the mission or operational state.	

Failure ID	Definition	Explanation	Examples
SF8	<Role> fails to observe and identify the failure of supporting subsystems	The role contains or interacts with supporting subsystems that fail without being noticed. The health monitoring application fails to identify the improper operation of the supporting subsystems	

4 Security Controls

This section defines the set of recommended security controls for WAMPAC systems and components as that satisfy the functionality of the roles delineated earlier in this document. 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 synchrophasor technology and related systems. The controls presented herein may then, in turn, be satisfied by communications protocol definition-level standards and manufacturing specifications. This section first introduces a recommended network architecture, then defines the controls, and closes by allocating the controls to roles and network segments.

4.1 Network Segmentation

This document recommends the purposeful segregation of WAMPAC system resources into groups that serve similar functions. We recommend allocating these groups to dedicated network segments and placing security controls at network segment boundaries and within each segment according to the segment's function. In general, network segments are only connected to other segments as necessary to serve the function of the resources on each segment, and security controls are placed intentionally to facilitate layered and compartmentalized defenses against uncontrolled and potentially adversarial traffic. Figure 7 provides a high-level overview of the recommended network segmentation.

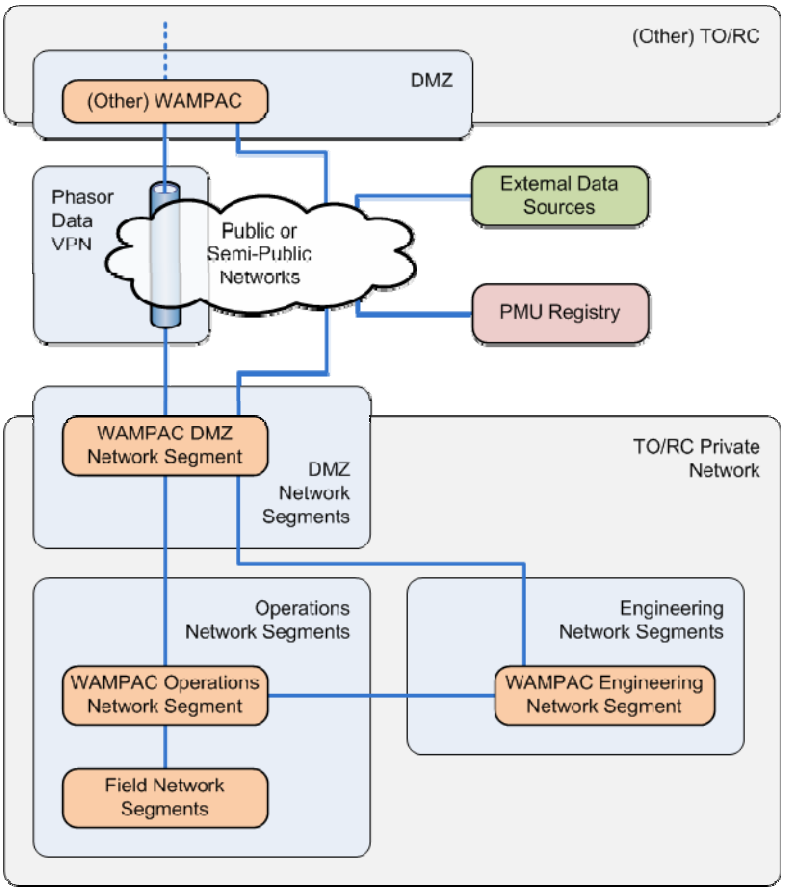

Figure 7 – Network Segmentation

We display the various types of networks and network segments in a hierarchy. The Transmission Owner /Reliability Coordinator (TO/RC) Private Networks are represented by the grey rounded rectangles. The TO/RC Private Networks are further broken into several network segments, namely Demilitarized Zones (DMZ), Operations, and Engineering Network Segments, represented by pale blue rounded rectangles. The WAMPAC portions of these segments are identified by orange rounded rectangles. This document prescribes some aspects of the WAMPAC portions of the indicated segments. The other groupings are intended to provide context for the WAMPAC portions, but are not further specified in this document.

Blue right-angles and straight lines indicate connections between network segments. The cloud indicates additional networks that may facilitate some WAMPAC communications, and the blue pipe is representative of a Virtual Private Network (VPN) that spans these networks. This diagram is broken down further in Figure 8 below, where the network segments are expanded to show allowable assignment of in-scope roles.

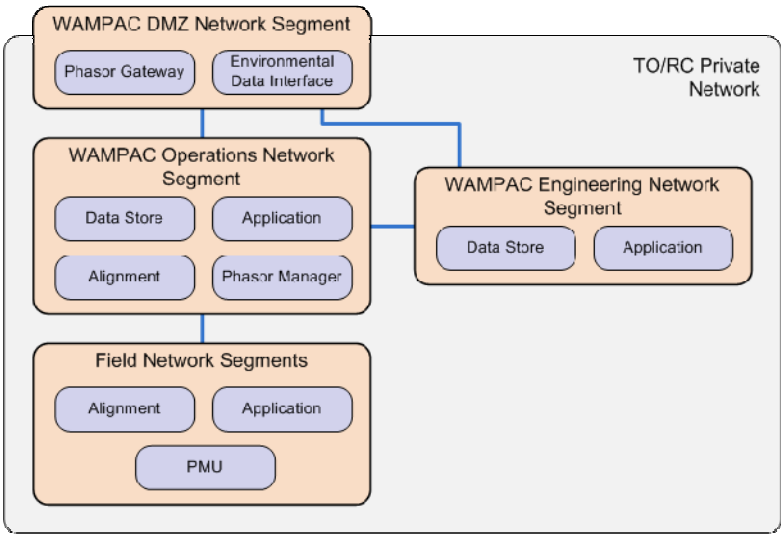

Figure 8 – Role Assignments to Network Segments

In this diagram, roles are displayed as purple rectangles within the network segments where they may be deployed. These allowable allocations are reiterated in the descriptions below as well as in the controls in Section 4.1.2.

4.1.1 Network Segment Descriptions

Table 5 describes the hierarchy of networks, network segments, allowed roles, and other relevant characteristics of the recommended network segmentation.

Table 5 – Network Segment Descriptions

Transmission Owner / Reliability Coordinator Private Network		
The Transmission Owner / Reliability Coordinator (TO/RC) Private Network is a collection of network segments owned and operated by either a transmission owner or reliability coordinator implementing functionality as defined by the WAMPAC Security Profile. The TO/RC may also own and operate other network segments not discussed herein. The segments included in this network are the WAMPAC DMZ, the WAMMPAC Operations Network Segment, the Field Networks Segments, and the WAMPAC Engineering Network Segment.		
Field Network Segment	Field Network Segment(s) contain all of the assets that monitor or directly interact with the electric power system, and includes field-deployed equipment physically residing outside of utility offices. Assets on the Field Network Segment may be deployed in a substation control house, in the substation yard, or outside the substation yard but connected to the electric systems (e.g., mounted on a tower or pole).	The roles that may reside in this segment are PMUs, Alignment, and Applications.
WAMPAC Operations Network Segment	The WAMPAC Operations Network Segment contains all of the servers that run centralized WAMPAC applications and real-time services that interact with other systems, and provides the only connection to assets deployed on the Field Network Segment. The WAMPAC Operations Network Segment may reside in the control center of a relevant entity, and is intended to support communications among the functions carried out in a control center setting.	The roles that may reside in this segment are Alignment, Application, Data Store, and Phasor Manager.

WAMPAC Engineering Network Segment	The WAMPAC Engineering Network Segments contain all of the engineering and analysis applications that are typically performed off-line and/or not in real-time. Manual interaction with servers or field assets outside of that involved in performing system operations shall be performed from workstations deployed on a WAMPAC Engineering Network Segment.	The roles that may reside in this segment are WAMPAC Application and WAMPAC Data Store.
WAMPAC Demilitarized Zone Network Segment	The WAMPAC DMZ Network Segment serves as the buffer between all other TO/RC owned and operated WAMPAC assets and all external systems. All traffic from any WAMPAC system headed outside the organization and all traffic from outside the organization destined for a WAMPAC system passes through the WAMPAC DMZ Network Segment.	The Phasor Gateway and Environmental Data Interface reside in the WAMPAC DMZ Network Segment.
PMU Registry	The PMU Registry may be deployed in a designated and sanctioned (e.g., by NERC) environment.	The PMU Registry resides on its own network segment external to the TO/RC organization.
External Data Sources	External Data Sources such as those used for weather, fire, earthquake, and traffic data reside on their own network segments, likely using an external network such as the Internet for communications.	No prescription is provided herein regarding External Data Source deployment.
Public or Semi-Public Networks		
Communications between the TO/RC WAMPAC system and the PMU Registry or External Data Sources may take place over public networks such as the Internet, or semi-public networks such as infrastructure provided by a third party. Negotiation of a Virtual Private Network between TO/RC WAMPAC systems may also take place over public or semi-public networks.		
Phasor Data Virtual Private Network		
Phasor data communicated between TO/RC organizations (i.e., passed from the Phasor Gateway of one organization to that of another) uses a Phasor Data Virtual Private Network (VPN) to traverse public or semi-public networks.		

4.1.2 "Public" vs. "Private" Networks

This document makes multiple references to both "public" and "private" networks. For the purposes of this profile, public networks contain devices using IP addresses that are reachable from any point in the Internet. For instance, a substation with a backhaul across a normal DSL link would be considered public if that DSL modem uses an IP address someone can ping from their home, even if the substation's DSL modem is using a firewall blocking external pings. Another example would be cellular technologies that are not deployed in a "private" mode, resulting in addresses that may be pinged from any location on the Internet. In the same vein, a dial-up modem with a phone number that someone can successfully dial from their home would also be considered a public network.

Within this document, networks that do not fall within the "public network" criteria defined above are considered to be private. Examples include:

- Devices using "private" IP addresses according to RFC 1918 and RFC 4193 (i.e., 10.x.x.x, 172.16-31.x.x, 192.168.x.x, and fc00::/7)
- Dial-up modems using phone numbers that can only be dialed within an organization, preferably only within the operations department's physical areas

- Cellular technologies in their private modes (which most cellular providers offer)
- Technologies such as T1/T3, ISDN, and MPLS that cannot be accessed from anywhere on the Internet (e.g., a coffee shop)
- RF technologies (regardless of spectrum) that a utility controls or pays a third party to control, which use private IP addresses (or no IP at all) and are restricted to the infrastructure that the utility deploys

The litmus test may be loosely interpreted as whether an attacker can communicate with any piece of the network from a remote geographic location with no privileged organizational connections (e.g., their home) through phone or Internet, regardless of any Access Control List (ACL) or firewall technologies deployed on the network. The primary motivation for using this criterion is to require layers of defense. A DSL modem in a substation that is directly attached to the public Internet would have a single layer of defense from attack – namely the software that is installed on it. One misconfiguration or vulnerability would allow an attacker some degree of access to the substation, or at least to all the traffic going through that DSL modem. In contrast to this, a MPLS router in a substation using private IP addresses cannot even be reached unless the attacker successfully compromises the utility or the network provider first.

4.2 Control Definitions

The process for defining the controls in this document is based on an analysis of the roles, use cases, and failures 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 includes the following steps (with natural iteration and review):

1. Examine the failures and associated controls from the Distribution Management Security Profile for similarities to the failures as defined in this document and for potential re-use of control material.
2. Re-write selected controls from the Distribution Management Security Profile to apply to WAMPAC systems. Verify, augment, or correct the mapping of each re-written control to the WAMPAC failures.
3. Examine the list of WAMPAC failures for complete coverage. Compose new controls as needed to ensure all WAMPAC failures are addressed.
4. Explicitly document the applicability of each control to roles or network segments. Tailor and/or split controls where necessary to accommodate implementation and environmental constraints for each role or network segment.
5. Map each WAMPAC control against the technical requirements in the NIST IR 7628. Assess coverage of technical requirements in the NIST IR 7628 by WAMPAC controls.
6. Modify WAMPAC controls to complete coverage of individual NIST IR 7628 requirements where appropriate. Document NIST IR 7628 requirements not completely covered along with reasoning.

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. 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 that apply to organizational policy. The controls herein are strictly focused on detailed recommendations for building and implementing synchrophasor systems and technology where guidance may not be found in other broadly accepted reference material.

The following tables define technical security controls that, if followed, will improve the security of a WAMPAC system. The elements of each control include:

- Control ID: This ID is composed of the control's category and a sequence number within that category.
- Short Name: This is a unique string that concisely references the intent of the control.
- Definition: This is the text that defines the control itself.

- Reference(s): These are the requirements from the NIST IR 7628 that are partially or fully satisfied by the control. Requirements listed in parenthesis are not required by the NIST IR 7628, but are included here for completeness.
- Failure(s): These are the failures from Section 3.3 addressed by the control.

