EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Wide Area Monitoring, Protection, and Control Systems (WAMPAC)

Standards for Cyber Security Requirements

DRAFT

October 26, 2012

National Electric Sector Cybersecurity Organization Resource (NESCOR)

Wide Area Monitoring, Protection, and Control Systems (WAMPAC)

Standards for Cyber Security Requirements

DRAFT, Oct 26, 2012

Primary Authors:
Mladen Kezunovic, XpertPower Associates
Tomo Popovic, XpertPower Associates

Other Contributors:
Carol Muehrcke, Adventium Enterprises
Brian Isle, Adventium Enterprises
Steven Harp, Adventium Enterprises
Elizabeth Sisley, Calm Sunrise Consulting
Sami Ayyorgun, Applied Communication Sciences

Reviewers:
Annabelle Lee, EPRI
NESCOR Team 2 Members and Volunteers

Principal Investigator:
Annabelle Lee, EPRI

The research was paid for by the Department of Energy (DOE) under the NESCOR grant DE-OE0000524.

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

Revision history

version	date	changes
0.1	2012.07.09	Initial draft for internal XPA review
0.2	2012.07.20	Initial draft for WAMPAC Team review
0.3	2012.07.27	Draft with the comments from the WAMPAC Team incorporated
0.4	2012.07.28	Updated draft from XpertPower Associates staff (XPA)
0.5	2012.07.29	Draft with formatting feedback and XPA staff updates incorporated
1.0	2012.07.30	Draft submitted to EPRI (WAMPAC team members feedback incorporated)
1.2	2012.08.14	Draft revised by EPRI
2.0	2012.10.26	Draft revised by Mladen Kezunovic and EPRI

EXECUTIVE SUMMARY

The National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group 2 (TWG2) has been examining issues of cyber security requirements and coverage in related standards. As a part of that effort, several domain areas of interest were identified. This report summarizes findings related to the cyber security requirements as reflected in the Wide Area Monitoring, Protection, and Control (WAMPAC) standards. The findings are discussed in the context of the recently published WAMPAC Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) and the National Institute of Standards and Technology Interagency Report (NISTIR) 7628 reports, on-going WAMPAC related standards development, existing cyber security standards, and on-going cyber security reviews of standards conducted through the Smart Grid Interoperability Panel (SGIP).

This document sets the stage by discussing some general WAMPAC solution characteristics relevant for cyber security considerations, and summarized as follows:

- Large-scale deployment of WAMPAC systems is recent, with major deployment projects initiated through DOE funding in the last few years and still on-going. There is not yet a mature and consistent cyber security approach defined.
- WAMPAC solutions are quite diverse in their use of measurement units, solution architecture, communications, visualization tools, and underlying applications. This leads to different designs, and hence differing cyber security requirements.
- An assessment of a representative list of WAMPAC failure scenarios and their related vulnerabilities has been included in a NESCOR TWG1 report. This list was developed in a bottom-up manner. A top-down analysis is not currently planned by TWG1, but would significantly expand the failure scenario list.
- A plan for WAMPAC cyber security penetration testing has been defined by NESCOR TWG3, and at this stage has been specified at an initial level. A systematic test process based on a comprehensive test plan and defined metrics is still to be developed.

In the context of the above assessment of WAMPAC solution development, a review of related standards reveals the following status:

- Development of WAMPAC related standards was rather slow until large-scale deployment projects were contracted. At that time, IEEE, SGIP, and the North American Synchrophasor Initiative (NASPI) joined forces to accelerate WAMPAC development.
- Several WAMPAC standards were developed on a fast track, and several new standards are either in the final approval or development stage. During this standards development organization (SDO) process, guidelines for a consistent approach to cyber security requirements across the standards were not developed.
- Most of the WAMPAC standards do not mention any cyber security requirements. Some that do mention cyber security but at a very generic level, suggesting that such issues should be addressed by separate standards focused on cyber security.