4.2.1 Access Control

Table 6 – Controls: Access Control

Control ID	Short Name	Definition	Reference(s)	Failure(s)
Access Control.01	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) SG.AU-2	GF 5 GF 13
Access Control.02	Least Privilege	<Role> 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>.	SG.AC-6 SG.AC-7 SG.SC-19 SG.SC-29	GF 13
Access Control.03	Access Enforcement	<Role> shall enforce access control policies and associated privileges for users and devices based on identity, role, and attributes. The <role>shall be able to limit the services accessible by users and devices.	(SG.AC-4) SG.AC-6 SG.AC-7 SG.AC-15 SG.SC-19 SG.SC-29	GF 13
Access Control.04	Unsuccessful Access 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.	SG.AC-8	GF 6 GF 11 GF 16 GF 12
Access Control.05	Emergency Access	The system shall provide a means of audited, limited, manual override of automated access control mechanisms for use in the event of an emergency requiring immediate Operator intervention.	SG.AC-14 SG.AU-2	GF 8 GF 9

Control ID	Short Name	Definition	Reference(s)	Failure(s)
Access Control.06	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 WAMPAC system. (More than 1 concurrent session requires justification.)	SG.AC-11	GF 16 GF 17 GF 18
Access Control.07	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 appropriate identification and authentication procedures. 3. The existing information on the display shall be obfuscated during session lock.	SG.AC-12 SG.AC-13	GF 13
Access Control.08	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 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	GF 13
Access Control.09	Remote Access Restrictions	The system shall not allow remote configuration or management access to any system or device from beyond the TO/RC private network.	SG.AC-15 SG.SC-18	GF 5 GF 7
Access Control.10	Wireless Encryption	All wireless communications shall use a FIPS certified method of link-layer encryption (FIPS 140-2) in addition to any encryption already required by other controls.	SG.AC-15 SG.SC-8 SG.SC-12	GF 18
Access Control.11	Wireless Usage	The system shall not allow the use of a wireless interface on any device upon which the <role> is deployed. The wireless interface on the device shall be disabled or not installed. (This does not apply to wireless infrastructure used in backhaul transport. I.e., microwave radio for site-to-site communications.)	SG.AC-15 SG.AC-16	GF 1 GF 4 GF 10
Access Control.12	Password Management	<Role> 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 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 SG.SC-12	GF 13

4.2.2 Audit & Accountability

Table 7 – Controls: Audit & Accountability

Control ID	Short Name	Definition	Reference(s)	Failure(s)
Audit & Accountability.1	Inappropriate User Activity	The <role> shall monitor all user activity and report indications of inappropriate or unusual activity as defined by the organization.	SG.AU-2 (SG.AU-6)	GF 13 GF17 GF 18
Audit & Accountability.2	User Access Monitoring/Logging	The system shall monitor and log all user interactive sessions to <role> including all administrative and maintenance activities.	SG.AU-16 (SG.MA-6)	GF 13 GF 18
Audit & Accountability.3	Local and Central Logging	<Role> shall maintain a local log of all local authority actions at the highest level of detail available for the longest period of time that local storage space permits which shall be at least one week. <Role> shall forward all log entries to a dedicated logging server via its management server (like PMUs to Phasor Managers) or directly to the log server (like Phasor Managers themselves). Retain centrally stored logs for at least one year, with a minimum of three months immediately available for analysis.	SG.AU-2 SG.AU-4 SG.AU-16	GF13 GF17 GF18
Audit & Accountability.4	Electronic Log Format	The system shall make all physical access logs available in electronic form suitable for long term storage and retrieval.	SG.AU-4	SF 2
Audit & Accountability.5	Content of Audit Records	<Role> 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	GF12 GF13 GF17,GF18 SF6 SF7 SF8

4.2.3 Configuration Management

Table 8 – Controls: Configuration Management

Control ID	Short Name	Definition	Reference(s)	Failure(s)
Configuration Management.1	Systems Inventory	The system shall create and maintain (on at least a daily basis) an inventory of WAMPAC systems 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	GF 13 GF 18

Control ID	Short Name	Definition	Reference(s)	Failure(s)
Configuration Management.2	Current Configuration	A designated system or systems shall daily or on request obtain current version numbers, installation date, configuration settings, and patch level on <role>; validate the sender's cryptographic signature; and compare this information with recorded values in the inventory and configuration databases. All discrepancies shall be logged and alerts shall be generated where appropriate.	(SG.CM-6) SG.SI-2 SG.SI-7	GF 17 GF 18
Configuration Management.3	Disabling Unnecessary Functionality	The system shall ensure that only the minimum functionality required for the proper operation and maintenance of <role> is enabled. The full set of allowable functions and services shall be documented and verified at startup and periodically thereafter. All unnecessary functions (including email, instant messaging, and social networking software) shall be uninstalled, removed, or never installed. This includes workstations in the WAMPAC Engineering Network Segment(s) and WAMPAC Operations Network Segment(s). Utility employees whose primary workstations are in these Internet-restricted network segments should be provided secondary non-WAMPAC accessible systems for Internet and email access.	SG.CM-7	GF 1 GF 4 GF 10
Configuration Management.4	Disabling Unnecessary Communication Services	Upon startup, the system shall ensure that all networking and communication capabilities not required for the operation or maintenance of <role> are disabled. This includes VOIP, instant messaging, ftp, HTTP, file sharing. Vendor defaults for all wireless options shall be initially set "off". Any unused ports shall be disabled. Modems shall be disabled by default. Every modem port and LAN port shall be disabled by default.	SG.CM-7 SG.SC-17	GF 7 GF 10 GF 4
Configuration Management.5	Factory Default Credentials	The system shall force a change of all factory default access and authentication credentials on <role> upon installation.	(SG.CM-10)	GF 17 GF 18

4.2.4 Continuity of Operations

Table 9 – Controls: Continuity of Operations

Control ID	Short Name	Definition	Reference(s)	Failure(s)
Continuity of Operations.1	Alternate Control Center	<Role> involved in supporting class A or class B Applications shall be replicated at both primary and alternate control center facilities. Loss of either control center shall not impair communications from any field device to the other control center.	(SG.CP-9)	GF 13 GF 18
Continuity of Operations.2	WAN Communication Outage	WAMPAC field systems must be able to carry out all essential functionality without any connection beyond its local network. (For example, a field segment should be able to carry out normal functionality if communications to the WAMPAC Control Systems Server segment is lost.)	(SG.PE-12) SG.SC-5	SF 7
Continuity of Operations.3	Operations Continuity	The system shall provide a means to compensate for loss of a single component implementing <role> without loss of system functionality.	(SG.PE-12) SG.SC-5	SF 7

Control ID	Short Name	Definition	Reference(s)	Failure(s)
Continuity of Operations.4	Graceful Degradation	The system shall provide a means to continue operations with reduced system functionality in the event of complete loss of the <role> function.	NONE	GF 17 GF 18 GF 14
Continuity of Operations.5	System Restoration	The system shall have the ability to recover <role> from securely maintained backups, images, and configurations in the event of compromised device(s) or network (exception: hardware changes).	(SG.CP-10)	SF 7
Continuity of Operations.6	Alternative Time Source	The <role> shall support alternative time source for redundancy and consistency checking.	SG.SC-5	Clock 1 Clock 3

4.2.5 Identification & Authorization

Table 10 – Controls: Identification & Authorization

Control ID	Short Name	Definition	Reference(s)	Failure(s)
Identification & Authorization.01	Identifier Management	The system shall assign unique identifiers to each individual, connected system, and device.	(SG.IA-2)	GF 13 GF 18 GF 1 GF 5 GF 7
Identification & Authorization.02	Credential Management	The system shall provide a single point of initiation to distribute, manage, and revoke all logical and physical access credentials for all WAMPAC systems and components. Revocation shall be carried out on all systems within 24 hours.	(SG.IA-3)	GF 13 GF 18
Identification & Authorization.03	Digital Certificates	<Role> shall provide cryptographically strong authentication credentials such as digital certificates signed by the organization (to which the <Role> belongs) or other trusted party (i.e., a trusted identity provider or vendor). Certificate issuance and signing must conform to a secure process such as NIST SP 800-53: FPKI Security Controls for PKI Systems and NIST SP 800-53A: Assessment Guidance for Security Controls in PKI Systems. The proof of authenticity must be generated by an organizational process that supports independent review, and credentials must be independently verifiable by external (to the organization) audit.	SG.AC-15 SG.AU-16 SG.AU-2 SG.IA-4 SG.SC-15	SF 6
Identification & Authorization.04	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-15 SG.IA-4	GF 13 GF 18

Control ID	Short Name	Definition	Reference(s)	Failure(s)
Identification & Authorization.05	Device Identification and Authentication	<Role> shall employ a cryptographic-based bi-directional identification and authentication (e.g. Client-authenticated TLS) for command, configuration, and management communications.	SG.AC-15 SG.IA-5 SG.SC-7 SG.SC-20	GF 5 GF 7
Identification & Authorization.06	Cryptographic Module Authentication	<Role> shall employ cryptographic module authentication for authenticating users and devices. <Role> shall use Trusted Platform Modules (TPMs) or Hardware Security Modules (HSMs) for device and user identification and authentication.	SG.AC-15 (SG.IA-3) SG.SC-7	GF 13 GF 18 GF 5 GF 7
Identification & Authorization.07	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.IA-5	GF 5 GF 7
Identification & Authorization.08	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	GF 13 GF 18
Identification & Authorization.09	Self Identification	The <role> shall be able to report identifying and configuration information of the software and hardware on request, consistent with Access Controls identified in this document. This shall at a minimum include version number, installation date, configuration settings, and patch level. This information shall be cryptographically signed upon sending.	SG.SC-12 SG.SI-7	GF 17 GF 18
Identification & Authorization.10	Authenticated Link Establishment	<Role> shall provide limited communication functionality until an authenticated link to a centralized credential management system is established. Communications shall be limited to those functions required to establish an authenticated link.	NONE	GF12 GF13
Identification & Authorization.11	Authenticated Link Restoration	<Role> shall refuse local authority when an authenticated link to a centralized credential management system is established. If no such link is active, local authority may be granted to a predetermined account unique to the device with a one-time-use password. Upon logon, the password must be changed and a flag will be set indicating local authority has been established. The flag may not be cleared by anything other than a centralized credential management system.	NONE	GF12 GF13 GF18

4.2.6 Network

Table 11 – Controls: Network

Control ID	Short Name	Definition	Reference(s)	Failure(s)
Network.1	Field Network Allocation	All field-deployed WAMPAC equipment physically residing outside of utility offices that monitor or directly interact with the electric system shall reside on a Field Network Segment. Other field-deployed systems owned and operated by the same organization may also reside on the same Field Network Segment. No centralized services, engineering workstations, or systems owned or operated by another organization may reside on a Field Network Segment.	SG.SC-30	GF7 GF10 SF6
Network.2	Field Network Connection	Field Network Segments shall only be connected to Operations Network Segments owned and operated by the same organization.	SG.AC-15 SG.SC-7 SG.SC-30	GF7 GF10 SF6
Network.3	Operations Network Allocation	Centralized WAMPAC applications and services performing closed-loop, feed-forward, or other real-time automated functions shall reside on an Operations Network Segment. No field equipment, engineering workstations, or systems owned or operated by another organization may reside on an Operations Network Segment.	SG.SC-30	GF5 GF6 GF7 GF11 GF13 GF16 SF6
Network.4	Operations Network Connection	WAMPAC Operations Network Segments shall only be connected to Field Network Segments, Engineering Network Segments, and DMZ Network Segments owned and operated by the same organization. WAMPAC Operations Network Segments shall not be connected directly to enterprise or external networks.	SG.SC-7 SG.SC-30	GF5 GF6 GF7 GF11 GF13 GF16 SF6
Network.5	Engineering Network Allocation	WAMPAC engineering and analysis applications performing manual or off-line functions shall be deployed on Engineering Network Segments. No field equipment, centralized services, or systems owned or operated by another organization may reside on an Engineering Network Segment.	SG.SC-30	GF4 GF7 GF10 GF13 GF16

Control ID	Short Name	Definition	Reference(s)	Failure(s)
Network.6	Engineering Network Connection	WAMPAC Engineering Network Segments shall only be connected to Operations Network Segments and DMZ Network Segments owned and operated by the same organization. WAMPAC Engineering Network Segments shall not be connected directly to enterprise or external networks.	SG.SC-7 SG.SC-30	GF4 GF7 GF10 GF13 GF16
Network.7	DMZ Network Allocation	Centralized WAMPAC services retrieving data from or directly interacting with systems from other organizations shall reside in a DMZ Network Segment. No field equipment, engineering workstations, or systems owned or operated by another organization may reside on a DMZ Network Segment.	SG.SC-30	GF4 GF7 GF10 GF13 GF18
Network.8	DMZ Network Connection	WAMPAC DMZ Network Segments shall not connect directly to Field Network Segments.	SG.SC-7 SG.SC-30	GF4 GF7 GF10 GF13 GF18

4.2.7 Physical & Environmental

Table 12 – Controls: Physical & Environmental

Control ID	Short Name	Definition	Reference(s)	Failure(s)
Physical & Environmental.01	Physical Access Authentication	Supporting systems shall implement a minimum of two factor authentication for unescorted physical access to facilities containing <role>.	(SG.PE-2)	GF 13 GF 18
Physical & Environmental.02	Limited Access - Interactive Resources	Supporting systems shall limit physical access to <role> to only those personnel responsible for operating, maintaining, or managing the <role>.	(SG.PE-3)	GF 13 GF 17 GF 18
Physical & Environmental.03	Limited Access - Non-interactive Resources	Supporting systems shall limit physical access to <role> to only those personnel responsible for maintenance and management of the <role>. This can be accomplished by segregating these components within a room internal to a control center facility, the use of lockable enclosures or cabinets, or other similar mechanisms.	(SG.PE-3)	GF 13 GF 17 GF 18

Control ID	Short Name	Definition	Reference(s)	Failure(s)
Physical & Environmental.04	Limited Field Component Access	Supporting systems shall control physical access to <role> at all times. This can be accomplished by installation of the component within a substation control building or a lockable cabinet. The mechanism used for physical access shall provide unique credentials per user which shall be authorized on a per lock basis. Periodic re-authorization shall be required at least every 24 hours and shall automatically expire by default if not re-authorized. This precludes the use of a standard mechanical lock and key mechanism.	(SG.PE-3)	GF 13 GF 17 GF 18
Physical & Environmental.05	Tamper Resistant and Tamper Evident Field Components	For field components, supporting systems shall use tamper resistant and tamper evident capabilities to supplement Physical & Environment.4 physical access controls as another layer of defense-in-depth. This document recommends that the system send tamper alarms to the organization's incident response team for review and response. Evidence of tampering that is obvious upon visual inspection is also important to support forensic analysis.	(SG.PE-4)	GF 13 GF 17 GF 18
Physical & Environmental.06	Facility Access Monitoring/Logging	Supporting systems shall provide continuous monitoring and logging of all physical access to any six-walled physical facility (e.g., control center, data center, or substation control building) that houses <role>.	(SG.PE-4)	GF 13 GF 18
Physical & Environmental.07	Cabinet Access Monitoring/Logging	Supporting systems shall provide continuous monitoring and logging of all physical access to cabinets and/or enclosures containing WAMPAC system cyber components that are not housed in six-walled physical facilities. Mechanisms utilized to monitor entry to cabinets shall be capable of operating in the event of a local power outage.	(SG.PE-4)	GF 13 GF 18 SF 2
Physical & Environmental.08	Physical Access Indications	Supporting systems shall provide real-time visibility of all events relating to physical access to <role> to utility operations personnel (e.g. system operator).	(SG.PE-4)	GF 13 GF 18
Physical & Environmental.09	Power Sources and Cables	Supporting systems shall physically protect power sources and power cables for <role> from damage or unauthorized manipulation.	NONE	SF 2
Physical & Environmental.10	Power Source Monitoring/Logging	Supporting systems shall provide continuous monitoring of the state of the primary and alternate power sources for <role>, and shall log all interruptions of these power sources.	NONE	SF 2 Clock 6
Physical & Environmental.11	Emergency Power Shutoff	Supporting systems shall protect emergency power shutoff capability for facilities containing <role> such as control center and data center facilities from unauthorized activation by using physical access controls.	(SG.PE-8)	SF 2 Clock 6

Control ID	Short Name	Definition	Reference(s)	Failure(s)
Physical & Environmental.12	Alternate Power Source	The system shall provide a long-term alternate power supply located at primary and alternate control facilities capable of maintaining uninterrupted, minimally required operational capability for essential WAMPAC system cyber components in the event of an extended loss of the primary power source.	(SG.PE-9)	Clock 6
Physical & Environmental.13	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)	Clock 6
Physical & Environmental.14	Component Location	The physical location of <role> shall minimize potential damage from physical and environmental hazards and minimize the opportunity for unauthorized access.	(SG.PE-12)	SF 2
Physical & Environmental.15	Fire Detection	All facilities housing <role> shall implement fire detection devices/systems. These devices/systems shall activate automatically and notify the organization and emergency responders in the event of a fire. All activations of the system shall be logged.	NONE	SF 2
Physical & Environmental.16	EMI/Surge Protection	<Role> located within, on, or nearby high-voltage power equipment or facilities shall be resistant to EMI and heavy electrical surges that can be expected within an electrical substation or electrical distribution feeder circuit. Purchasing equipment that meets IEEE 1613 or IEC 61850-3 specifications will satisfy this requirement.	NONE	SF 2

4.2.8 System & Communication Protection

Table 13 – Controls: System & Communication Protection

Control ID	Short Name	Definition	Reference(s)	Failure(s)
System & Communication Protection.01	Management/Configuration Isolation	The management/configuration port or function for <role> shall be physically or logically (e.g., separate VLAN not routed to other networks) separated from non-management/configuration data. Management and configuration shall also use separate authentication credentials from the credentials used by <role>. No management segment shall cross any boundary defined in the Network controls. There shall be one management segment corresponding to each non-management segment.	SG.SC-2	GF 1 GF 4 GF 5 GF 7 GF 10

Control ID	Short Name	Definition	Reference(s)	Failure(s)
System & Communication Protection.02	Security Function Isolation	<Role> data and functionality shall be physically or logically (e.g., separate VLAN not routed to other networks) separated from security devices and functionality. Security devices and functionality can exist on management networks, however, the authentication for these devices and functionality will use separate multi-factor credentials.	SG.SC-3	GF 13 GF 17
System & Communication Protection.03	Secure Coding Practices	WAMPAC 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	SF 4
System & Communication Protection.04	Secure Communications Services	Upon startup insecure protocols such as FTP, HTTP, and Telnet shall be disabled or removed. Only secure replacements of these protocols such as SFTP, FTPS, SCP, HTTP over TLS, and SSH shall be used in production.	NONE	GF 5 GF 7
System & Communication Protection.05	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.	NONE	SF 7
System & Communication Protection.06	Quality of Service - Specification	<Role> shall use a QoS or other resource reservation control mechanism on all outgoing communications. Relative priority for traffic related to WAMPAC systems shall be from highest to lowest: 1) commands, 2) configuration and management, 3) PMU data streams, and 4) environmental data.[8]	SG.SC-6	GF 11
System & Communication Protection.07	Quality of Service - Enforcement	The network shall process all traffic in accordance with the QoS or other resource reservation control identifier.	SG.SC-6	GF 6 GF 11
System & Communication Protection.08	Resource Consumption	The <role> shall implement resource monitoring and control mechanisms for all devices/processes to identify and mitigate excessive resource consumption (e.g., runaway processes).	SG.SC-6	GF 16
System & Communication Protection.09	Resource Monitoring	The system shall provide operator visibility and appropriate alerting for <role> resources and activity, including available memory and disk space, CPU utilization, status of queues, and message transmit/receive rates.	NONE	GF 16

[8] Definitions for each category of communication may be found in Section 0.

Control ID	Short Name	Definition	Reference(s)	Failure(s)
System & Communication Protection.10	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.AC-15 SG.AU-16 SG.SC-7 SG.SC-8 SG.SC-12	GF 7 GF 9
System & Communication Protection.11	Communication Confidentiality	The <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.AC-15 SG.SC-7 SG.SC-9 SG.SC-12	GF 5 GF 7
System & Communication Protection.12	Traffic Control and Filtering	The system shall enforce the flow of information into, out of, and within the WAMPAC 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-15 SG.SC-5 SG.SC-7	GF 1 GF 4 GF 5 GF 7 GF 10
System & Communication Protection.13	No Internet Access	No internet access (including e-mail or software updates) shall be allowed from , even if through a proxy or through a firewall.	SG.SC-7	GF 4 GF 10
System & Communication Protection.14	Non-adjacent Network Restrictions	The system shall prohibit all direct communication between devices/systems in non-adjacent network segments.	SG.AC-15 SG.SC-7	GF 1 GF 4 GF 5 GF 7 GF 10
System & Communication Protection.15	Emergency Network Segmentation	If an attack is detected, the system shall label all traffic from compromised WAMPAC network segments as potentially malicious, and provide tools to isolate the compromised segment from network segments that are confirmed as trustworthy and defensible.	NONE	GF 1 GF 4 GF 5 GF 7 GF10
System & Communication Protection.16	Separate Keys for Separate Functions	Field <roles> will use separate encryption keys based on functionality for all messages that are encrypted. For example, the key used for encrypting PMU data will be different than the key used for firmware updates.	SG.SC-8 SG.SC-9	GF 7 GF 9

Control ID	Short Name	Definition	Reference(s)	Failure(s)
System & Communication Protection.17	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-15 SG.SC-9 SG.SC-12	GF 5 GF 7
System & Communication Protection.18	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	GF 5 GF 7
System & Communication Protection.19	Mobile Code	<Role> shall accept mobile/active code technologies such as JavaScript, ActiveX, Flash, Java Applets, etc. only from trusted components deployed on WAMPAC Operations Network Segments or WAMPAC Engineering Network Segments. The system shall actively detect and prevent any unauthorized code from executing on <role>. All use of mobile code shall be monitored.	SG.SC-16	GF 18
System & Communication Protection.20	Phasor Data Transmission	The system shall use Private Networks to transmit phasor and WAMPAC management data.	SG.SC-18 SG.SC-20	GF 5 GF 10
System & Communication Protection.21	No Shared Accounts	The system shall associate each individual account (no shared accounts) 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.SC-19	GF 13 GF 17 GF18
System & Communication Protection.22	Addressing	DNS services shall only be deployed in conjunction with DNSSec. Otherwise addressing shall be performed using static IP and/or host tables.	SG.SC-21	GF 1 GF 7
System & Communication Protection.23	Centralized Authentication	Authentication servers for the WAMPAC systems shall be separate from authentication servers used for corporate and business systems. The WAMPAC authentication system should be placed in the WAMPAC Operations Network Segments and should not have any trust relationships with other non-WAMPAC centralized authentication systems.	NONE	GF 5 GF 13 GF 8
System & Communication Protection.24	PMU Management	The Phasor Manager and the PMUs it manages shall reside on a network controlled by the same organization.	NONE	GF 4 GF 10

4.2.9 System & Information Integrity

Table 14 – Controls: System & Information Integrity

Control ID	Short Name	Definition	Reference(s)	Failure(s)
System & Information Integrity.01	Testing Updates	The system shall include an isolated environment that replicates the configuration and behavior of the actual architecture and environment for testing and scanning of updates to firmware and software prior to deployment to determine effectiveness and potential side effects.	SG.SI-2	GF 18
System & Information Integrity.02	System/Device Deficiency	The system shall flag any <role> that does not satisfy an organization approved baseline secure configuration.	SG.SI-2	SF 7
System & Information Integrity.03	Process White Listing	<Role> shall be configured with a process white list to restrict processes to only those necessary to support the <role's> function.	NONE	GF 5 GF 6 GF 16 GF 18
System & Information Integrity.04	End Point Security	<Roles> using a general purpose operating system shall implement end point security mechanisms to scan software for malicious code.	(SG.SI-3)	GF 18
System & Information Integrity.05	End Point Isolation	The system shall provide the capability to isolate compromised devices from the rest of the WAMPAC system upon detection of compromise.	NONE	GF 5 GF 7
System & Information Integrity.06	Intrusion Detection	The system shall detect anomalous events within network segments and across network segment boundaries. This detection shall be WAMPAC 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.AC-15 (SG-SI-4)	GF 5 GF 4
System & Information Integrity.07	Configuration File Authenticity	<Role> shall not accept any message payload containing configuration files that is not cryptographically signed. Acceptable technologies shall be specified by FIPS 186.	SG.AU-16 SG.SC-12 SG.SI-7	GF9 GF 17
System & Information Integrity.08	Configuration File and Sensitive Data Integrity Check	Configuration files and other sensitive data should include cryptographic integrity checks (e.g., keyed or safely protected cryptographic hashes) and the integrity of the file should be checked whenever it is read by an application	SG.SI-7	GF 17
System & Information Integrity.09	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.AU-16 SG.SC-12 SG.SI-7	GF 9 GF 18

Control ID	Short Name	Definition	Reference(s)	Failure(s)
System & Information Integrity.10	Software Integrity Check	The system shall maintain a complete image of all currently deployed component software. All components shall maintain a hash of installed software, including patches, in protected repository Any update to component software shall require a recalculation of the hash. A periodic integrity check of all component software shall be performed by comparing the hash on the component to the hash in the repository. This check shall be performed at least once every 30 days. Acceptable technologies shall be specified by FIPS 186.	SG.SC-12 SG.SI-7	GF 18
System & Information Integrity.11	Storage Integrity Check	<Role> shall perform automated checks (e.g., file system checks, database integrity checks, and checksum comparisons) 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>.	NONE	GF 14
System & Information Integrity.12	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.	NONE	SF 8
System & Information Integrity.13	Manual Input Checking	The <role> employs mechanisms to check manual input for accuracy, completeness, validity, and authenticity.	SG.SI-8	GF 8 GF 9
System & Information Integrity.14	Message Validation	<Role> shall validate all application protocol fields that it uses for logical and expected values including source, destination, time stamps, and state indicators. <Role> shall use its context and history when assessing the validity of the message. For Alignment and Alignment (Field), this shall include timestamps on all PMU data. For Application and Application (Field) this shall include phasor values in all PMU data.	SG.SI-8	GF 8 GF 9
System & Information Integrity.15	Sufficient Error Message Content	The system shall log all errors identified in an organization-defined list and error messages shall provide information necessary for corrective action.	SG.SI-9	SF 8
System & Information Integrity.16	Minimal Error Message Content	<Role> shall not reveal potentially harmful (e.g., exploitable) information in error messages.	SG.SI-9	GF 13
System & Information Integrity.17	Message Timestamping	<Role> shall time stamp all configuration and management messages that it sends.	NONE	GF 17
System & Information Integrity.18	Verify Configuration and Management Message Currency	<Role> shall verify that all configuration and management messages that it receives arrive within an organizationally-defined time window that meets its design or process requirements. <Role> shall log and report all delays exceeding this time window.	NONE	GF 17

Control ID	Short Name	Definition	Reference(s)	Failure(s)
System & Information Integrity.19	Internal Clock Drift	<Role> shall use an accurate internal clock with minimal drift (no greater than 3 ms) upon loss of synchronization from the external time source.	NONE	Clock 1
System & Information Integrity.20	Clock Record	<Role's> clock record shall indicate time source used for synchronization and when last synchronized.	NONE	Clock 2 Clock 3 Clock 5
System & Information Integrity.21	Clock Deviation	<Role> shall continually compare external time source to local clock and flag if deviation exceeds 3 ms.	NONE	Clock 2
System & Information Integrity.22	Multiple Clock Source	<Role> shall continually compare 2 or more external time sources and flag if deviation exceeds 3 ms.	NONE	Clock 1 Clock 3
System & Information Integrity.23	Time Source	<Role> shall always use stratum one time source(s) for time synchronization.	NONE	Clock 4
System & Information Integrity.24	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.	SG.AU-4	GF 15
System & Information Integrity.25	Disk Provisioning	<Role> shall have its logical media overprovisioned by at least 25%.	SG.AU-4	GF 15
System & Information Integrity.26	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.	NONE	GF 15
System & Information Integrity.27	Select Before Operate	The <role> shall support "Select Before Operate" when issuing or confirming commands.	NONE	GF 2 GF 3

4.3 Security Controls Mapping

The following tables allocate controls to either roles or network segments. If an organization cannot meet an indicated control, the organization shall note an exception, implement other mitigating controls, and supply rationale indicating why the mitigating control is sufficient to satisfy the indicated control.

Table 15 includes four controls (at the end of the table) that are not defined in this document. These are controls from the NIST IR 7628 that are allocated, unchanged, to WAMPAC roles.

4.3.1 Controls Mapped to Roles

Table 15 – Controls Mapped to Roles

Control ID	Short Name	Alignment	Alignment (Field)	Application	Application (Field)	Data Store	Environmental Data Interface	Phasor Gateway	PMU	Phasor Manager	Registry
Access Control.01	Automated Account Management	x	x	x	x	x	x	x	x	x	x
Access Control.02	Least Privilege	x	x	x	x	x	x	x	x	x	x
Access Control.03	Access Enforcement	x	x	x	x	x	x	x	x	x	x
Access Control.04	Unsuccessful Access Attempts	x	x	x	x	x	x	x	x	x	x
Access Control.05	Emergency Access			x	x						
Access Control.06	Concurrent Session Management	x	x	x	x	x	x	x	x	x	x
Access Control.07	Session Duration	x	x	x	x	x	x	x	x	x	x
Access Control.08	Portable Device Attachment	x	x	x	x	x	x	x	x	x	x
Access Control.10	Wireless Encryption		x		x				x		
Access Control.11	Wireless Usage	x	x	x	x	x	x	x	x	x	x
Access Control.12	Password Management	x	x	x	x	x	x	x	x	x	x
Audit & Accountability.1	Inappropriate User Activity	x	x	x	x	x	x	x	x	x	x
Audit & Accountability.2	User Access Monitoring/Logging	x	x	x	x	x	x	x	x	x	x
Audit & Accountability.3	Local and Central Logging	x	x	x	x	x	x	x	x	x	
Audit & Accountability.4	Electronic Log Format	x	x	x	x	x	x	x	x	x	x
Audit & Accountability.5	Content of Audit Records	x	x	x	x	x	x	x	x	x	x
Configuration Management.1	Systems Inventory	x	x	x	x	x	x	x	x	x	x
Configuration Management.2	Current Configuration	x	x	x	x	x	x	x	x	x	x

Control ID	Short Name	Alignment	Alignment (Field)	Application	Application (Field)	Data Store	Environmental Data Interface	Phasor Gateway	PMU	Phasor Manager	Registry
Configuration Management.3	Disabling Unnecessary Functionality	x	x	x	x	x	x	x	x	x	x
Configuration Management.4	Disabling Unnecessary Communication Services	x	x	x	x	x	x	x	x	x	x
Configuration Management.5	Factory Default Credentials	x	x	x	x	x	x	x	x	x	x
Continuity of Operations.1	Alternate Control Center	x		x		x		x		x	
Continuity of Operations.2	WAN Communication Outage		x		x				x		
Continuity of Operations.3	Operations Continuity	x	x	x	x	x	x	x	x	x	x
Continuity of Operations.4	Graceful Degradation	x		x		x	x	x		x	
Continuity of Operations.5	System Restoration	x	x	x	x	x	x	x	x	x	x
Continuity of Operations.6	Alternative Time Source	x	x						x		
Identification & Authorization.01	Identifier Management	x	x	x	x	x	x	x	x	x	x
Identification & Authorization.02	Credential Management	x	x	x	x	x	x	x	x	x	x
Identification & Authorization.03	Digital Certificates	x	x	x	x	x		x	x	x	
Identification & Authorization.04	Two Factor Authentication	x	x	x	x	x	x	x	x	x	x
Identification & Authorization.05	Device Identification and Authentication	x	x	x	x	x	x	x	x	x	x
Identification & Authorization.06	Cryptographic Module Authentication	x	x	x	x	x	x	x	x	x	x
Identification & Authorization.07	Message Identities	x	x	x	x	x	x	x	x	x	x
Identification & Authorization.08	Authenticator Feedback	x	x	x	x	x	x	x	x	x	x

Control ID	Short Name	Alignment	Alignment (Field)	Application	Application (Field)	Data Store	Environmental Data Interface	Phasor Gateway	PMU	Phasor Manager	Registry
Identification & Authorization.09	Self Identification	x	x	x	x	x	x	x	x	x	x
Identification & Authorization.10	Authenticated Link Establishment		x		x		x	x	x		
Identification & Authorization.11	Authenticated Link Restoration		x		x		x	x	x		
Physical & Environmental.01	Physical Access Authentication	x		x		x	x	x		x	x
Physical & Environmental.02	Limited Access - Interactive Resources			x			x			x	x
Physical & Environmental.03	Limited Access - Non-interactive Resources	x				x		x			
Physical & Environmental.04	Limited Field Component Access		x		x				x		
Physical & Environmental.05	Tamper Resistant and Tamper Evident Field Components		x		x				x		
Physical & Environmental.06	Facility Access Monitoring/Logging	x	x	x	x	x	x	x	x	x	x
Physical & Environmental.07	Cabinet Access Monitoring/Logging		x		x				x		
Physical & Environmental.08	Physical Access Indications		x		x				x		
Physical & Environmental.09	Power Sources and Cables	x	x	x	x	x	x	x	x	x	x
Physical & Environmental.10	Power Source Monitoring/Logging	x	x	x	x	x		x	x	x	
Physical & Environmental.11	Emergency Power Shutoff	x		x		x		x		x	
Physical & Environmental.12	Alternate Power Source	x		x		x		x		x	
Physical & Environmental.13	Backup Power Requirement		x		x				x		
Physical & Environmental.14	Component Location	x	x	x	x	x	x	x	x	x	x

Control ID	Short Name	Alignment	Alignment (Field)	Application	Application (Field)	Data Store	Environmental Data Interface	Phasor Gateway	PMU	Phasor Manager	Registry
Physical & Environmental.15	Fire Detection	x		x		x		x		x	
Physical & Environmental.16	EMI/Surge Protection		x		x				x		
Physical & Environmental.17	Supporting systems shall implement a minimum of two factor authentication for local <role> access to devices and applications in the field.		x		x						
System & Communication Protection.01	Management/Configuration Isolation	x	x	x	x	x	x	x	x	x	x
System & Communication Protection.02	Security Function Isolation	x	x	x	x	x	x	x	x	x	x
System & Communication Protection.03	Secure Coding Practices	x	x	x	x	x	x	x	x	x	x
System & Communication Protection.04	Secure Communications Services	x	x	x	x	x	x	x	x	x	x
System & Communication Protection.05	Startup in Known State	x	x	x	x	x	x	x	x	x	x
System & Communication Protection.06	Quality of Service - Specification	x	x	x	x	x	x	x	x	x	x
System & Communication Protection.08	Resource Consumption	x	x	x	x	x			x	x	
System & Communication Protection.09	Resource Monitoring	x	x	x	x	x		x	x	x	
System & Communication Protection.10	Communication Integrity	x	x	x	x	x	**9**	x	x	x	x

[9] The Environmental Data Interface is only required to implement this control for communications with Applications. This control should also be implemented for communications with any External Data Source that supports the necessary mechanisms.

Control ID	Short Name	Alignment	Alignment (Field)	Application	Application (Field)	Data Store	Environmental Data Interface	Phasor Gateway	PMU	Phasor Manager	Registry
System & Communication Protection.11	Communication Confidentiality	x	x	x	x	x	x	x	x	x	x
System & Communication Protection.16	Separate Keys for Separate Functions	x	x	x	x	x	x	x	x	x	x
System & Communication Protection.17	Remote Interactive Sessions		x		x				x		
System & Communication Protection.18	Cryptographic Key Implementation and Management	x	x	x	x	x	x	x	x	x	x
System & Communication Protection.19	Mobile Code	x	x	x	x	x	x	x	x	x	x
System & Communication Protection.21	No Shared Accounts	x	x	x	x	x	x	x	x	x	x
System & Information Integrity.01	Testing Updates	x	x	x	x	x	x	x	x	x	x
System & Information Integrity.02	System/Device Deficiency	x	x	x	x	x	x	x	x	x	x
System & Information Integrity.03	Process White Listing	x	x	x	x	x		x	x		
System & Information Integrity.04	End Point Security	x	x	x	x	x	x	x		x	x
System & Information Integrity.05	End Point Isolation	x	x	x	x	x	x	x	x	x	x
System & Information Integrity.07	Configuration File Authenticity	x	x	x	x	x	x	x	x	x	x
System & Information Integrity.08	Configuration File and Sensitive Data Integrity Check	x	x	x	x	x	x	x	x	x	x

Control ID	Short Name	Alignment	Alignment (Field)	Application	Application (Field)	Data Store	Environmental Data Interface	Phasor Gateway	PMU	Phasor Manager	Registry
System & Information Integrity.09	Software and Firmware Authenticity	x	x	x	x	x	x	x	x	x	x
System & Information Integrity.10	Software Integrity Check	x	x	x	x	x	x	x	x	x	x
System & Information Integrity.11	Storage Integrity Check	x	x	x	x	x	x	x	x	x	x
System & Information Integrity.12	Health Monitoring	x	x	x	x	x	x	x	x	x	**10**
System & Information Integrity.13	Manual Input Checking	x	x	x	x		x		x	x	x
System & Information Integrity.14	Message Validation	x	x	x	x	x	x	x	x	x	x
System & Information Integrity.15	Sufficient Error Message Content	x	x	x	x	x	x	x	x	x	x
System & Information Integrity.16	Minimal Error Message Content	x	x	x	x	x	x	x	x	x	x
System & Information Integrity.17	Message Timestamping	x	x	x	x	x	x	x	x	x	x
System & Information Integrity.18	Verify Configuration and Management Message Currency	x	x	x	x	x	x	x	x	x	x
System & Information Integrity.19	Internal Clock Drift	x	x						x		
System & Information Integrity.20	Clock Record	x	x						x		

[10] Only the organization operating the Registry is expected to monitor the Registry.

Control ID	Short Name	Alignment	Alignment (Field)	Application	Application (Field)	Data Store	Environmental Data Interface	Phasor Gateway	PMU	Phasor Manager	Registry
System & Information Integrity.21	Clock Deviation	x	x						x		
System & Information Integrity.22	Multiple Clock Source	x	x						x		
System & Information Integrity.23	Time Source	x	x						x		
System & Information Integrity.24	Configured Size Warnings	x	x	x	x	x	x	x	x	x	x
System & Information Integrity.25	Disk Provisioning	x	x	x	x	x	x	x	x	x	x
System & Information Integrity.26	Replacement of Data	x	x	x	x	x	x	x	x	x	x
System & Information Integrity.27	Select Before Operate			x	x						
SG.AC-9	Smart Grid Information System Use Notification	x	x	x	x	x	x	x	x	x	x
SG.AC-10	Previous Logon Notification	x	x	x	x	x	x	x	x	x	x
SG.SC-22	Fail in Known State	x	x	x	x	x	x	x	x	x	x
SG.SC-26	Confidentiality of Information at Rest	x	x	x	x	x	x	x	x	x	x

4.3.2 Controls Mapped to Network Segments

Table 16 – Controls Mapped to Network Segments

Control ID	Short Name	DMZ	Operations	Field	Engineering	NASPInet
Access Control.9	Remote Access Restrictions	x	x	x	x	x
Network.1	Field Network Allocation			x		
Network.2	Field Network Connection		x	x		
Network.3	Operations Network Allocation		x			
Network.4	Operations Network Connection		x			
Network.5	Engineering Network Allocation				x	
Network.6	Engineering Network Connection				x	
Network.7	DMZ Network Allocation	x				
Network.8	DMZ Network Connection					
System & Communication Protection.07	Quality of Service - Enforcement		x	x		
System & Communication Protection.12	Traffic Control and Filtering	x	x	x	x	x
System & Communication Protection.13	No Internet Access		x	x	x	
System & Communication Protection.14	Non-adjacent Network Restrictions		x	x	x	x
System & Communication Protection.15	Emergency Network Segmentation	x	x	x	x	x
System & Communication Protection.20	Phasor Data Transmission	x	x	x	x	x
System & Communication Protection.22	Addressing	x	x	x	x	x
System & Communication Protection.23	Centralized Authentication	x	x	x	x	
System & Communication Protection.24	PMU Management		x	x		
System & Information Integrity.06	Intrusion Detection	x	x	x	x	x

Appendix A: Relation to the NIST Interagency Report 7628

A goal of the WAMPAC security profile is to support and align with the NIST IR 7628. The WAMPAC Security Profile is an in-depth approach to wide-area monitoring, protection and control using synchrophasors that leverages work done in the NIST IR 7628. WAMPAC also includes wide-area situational awareness (WASA) functionality as a subset of this profile. The reader will find that the WAMPAC Security Profile does not apply the Logical Interface Categories (LIC) found in the NIST IR 7628. Instead, this document approaches analyzing each interface with finer granularity at each process step in regard to failure analysis and control development (refer to Figure 9).

A.1 Traceability

This section documents the traceability found between the NIST IR 7628 and the WAMPAC Security Profile. The WAMPAC Security Profile incorporates the NIST IR 7628 in each of the five major phases of the security profile development.

1. Scope – This document incorporates a review and analysis of NIST IR 7628 use cases to guide the development of WAMPAC scope.
2. Logical Architecture – This document incorporates a review and analysis of relevant architectural elements from the NIST IR 7628 in the WAMPAC logical architecture development, re-using actors where possible and further decomposing the architecture where needed.

3. Security Influences – This document incorporates an analysis of the security objectives defined in the NIST IR 7628 use cases in developing and expanding security principles for WAMPAC.
4. Security Controls – This document used the relevant technical requirements from NIST IR 7628 as a source of inspiration for the development of the controls for this security profile. The NIST IR 7628 controls were also used as a means to verify coverage by way of identifying controls that this document might not have otherwise considered.
5. Validation – the validation step is an iterative process in the development of a security profile. This document incorporates a review of the NIST IR 7628 controls and actor-to-control mappings as a means to ensure completeness in the WAMPAC Security Profile.

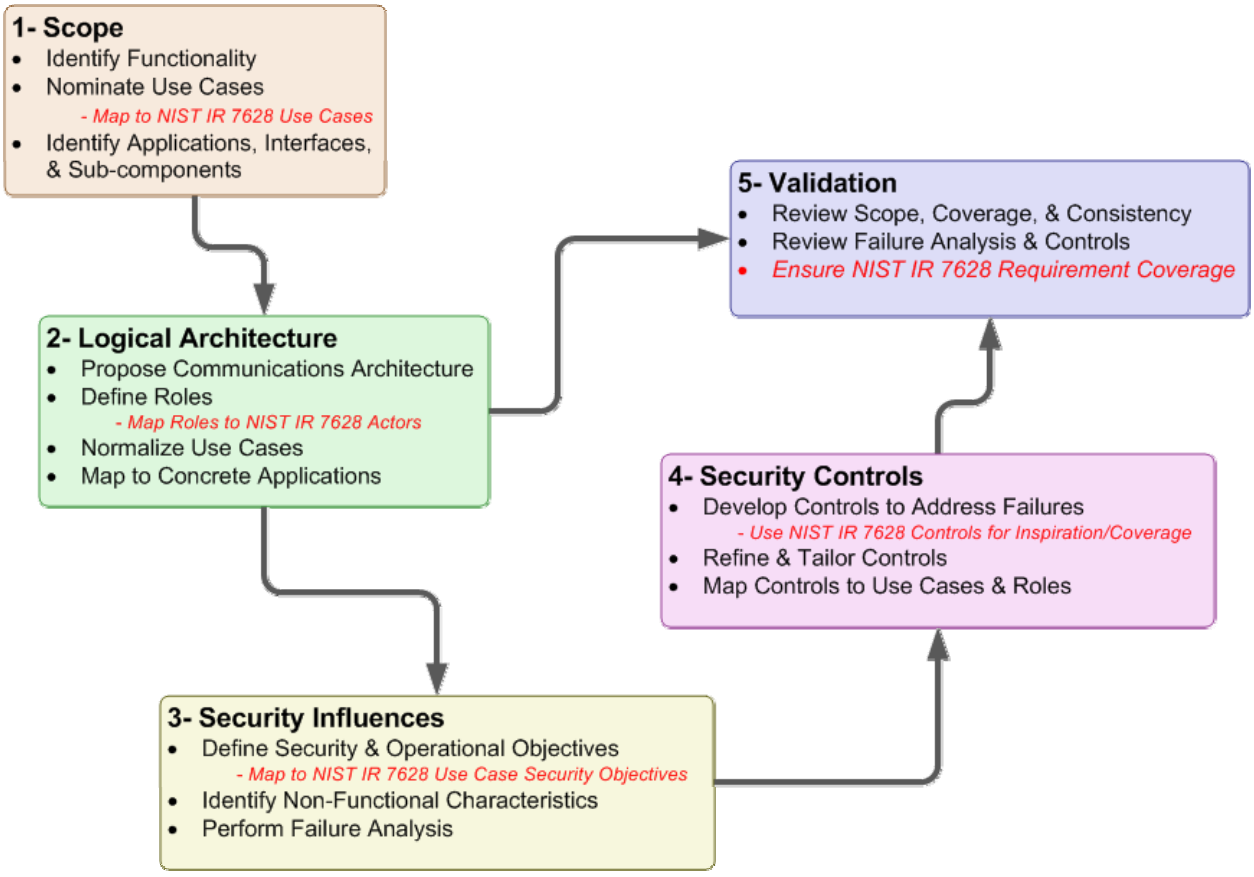

Figure 9 – Security Profile Workflow NIST-IR 7628 Mapping

A.2 NIST IR 7628 Actors to WAMPAC Roles Mapping

This section documents the mapping from NIST IR 7628 actors to WAMPAC Security Profile roles. This document uses the term "Role" to denote the function performed by the object within the use cases since a given device may perform more than one function. This approach supported the understanding of security failures and controls at the lowest level practical.

By comparison, although subtle, an "Actor" as defined by the OMG for unified modeling language is:

> *A type of role played by an entity that interacts with the subject, but which is external to the subject. Actors may represent roles played by human users, external hardware, or other subjects. Note that an actor does not necessarily represent a specific physical entity but merely a particular facet (i.e., "role") of some entity that is relevant to the specification of its associated use cases. Thus, a single physical instance may play the role of several different actors and, conversely, a given actor may be played by multiple different instances. (p.604-5, OMG Unified Modeling Language (OMG UML), Superstructure Version 2.3)*

Briefly, NIST IR 7628 actors are entities that may perform many WAMPAC roles. NIST IR 7628 actors are derived from Figure F-6, Volume 3 page F-21.

Where the WAMPAC role is labeled "no role identified" the NIST IR 7628 actor was determined out of scope for this security profile. In some cases the NIST IR 7628 actor maps to an aggregate of WAMPAC roles. This document identifies one role, the Registry, that does not have a mapping in the current NIST IR 7628 (Refer to Table 17).

Table 17 – NIST IR 7628 Actor to WAMPAC Role Mapping

NIST IR 7628 Actor	WAMPAC Role
Phasor Measurement Unit	Phasor Measurement Unit
Transmission RTU	External Data Source
Transmission IED	External Data Source
Distribution RTUs or IEDs	External Data Source
Wide Area Measurement System	WAMPAC Application
	WAMPAC Alignment
	WAMPAC Data Store
	Phasor Gateway
Transmission SCADA	Non-WAMPAC Application
	Non-WAMPAC Data Store
	Environmental Data Interface
Energy Management System	Non-WAMPAC Application
	Non-WAMPAC Data Store
	Environmental Data Interface
Distribution Management System	Non-WAMPAC Application
	Non-WAMPAC Data Store

NIST IR 7628 Actor	WAMPAC Role
	Environmental Data Interface
ISO/RTO Operations	Non-WAMPAC Application
	Non-WAMPAC Data Store
	Environmental Data Interface
Plant Control System	No role identified
ISO/RTO/Wholesale Market	No Role identified
Aggregator/Retail Energy Provider	No Role identified
Customer Energy Management System	No Role identified
No Actor identified	WAMPAC Registry

A.3 NIST IR 7628 and WAMPAC Use Case Mapping

This section documents the mapping between NIST IR 7628 and WAMPAC Security Profile use cases. The NIST IR 7628 was examined to identify use cases that support WAMPAC scenarios and functions. Two scenarios within the Transmission Operations category map to the WAMPAC Security Profile use cases:

> ***Transmission Operations Category Description:*** *Transmission operations involve monitoring and controlling the transmission system using the SCADA system to monitor and control equipment in transmission substations. The EMS assesses the state of the transmission system using applications typically based on transmission power flow models. The SCADA/EMS is located in the utility's control center, while the key equipment is located in the transmission substations. Protective relaying equipment monitors the health of the transmission system and takes corrective action within a few milliseconds, such as tripping circuit breakers if power system anomalies are detected.*
>
> ***Scenario:*** *Real-Time Normal Transmission Operations Using Energy Management Systems (EMS) and SCADA Data*[11]
>
> ***Scenario Description:*** *Real-Time Normal Transmission Operations Using Energy Management System (EMS) Applications and SCADA Data (NIST-IR 7628 Vol. III, p. 129). Transmission normal real-time operations involve monitoring and controlling the transmission system using the SCADA and EMS. The types of information exchanged include—*
>
> *Monitored equipment states (open/close), alarms (overheat, overload, battery level, capacity), and measurements (current, voltage, frequency, energy)*

[11] NIST IR 7628, Volume III, p. 129

Operator command and control actions, such as supervisory control of switching operations, setup/options of EMS functions, and preparation for storm conditions

Closed-loop actions, such as protective relaying tripping circuit breakers upon power system anomalies

Automation system controls voltage, VAR, and power flow based on algorithms, real-time data, and network linked capacitive and reactive components

…

Scenario: *Wide Area Synchro-Phasor System*[12]

Scenario Description: *The wide area synchrophasor system provides synchronized and time-tagged voltage and current phasor measurements to any protection, control, or monitoring function that requires measurements taken from several locations, whose phase angles are measured against a common, system-wide reference. Present day implementation of many protection, control, or monitoring functions is hobbled by not having access to the phase angles between local and remote measurements. With system-wide phase angle information, they can be improved and extended. The essential concept behind this system is the system-wide synchronization of measurement sampling clocks to a common time reference.*

The WAMPAC Security Profile has built on these scenarios and extended them into 16 detailed use cases, each with specifically defined process steps.

Table 18 – NIST IR 7628 Use Cases to WAMPAC Use Cases

NIST IR 7628 Use Case Category	NIST IR 7628 Use Case Scenarios	Overlapping WAMPAC Use Cases	Notes
Transmission Operations	1) Real-Time Normal Transmission Operations Using Energy Management System (EMS) Applications and SCADA Data (p.129)	13 - Environmental Data Interface forwards data to Application 14- Non-WAMPAC Application sends data to WAMPAC Application 15 - Application processes new data	Non-WAMPAC Application (EMS) feeds WAMPAC Application with SCADA data
Transmission Operations	2) EMS Network Analysis Based on Transmission Power Flow Models, Real-Time Emergency Transmission Operations	13 - Environmental Data Interface forwards data to Application 14- Non-WAMPAC Application sends data to WAMPAC Application 15 - Application processes new data	
Transmission Operations	3) Real-Time Emergency Transmission Operations	13 - Environmental Data Interface forwards data to Application 14- Non-WAMPAC Application sends data to WAMPAC Application 15 - Application processes new data	

[12] NIST IR 7628, Volume III, p. 132

NIST IR 7628 Use Case Category	NIST IR 7628 Use Case Scenarios	Overlapping WAMPAC Use Cases	Notes
Transmission Operations	4) Wide Area Synchro-Phasor System	All Use Cases	
RTO/ISO Operations	1) RTO/ISO Management of Central and DER Generators and Storage	13 - Environmental Data Interface forwards data to Application 14- Non-WAMPAC Application sends data to WAMPAC Application 15 - Application processes new data	Application is a management application

A.4 NIST IR 7628 Security Objectives to WAMPAC Security Principles Mapping

This section documents the mapping between NIST IR 7628 security objectives and the security principles embodied in the WAMPAC Security Profile. The Security Principles that serve as the foundation for the WAMPAC Security Profile can be found in Section 3.2.3 of this document. The NIST IR 7628 Cyber Security Objectives/Requirements are embedded within each use case description found in Section 10.3 of Volume 3 of NIST IR 7628.

Table 19 below, maps WAMPAC security principles to the NIST IR 7628 scenarios in which the listed security principles apply. Each of the scenarios in the table comes from 10.3.8 Transmission Resources Security Use Cases.

Table 19 – NIST IR 7628 Use Case Objectives to WAMPAC Security Principles

NIST IR 7628 Scenario	Cyber Security Objective / Requirements	WAMPAC Security Principle
Electricity Market Security - Bulk Power Electricity Market	Integrity for pricing and generation information is critical Availability for pricing and generation information is important within minutes to hours Confidentiality for pricing and generation information is critical	3, 4, 7, 13,14
Retail Power Electricity Market	Integrity for pricing and generation information is critical Availability for pricing and generation information is important within minutes to hours Confidentiality for pricing and generation information is critical	3, 4, 7, 13, 14
Real-Time Normal Transmission Operations Using Energy Management System (EMS) Applications and SCADA Data	Integrity is vital to the safety and reliability of the transmission system Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g., 1 s) Confidentiality is not important	1,2,3,7

NIST IR 7628 Scenario	Cyber Security Objective / Requirements	WAMPAC Security Principle
EMS Network Analysis Based on Transmission Power Flow Models	Integrity is vital to the reliability of the transmission system Availability is critical to react to contingency situations via operator commands (e.g. one second) Confidentiality is not important	3,7
Wide Area Synchro-Phasor System	Integrity is vital to the safety and reliability of the transmission system Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g., 1 s) Confidentiality is not important	3,7

Table 1Table 19 shows the Use Cases and related Cyber Security Objectives from NIST IR 7628 which are relevant to the scope of this security profile. The security objectives as defined in the NIST IR 7628 include the confidentiality, integrity, and availability (CIA) aspect of the Use Case under consideration. Fourteen objectives for the WAMPAC system were identified and utilized throughout the profile for use case development and failure identification. These principles are described in Section 3.2. Table 20 below maps the WAMPAC security principles to the confidentiality, integrity, and availability attributes used by the NIST IR 7628 to describe its security objectives. Note that some WAMPAC security principles may map to more than one attribute, however each is only correlated to their primary attribute here for simplicity.

Table 20 – Security Attributes to WAMPAC Security Principles

Attribute	WAMPAC Security Principle
Availability	1-Security controls should have minimal impact on, and in no way prevent the primary mission of the WAMPAC system. 2-Security controls should minimize the impact of adverse events on the quality of service for WAMPAC communications and functions. 8-Asset owners should not rely exclusively on security measures outside their direct observation and control. 9-The introduction or integration of WAMPAC systems should not expose other utility systems to unauthorized access or attack (i.e.: don't increase the attack surface). 10-Utility systems should be able to continue essential functions in the absence of PMU data. 12-Essential WAMPAC functionality should not have single points of failure.
Integrity	5-Only authenticated and authorized configuration changes (e.g.: firmware, settings, etc.) should be processed by WAMPAC systems. 6-All configuration changes and access requests to WAMPAC systems should be auditable 7-WAMPAC applications should validate the authenticity and integrity of all data acquired. 11-Authorized operators should have the ability to disable automated protection and control associated with WAMPAC systems while maintaining monitoring functionality.
Confidentiality	3-No external entity should have direct access to a utility's PMU. 4-All WAMPAC systems and components should restrict logical and physical access to authenticated and authorized systems and personnel.

Attribute	WAMPAC Security Principle
	13-WAMPAC systems should protect synchrophasor and other system data from unauthorized disclosure. 14-WAMPAC systems should at all times be able to determine who has access to synchrophasor and other system data.

A.5 NIST IR 7628 Technical Requirements Mapped to WAMPAC Controls

This section documents the mapping and degree of coverage between NIST IR 7628 technical requirements and WAMPAC security profile controls.

Table 21 – NIST IR 7628 Requirements to WAMPAC Controls

NIST IR 7628 Requirement	NIST IR 7628 Short Name	WAMPAC Control	Coverage
SG.AC-5	Information Flow Enforcement	System & Communication Protection.12	fully covered
SG.AC-6	Separation of Duties	Access Control.2 Access Control.3	covers non-organizational portions
SG.AC-7	Least Privilege	Access Control.2 Access Control.3	fully covered
SG.AC-8	Unsuccessful Login Attempts	Access Control.4	fully covered
SG.AC-11	Concurrent Session Control	Access Control.6	fully covered
SG.AC-12	Session Lock	Access Control.7	fully covered
SG.AC-13	Remote Session Termination	Access Control.7	fully covered
SG.AC-14	Permitted Actions without Identification or Authentication	Access Control.5	NIST IR 7628 is organizational, but supported by our control

NIST IR 7628 Requirement	NIST IR 7628 Short Name	WAMPAC Control	Coverage
SG.AC-15	Remote Access	Access Control.3 Access Control.9 Access Control.10 Access Control.11 Identification & Authorization.3 Identification & Authorization.4 Identification & Authorization.5 Identification & Authorization.6 Network.2 System & Information Integrity.6 System & Communication Protection.10 System & Communication Protection.11 System & Communication Protection.12 System & Communication Protection.14 System & Communication Protection.17	fully covered
SG.AC-16	Wireless Access Restrictions	Access Control.10 Access Control.11	fully covered
SG.AC-17	Access Control for Portable and Mobile Devices	Access Control.8	fully covered
SG.AC-21	Passwords	Access Control.12	fully covered
SG.AU-2	Auditable Events	Access Control.1 Access Control.5 Audit & Accountability.1 Audit & Accountability.3 Identification & Authorization.3	covers non-organizational portions
SG.AU-3	Content of Audit Records	Audit & Accountability.5	fully covered
SG.AU-4	Audit Storage Capacity	Audit & Accountability.3 Audit & Accountability.4 System & Information Integrity.24 System & Information Integrity.25	fully covered
SG.AU-15	Audit Generation	Audit & Accountability.5	fully covered

NIST IR 7628 Requirement	NIST IR 7628 Short Name	WAMPAC Control	Coverage
SG.AU-16	Non-Repudiation	Audit & Accountability.2 Audit & Accountability.3 Identification & Authorization.3 System & Communication Protection.10 System & Information Integrity.7 System & Information Integrity.9	fully covered
SG.CM-7	Configuration for Least Functionality	Configuration Management.3 Configuration Management.4	fully covered
SG.CM-8	Component Inventory	Configuration Management.1	fully covered
SG.IA-4	User Identification and Authentication	Identification & Authorization.4	fully covered
SG.IA-5	Device Identification and Authentication	Identification & Authorization.5 Identification & Authorization7	fully covered
SG.IA-6	Authenticator Feedback	Identification & Authorization.8	fully covered
SG.SC-2	Communications Partitioning	System & Communication Protection.1	fully covered
SG.SC-3	Security Function Isolation	System & Communication Protection.2	fully covered
SG.SC-4	Information Remnants	System & Communication Protection.3	partially covered; object reuse is not addressed by our control.
SG.SC-5	Denial-of-Service Protection	System & Communication Protection.12 Continuity of Operations.2 Continuity of Operations.3 Continuity of Operations.6	partially covered – NIST IR 7628 does not give specific guidance on how to meet requirement. WAMPAC provides four specific mitigations for DoS, but does not directly address DoS and shouldn't IMHO.
SG.SC-6	Resource Priority	System & Communication Protection.6 System & Communication Protection.7 System & Communication Protection.8	

NIST IR 7628 Requirement	NIST IR 7628 Short Name	WAMPAC Control	Coverage
SG.SC-7	Boundary Protection	Network.2 Network.4 Network.6 Network.8 Identification & Authorization.5 Identification & Authorization.6 System & Communication Protection.10 System & Communication Protection.11 System & Communication Protection.12 System & Communication Protection.13 System & Communication Protection.14	fully covered
SG.SC-8	Communication Integrity	Access Control.10 System & Communication Protection.10 System & Information Integrity.9	fully covered
SG.SC-9	Communication Confidentiality	System & Communication Protection.11 System & Communication Protection.16 System & Communication Protection.17 System & Communication Protection.18	fully covered

NIST IR 7628 Requirement	NIST IR 7628 Short Name	WAMPAC Control	Coverage
SG.SC-10	Trusted Path	Access Control.3 Access Control.7 Access Control.10 Configuration Management.4 Identification & Authorization.1 Identification & Authorization.3 Identification & Authorization.4 Identification & Authorization.6 Identification & Authorization.7 Network.2 Network.4 Network.6 Network.8 Physical & Environmental.2 Physical & Environmental.3 Physical & Environmental.14 System & Communication Protection.4 System & Communication Protection.5 System & Communication Protection.10 System & Communication Protection.11 System & Communication Protection.12 System & Communication Protection.13 System & Communication Protection.14 System & Communication Protection.17 System & Communication Protection.20 System & Communication Protection.21 System & Communication Protection.22 System & Information Integrity.4 System & Information Integrity.6 System & Information Integrity.14 System & Information Integrity.17	fully covered
SG.SC-11	Cryptographic Key Establishment and Management	System & Communication Protection.18	fully covered

NIST IR 7628 Requirement	NIST IR 7628 Short Name	WAMPAC Control	Coverage
SG.SC-12	Use of Validated Cryptography	Access Control.10 Access Control.12 Identification & Authorization.9 System & Communication Protection.10 System & Communication Protection.11 System & Communication Protection.17 System & Information Integrity.7 System & Information Integrity.9 System & Information Integrity.10	fully covered
SG.SC-15	Public Key Infrastructure Certificates	Identification & Authorization.3	covers non-organizational portions
SG.SC-16	Mobile Code	System & Communication Protection.19	fully covered
SG.SC-17	Voice-Over Internet Protocol	Configuration Management.4 System & Communication Protection.9	fully covered
SG.SC-18	System Connections	Access Control.9 System & Communication Protection.20	fully covered
SG.SC-19	Security Roles	Access Control.2 Access Control.3 System & Communication Protection.21	covers non-organizational portions
SG.SC-20	Message Authenticity	Identification & Authorization.5 System & Communication Protection.20	fully covered
SG.SC-21	Secure Name/Address Resolution Service	System & Communication Protection.22	fully covered
SG.SC-29	Application Partitioning	Access Control.2 and Access Control.3	seems redundant with NIST IR 7628 least privilege controls
SG.SC-30	Smart Grid Information System Partitioning	Network.1 - Network.8	fully covered
SG.SI-2	Flaw Remediation	Configuration Management.2 System & Information Integrity.1 System & Information Integrity.2	fully covered

NIST IR 7628 Requirement	NIST IR 7628 Short Name	WAMPAC Control	Coverage
SG.SI-7	Software and Information Integrity	Configuration Managment.2 Identification & Authorization.9 System & Information Integrity.7 System & Information Integrity.8 System & Information Integrity.9 System & Information Integrity.10	fully covered
SG.SI-8	Information Input Validation	System & Information Integrity.13 System & Information Integrity.14	fully covered
SG.SI-9	Error Handling	System & Information Integrity.15 System & Information Integrity.16	fully covered
SG.AC-5	Information Flow Enforcement	System & Communication Protection.12	fully covered
SG.AC-6	Separation of Duties	Access Control.2 and Access Control.3	covers non-organizational portions
SG.AC-7	Least Privilege	Access Control.2 and Access Control.3	fully covered

A.6 NIST IR 7628 Relationship Summary

This document leverages NIST IR 7628 as an invaluable resource in examining and defining security controls for WAMPAC. The work of the NIST IR 7628 has been expanded within this document to include detailed use cases, reference models, and network topologies used in the selection of controls. Although there is not direct mapping, implementing the WAMPAC Security Profile seeks to satisfy NIST IR 7628 security requirements as they apply to the use cases specified in this document.

Appendix B: Use Case Notation Guide

The use cases presented in Section 2.4 of this document include activity diagrams that graphically depict the flow of information/data and activities performed by roles in order to complete the use case. An example is shown in Figure 10 below.

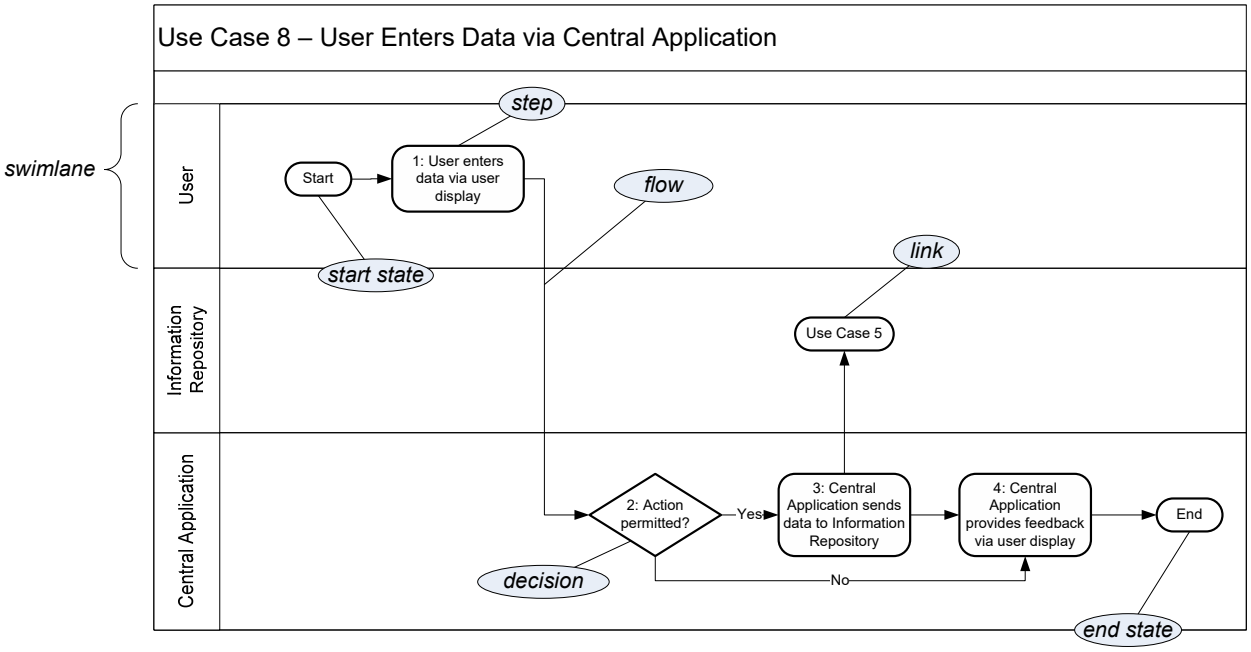

Figure 10 – An Annotated Activity Diagram

This example is annotated to illustrate key features of the notation.

1. Activity diagrams are organized around *swimlanes*. A swimlane is a horizontal region used to represent the activities of a particular role. For example, Figure 10 contains three swimlanes, one each for the User, Information Repository, and Central Application roles.
2. A swimlane contains *steps* that indicate the activities performed by its role during the use case. A step is represented by a rounded box, is numbered, and includes a short description of the work performed during that step.
3. Steps are ordered across a use case by indicating the *flow* of activities using arrows. A flow points from one step to the step that follows it. Flows can cross swimlanes, typically indicating a communication between the roles represented by the swimlanes.
4. In addition to a general step, there are several special kinds of steps:
    a. A *begin state* is a step labeled "Start" that indicates where a use case begins.
    b. A *decision* is a step in which a role makes a decision as to what step should follow. Flows coming from a decision step are labeled (often with "yes" or "no") to indicate the condition (relative to the decision) under which each flow should be followed; if a flow from a decision step is not labeled, then its condition is considered to be always satisfied. Typically only one flow out of a decision step is followed.
    c. An *end state* is a step labeled "End" that indicates the completion of the use case.
    d. A *link* is a step labeled with the name of some other use case (and optionally with a use case step number if the linked use case has more than one starting step). A link indicates that the activity of this use case is followed by the activity of the linked use case.
5. All steps, except for an end state or link, must have at least one outgoing flow. If a non-decision step has multiple outgoing flows, this indicates a split in the flow. Multiple paths will proceed independently in the use case following such a split.
6. Dashed arrows represent *optional flows*. An optional flow indicates a flow that may or may not always happen in a use case, usually based on variation in the implementation or configuration of a role. For example, if some Field Applications always log their activities with an Information Repository but others do not, then an optional flow would be used to indicate that a Field Application may update an Information Repository. Individual implementations would have to determine whether to exercise optional flows.
7. A use case ends when all of its steps have been completed and all remaining flows lead to a terminal—an end state or a link.
8. If multiple flows lead to a common step, this represents a choice of paths for reaching that step; no synchronization is implied.

Appendix C: Evaluating a Wide-Area Monitoring, Protection, & Control System

This document can be used to evaluate a proposed WAMPAC deployment. The security controls and the failure analysis in this security profile are based on the definition of uses cases and roles. In different WAMPAC deployments, the use cases and roles will be mapped to different elements of the actual deployment (as illustrated in Section 4.1). For example, an application may or may not be co-located with the phasor manager. An architectural analysis of a proposed deployment against this document, then, has the following steps.

1. Map the proposed deployment to the network segmentation described in Section 4.1. Identify the different segment types within the deployment. Verify that all of the network controls are in place for the various segments.
2. Map the proposed deployment to the roles in Section 2.2. For every operational element of the proposed deployment (not including communications infrastructure), determine what elements exist. Which elements are data stores, which are applications, which are alignments, which are phasor managers, which are phasor measurement units, which are phasor gateways, which are the environmental data interface, and what external data sources and registries are assumed in the deployment.
3. For each use case, use the mapping generated in step 2 to determine which elements are involved in the use case. Typically, each use case will have multiple instantiations, each with their own elements involved. For example, some alignments may be co-located with a phasor manager, some may not.

4. For each instance of each use case, determine the possible failures, per role and per step. This information comes from the three failure tables in Section 3.3. Then determine the controls that mitigate each possible failure using the mappings in Section 4.1.2.
5. For each element of the proposed WAMPAC deployment, determine the recommended controls for that element. This involves mapping each element to the appropriate use cases and use case steps, proceeding through possible failures and determining the recommended controls. This is the information gathered in steps 1-4 above.
6. For each element of the proposed WAMPAC deployment, and each recommended control for that element, determine how the control is implemented. If the control is not implemented, ensure that all the failures that would be mitigated by the recommended control are being mitigated by one or more alternate controls. Perform a risk analysis to determine the adequacy of the alternate control(s).
7. For each possible failure that is not mitigated, perform a risk analysis that determines the probability of the failure occurring and the cost if the failure does occur.

Appendix D: Glossary and Acronyms

Many of the definitions in this section have been adapted or directly quoted from Smart Grid Today's Glossary of Terms and Abbreviations.[13]

AC: Alternating Current

Actuator: Within an electric power system, an actuator is a device which performs physical actions. Examples include reclosers and switches.

Alignment: Role that may execute in the field or control center. The responsibilities of the Alignment role are to monitor clock and determine when data has reached maximum allowable time lag, send data to data store as appropriate, buffer incoming data until all data has been received, aggregate incoming data for the current time period into a super-packet, interact with other roles and the PMUs to ensure the PMUs information is correctly configured and that the Alignment is correctly configured to receive the time-series data from PMUs, and interact with PMUs to control the data stream.

AMI: Automated or advanced metering infrastructure. Utility infrastructure with two-way communications for metering and associated systems allowing delivery of a wide variety of services and applications to the utility and customer.

Application: Within an electric power system, an application refers to software programs designed to manage and operate physical devices.

ASAP-SG: Advanced Security Acceleration Project for the Smart Grid. This group has been tasked with developing security profiles for the smart grid to accelerate the development of

[13] http://www.smartgridtoday.com/public/department40.cfm

security requirements & standards, requiring vendor products with built-in security, and provide tools for understanding failure mitigation and RFP language.

Authentication: The process of verifying the identity that an entity (e.g., person, or a computer system) is what it represents itself to be.

Authorization: Specifying access rights to IT or electric power system resources.

Begin State: is a step labeled "Start" that indicates where a use case begins.

Central Application: Back office applications which provide supervisory control over other applications and physical devices.

CERT: Computer Emergency Response Team

COBIT: Control Objectives for Information and related Technologies

Composable: Composability is a system design principle that deals with the inter-relationships of components. A highly composable system provides recombinant components that can be selected and assembled in various combinations to satisfy specific user requirements.

CRC: cyclic redundancy check

CSWG: Cyber Security Working Group. A sub-group formed under the Smart Grid Interoperability Panel to address the cyber security aspects of the Smart Grid Interoperability Framework.[14]

Data Store: Persistent repository of PMU data typically used for purposes of off-line analysis by WAMPAC and Non-WAMPAC applications.

Decision: a step in which a role makes a decision as to what step should follow. Flows coming from a decision step are labeled (often with "yes" or "no") to indicate the condition (relative to the decision) under which each flow should be followed; if a flow from a decision step is not labeled, then its condition is considered to be always satisfied. Typically only one flow out of a decision step is followed.

DHS: Department of Homeland Security

DOD: Department of Defense

DMZ: Demilitarized Zone

DNMTT: Data and Network Management Task Team

DNSSec: Domain Name System Security Extensions

DSL: Digital Subscriber Line

EMI: Electromagnetic Interference

EMS: Energy Management System

End State: a step labeled "End" that indicates the completion of the use case.

[14] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG

Environmental Data Interface: This is an interface that bridges the network used by applications and another network that provides access to sources of external data, including but not limited to weather, traffic, and other similar types of data. Data accessed via this interface is provided by an external data source.

ERP: Enterprise Resource Planning. Information system used to manage assets, financial resources, and human resources.

External Application: Applications that reside outside of the physical infrastructure of the demand response system.

External Data Source: A source of data that does not originate with the electric utility

Fault: A defect in a circuit which causes some level of equipment or system failure.

FERC: The Federal Energy Regulatory Commission. An independent agency that regulates the interstate transmission of natural gas, oil, and electricity. FERC also regulates natural gas and hydropower projects.[15]

Field Alignment: Alignment role that executes in the field

Field Application: A program role that executes in the field

Field Equipment: Equipment that produces phasor measurements used in wide-area applications is in scope.

FIPS: Federal Information Processing Standard. Publicly announced standards developed by the United States government.

Firewall: A network device designed to block or allow packets based on a pre-determined set of rules.

Firmware: Software embedded in a hardware device including in computer chips.

FMEA: Failure Modes and Effects Analysis

FPKI: Federal Public Key Infrastructure

FTP: File Transfer Protocol

FTPS: File Transfer Protocol over SSL. FTPS is an extension to the FTP protocol that adds application layer encryption via TLS and SSL. For "Secure FTP" or "SSH File Transfer Protocol", please see SFTP.

Gateway: A network management device that functions as the entry and exit point for a network segment.

GF: General Failure

GPS: Global Positioning System

GUID: Globally Unique Identifier

Historian: Acts as the WAMPAC data store to archive the time-series phasor data

[15] http://www.ferc.gov/about/about.asp

HSM: Hardware Security Module. An external physical type of secure crypto-processor targeted at managing digital keys, accelerating crypto-processes such as digital signings, and for providing strong authentication to access critical keys for server applications.

HTTP: Hyper Text Transmission Protocol

IDS: Intrusion Detection System. A passive monitoring system used to monitor network and/or system activity for malicious activity or policy violations.

IEC: International Electrotechnical Commission. A non-profit, non-governmental international standards organization that prepares and publishes International Standards for all electrical, electronic and related technologies – collectively known as "electrotechnology."

IED: Intelligent Electronic Device.

IEEE: Institute of Electrical and Electronics Engineers. An international non-profit, professional organization for the advancement of technology related to electricity.

Information Repository: Any location where the DM system stores data.

IP: Internet Protocol. The primary protocol used for network communications in packet-switched networks. This protocol is specifically used for node addressing and packet routing.

IPS: Intrusion Prevention System. An active monitoring system, similar to an IDS, used to monitor network and/or system activity for malicious activity or policy violations. Additionally, an IPS can terminate a connection upon detecting suspicious activity.

IPv4, IPv6: IP (above) version 4 is the fourth revision of IP based on RFC 791. IPv4 uses 32-bit addressing with a total of 4,294,967,296 (2^32) unique addresses. IPv6 is designed to supersede IPv4 and uses 128-bit addressing for a total of 2^128 unique addresses.

IR: Interagency Report

ISO: International Organization for Standardization

IT: Information Technology.

ITIL: Information Technology Infrastructure Library

LAN: Local Area Network. A network covering a small physical area.

LIC: Logical Interface Category

Link: is a step labeled with the name of some other use case. A link indicates that the activity of this use case is followed by the activity of the linked use case.

Load: Electric utility term for the infrastructure that uses the power the utility distributes -- such as homes, businesses, industry and in-the-field equipment -- thus, locating a power generation or storage device near load, for example, means putting it close to where the power will be used.

Local Phasor Gateway: a phasor gateway owned by the utility in question and is used to provide data to other utilities.

Mesh network: A network technology where each node or end-device can communicate with any nearby devices to create "smart" data routing that finds the most efficient path for data and can change the path when a node stops working.

MPLS: Multiprotocol Label Switching

Multi-factor Authentication: Similar to two-factor authentication, using two or more independent methods, something you have (token or smart card), something you know (password or passcode), and something you are (biometric), for authentication.

NASPI: North American SynchroPhasor Initiative

NDA: Non-Disclosure Agreement.

NERC: North American Electric Reliability Corporation. A self-regulatory, non-government organization which has statutory responsibility to regulate bulk power system users, owners, and operators through the adoption and enforcement of standards for fair, ethical and efficient practices.[16]

Network Equipment: Equipment implementing any intermediary function specifically aimed at facilitating or brokering exchange of synchrophasor data between organizations is in scope.

Network Segment: In networking, this is a network segment where all devices communicate using the same physical layer. Within WAMPAC, some switching devices may be used to extend the segment which is defined by the role of the devices in that segment.

NIST: National Institute of Standards & Technology. An office of the US Dept of Commerce, it handles standards and technology issued for the federal government including being tasked in the Energy Independence & Security Act of 2007 with heading up an effort to set interoperability standards for the smart grid industry.(www.nist.gov)

NOAA: National Oceanic and Atmospheric Administration

Non-WAMPAC Application: This is a utility operated application that does not rely critically on time-synchronized phasor measurements for its primary task.

NTP: Network Time Protocol

Open SG: Open Smart Grid users group – part of the UCA International users group.[17]

OMG UML: Object Management Group

Operations Center Equipment: Equipment in the Operations or Control Center that internalizes and processes phasor data in the course of performing synchrophasor application functionality is in scope.

Optional flows: An optional flow indicates a flow that may or may not always happen in a use case.

OWASP: Open Web Application Security Project

Phasor Gateway: This is software that bridges one or more utility networks for the purpose of exchanging phasor measurement data.

[16] http://www.nerc.com/page.php?cid=1

[17] http://osgug.ucaiug.org/org/default.aspx

Perimeter Equipment: Equipment implementing functions that bridge organizational boundaries to facilitate synchrophasor applications is in scope.

Phasor: A measurement of phase angle and magnitude of voltage

Phasor Manager: This is standalone software or a module within other software that permits the management of one or more phasor measurement units.

PKI: Public Key Infrastructure

PMU: Phasor Management Unit. This is a sensing and reporting device that measures magnitude and phase angle of a voltage signal at fixed points in time.

PMU ID: Phasor Management Unit Identifier

Private Network: In networking this refers to networks using private IP space as defined by RFC 1918. Within electric power systems this refers to networks owned, operated or controlled by the utility or retail electric provider.

Public Network: In networking this refers to networks using publicly-addressable IP space which can be routed via the Internet. Within electric power systems this refers to networks not owned, operated, or controlled by the utility or retail electric provider.

QoS: Quality of Service. In an IP network QoS provides guaranteed resource reservation to provide different priorities to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

RC: Reliability Coordinator, as defined by NERC[18]

RF: Radio Frequency. Used as a generic term in many industries to describe radio signals used for networking and even those signals that cause interference.

RFC: Request for Comments

RPN: Risk Priority Number. A measurement used when assessing risk in the FMEA process, which equals (Severity x Occurrence x Detection).

RFP: Request for Proposal.

RTO: Regional Transmission Organization

RTU: Remote Terminal Unit. A unit that collects data from electrical devices, such as meters, in real time.

SAMATE: Software Assurance Metrics and Tool Evaluation

SCADA: Supervisory Control and Data Acquisition. A system used by power utilities to gather data from and issue commands to devices in the field.

SCP: Secure Copy. SCP is an extension to the SSH protocol to implement a secure replacement for Remote Copy (RCP).

SCL: Substation Configuration Language[19]

[18] Need reference

SFTP: SSH File Transfer Protocol, also known as Secure FTP. STFP is an IETF extension to the Secure Shell (SSH) protocol to implement a secure replacement for FTP. For "FTP over SSL", please see FTPS.

SG Security: Smart Grid Security working group within Open SG.

SGIP: Smart Grid Interoperability Panel[20]

Sensor: A sensor is a device that collects information such as voltage, temperature, or device status.

Smart grid: The utility power distribution grid enabled with computer technology and two-way digital communications networking. The term encompasses the ever-widening palette of utility applications that enhance and automate the monitoring and control of electrical distribution networks for added reliability, efficiency and cost effective operations.

SOC: Security Operations Center. Often incorporated with the network operations center, but designed to monitor security logging and security-related events.

Step: indicates the activities performed by a role during a use case

Substation: An electrical substation is a subsidiary station of an electricity generation, transmission and distribution system where voltage is transformed from high to low or the reverse using transformers. Electric power may flow through several substations between generating plant and consumer, and may be changed in voltage in several steps.[21]

SVC: Static VAR Compensators

SVP: Synchronous Vector Processor

Swimlane: a horizontal region used to represent the activities of a particular role

Synchrophasor: A precisely time-stamped measurement of the AC waveform where the measurements are represented as a magnitude and angle relative to a full cycle of the wave form

TCP, TCP/IP: Transmission Control Protocol. Usually written with internet protocol as TCP/IP and the two make up the suite of protocols that are used to communicate via the Internet

TLS: Transport Layer Security

TO: Transmission Owner, as defined by NERC

TPM: Trusted Platform Module. The name of a published specification detailing a secure crypto-processor that can store cryptographic keys that protect information, as well as the general name of implementations of that specification, often called the "TPM chip" or "TPM Security Device"

---

[19] As defined in IEC 61850

[20] http://www.nist.gov/smartgrid/

[21] http://en.wikipedia.org/wiki/Electrical_substation

Two-Factor Authentication: The act of using two independent authorization methods. Examples are mixing something you have (token or smart card), something you know (password or passcode), and something you are (biometric).

UCAIug: UCA International Users Group. A not-for-profit corporation focused on assisting users and vendors in the deployment of standards for real-time applications for several industries with related requirements. The Users Group does not write standards, however works closely with those bodies that have primary responsibility for the completion of standards (notably IEC TC 57: Power Systems Management and Associated Information Exchange).[22]

UML: Universal Modeling Language

UPS: Universal Power Supply

URL: Universal Resource Locator

USB: Universal serial bus, a cable system with rectangular plugs used to connect a wide variety of devices to computers and computer peripherals.

VLAN: Virtual Local Area Network. A method of segmenting and routing traffic between devices on an IP network so that they communicate as if they were attached to the same broadcast domain, regardless of their physical location.

VOIP: Voice over Internet Protocol.

VPN: Virtual Private Network. A VPN encapsulates data transfers between two or more networked devices not on the same private network so as to protect the transferred data from other devices on one or more intervening local or wide area networks.

WAMPAC: Wide-Area Monitoring, Protection, and Control

WAN: Wide Area Network. A computer network that covers a broad geographic area.

WASA: Wide-area Situational Awareness

WECC: Western Electricity Coordinating Council

WiFi: Wireless Fidelity -- a standard for sending and receiving data -- such as in a home or small office network or LAN (or even an entire city). The standard includes a number of sub-standards under the IEEE's 802.11 standards.

[22] http://www.ucaiug.org/default.aspx

Appendix E: References

ASAP-SG. (2009, December 14). Security Profile Blueprint. Knoxville, Tennessee, United States of America. Retrieved 1 28, 2010, from Open Smart Grid - OpenSG > SG Security: http://osgug.ucaiug.org/utilisec

U.S. Department of Homeland Security. (2010, March). *Catalog of Control Systems Security: Recommendations for Standards Developers*. Arlington, Virginia, United States of America. http://www.us-cert.gov/control_systems/pdf/Catalog%20of%20Control%20Systems%20Security%20-%20Recommendations%20for%20Standards%20Developers%20June-2010.pdf

BSI Group, Department of Trade and Industry, United Kingdom. *BS 7799 Best practices for Information Security Management (1998) and BS 7799 Part 2: Information Security management Systems – Specification with Guidance for use.*

Control Objectives for Information and related Technologies: http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

Hinden, R. and Haberman, B. (2005). *RFC 4193: Unique Local IPv6 Unicast Addresses*

Institute of Electrical and Electronics Engineers, Inc. (2003). Standards [as listed below], New York, New York.

IEEE Std 1613-2003, Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations

IEEE C37.118 Synchrophasor Protocol

International Electrotechnical Commission. Standards [as listed below]. Geneva, Switzerland

IEC 61850 "Communication Networks and Systems in Substations"

IEC 61850-90-5 "Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118" (Draft Technical Specification)

IEC 62351 "Information Security for Power System Control Operations"

International Standard Organization *ISO/IEC 27000:2009. Information technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary.* Geneva, Switerzland

Quanta Technology LLC, *Phasor Gateway Technical Specification for North American Synchro-Phasor Initiative Network (NASPInet)*, May 29, 2009, page 1-4 (PDF page 11). Available at: http://www.naspi.org/naspinet.stm

Quanta Technology LLC, *Data Bus Technical Specification for North American Synchro-Phasor Initiative Network (NASPInet)*, May 29, 2009, page 1-4 (PDF page 11). Available at: http://www.naspi.org/naspinet.stm

Seacord, Robert C., (2008, October). *The CERT C Secure Coding Standard*. Addison-Wesley.

National Institute of Standards and Technology, Department of Commerce, United States of America. *Interagency Report 7628: Guidelines for Smart Grid Cyber Security*. Gaithersburg, Maryland.

National Institute of Standards and Technology, Department of Commerce, United States of America. *Special Publication SP 800-53: FPKI Security Controls for PKI Systems and SP 800-53A: Assessment Guidance for Security Controls in PKI Systems.* Gaithersburg, Maryland.

National Institute of Standards and Technology, Department of Commerce, United States of America. Federal Information Processing Standards (FIPS) [as listed below, available at http://csrc.nist.gov/publications/PubsFIPS.html]. Gaithersburg, Maryland.

OMG Unified Modeling Language (OMG UML), UML Superstructure Specification, Version 2.3. Online at http://www.omg.org/spec/UML/2.3/Superstructure/PDF/

FIPS 140-2 Security Requirements for Cryptographic Modules, May 2001

FIPS 186-3 Digital Signature Standard (DSS), June 2009

FIPS 112 Password Usage, May 1985

FIPS 180 Secure Hash Standard, October 2008

North American SynchroPhasor Initiative. Data and Network Management Task Team. http://www.naspi.org/resources/dnmtt/dnmttresources.stm

OWASP: Open Web Application Security Project Development Guide. https://www.owasp.org/index.php/Guide_Table_of_Contents

Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., Lear, E. (1996). *RFC: 1918:Address Allocation for Private Internets*