- The SGIP reviews of completed standards are focused on individual standards, and do not make an assessment of the standards in the context of an end-to-end solution. Hence the reviews do not address cyber security harmonization across standards.
- The following specific recommendations for future work are derived from the mentioned findings:
    - The published version of NISTIR 7628 and its current revision, related to the WAMPAC representation in the "spaghetti" diagram, needs to be further refined to achieve the granularity shown in some of the WAMPAC "swim lane" diagrams in this report. An initial mapping is included in this report.
    - Future revisions of the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards should consider defining cyber security requirements for WAMPAC implementations, in which the security of measurement devices takes on significant importance, and where such devices may be performing multiple functionalities at different impact levels. The latter case currently is not explicitly called out by the current or proposed NERC CIP standards.
    - WAMPAC cyber security (as well as interoperability) requirements need to be defined in the overall application context, augmenting the analysis of individual standards currently underway in the community. The end-to-end implementation of WAMPAC requires harmonization across all involved standards.
    - The cyber security WAMPAC policy may have to extend beyond a single enterprise when WAMPAC systems are used across multiple organizations, which requires broader stakeholder participation when deciding how to implement a policy.
    - Current WAMPAC related standards are addressing cyber security aspects of data management and communication issues, but the issues associated with an attack that affects the time reference signal are not fully explored.
    - Penetration testing of WAMPAC solutions for cyber security vulnerabilities is currently ad-hoc. WAMPAC penetration test plans would benefit from a systematic methodology and defined metrics for test performance assessment.
    - The certification process for interoperability of WAMPAC solutions should define clear test procedures for verifying cyber security interoperability for components of WAMPAC end-to-end solutions.
    - Identifying those WAMPAC cyber security policies, requirements, and tests that can be addressed by commonly employed methods, and those that cannot, due to the unique characteristics of this domain, will be a particularly important contribution.

This report has identified some critical WAMPAC cyber security issues that need further attention as WAMPAC solutions mature and become more widely used. In that sense the report

has outlined the elements of a more comprehensive study of the cyber security gaps and solutions for WAMPAC systems.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION AND SCOPE

The objective of this report is to survey the main standards guiding implementation of Wide Area Monitoring, Control, and Protection (WAMPAC) systems and to assess the cyber security coverage in the standards. The report presents a few WAMPAC implementation scenarios, where the standards are used for end-to-end applications. In such scenarios, the gaps regarding cyber security aspects of the entire solution are addressed. Suggestions for how to bridge the gaps in future designs are outlined at the end.

The report is organized into six main sections. The Background (Section 2) explains what the WAMPAC design is and what is meant by end-to-end solutions. WAMPAC design core elements that include data acquisition, synchronized sampling, variety of communication options, applications and end-user visualization options, are outlined next.

Section 3 argues for the importance of interoperability as it relates to the uniqueness of future developments in WAMPAC systems. The uniqueness drives the choice of the design approach, a "spiral" model, suggesting that various parts of WAMPAC end-to-end solutions will be exchanged continuously, but at different times, as the technology matures. This is illustrated with a few implementation scenarios, where it becomes clear from the number of interfaces between various WAMPAC parts why interoperability is highly desirable.

Section 4 includes an assessment of cyber security issues and requirements in selected standards used in WAMPAC implementations. The focus of the discussion is mostly on the standards that are being currently considered for inclusion in the SGIP Catalog of Standards (CoS). The status of the cyber security reviews for the CoS is discussed, followed by documentation of some selected issues in major standards such as IEC 61850, DNP 3, IEC 61970 and newly issued addition IEC TR 61850-90-5.

Section 5 provides suggestions of how the NESCOR work may be integrated across domains, including WAMPAC. Comments are made about the need for WAMPAC considerations in all three Technical WGs, reflecting of the current status of WAMPAC considerations in the draft documents published by TWG 1 and TWG 3.

The report ends with Conclusions (Section 6) that summarize identified gaps and provides recommendations for next steps.

Appendix A includes a review of standards.

2. WAMPAC BACKGROUND

2.1 What is WAMPAC?

The Wide Area Monitoring, Protection, and Control (WAMPAC) concept is described in a recent document developed by an informal industry group convened by NIST [1]. This group advised the Transmission and Distribution (T&D) Domain Expert Working Group (DEWG) in the early stages of the Smart Grid Interoperability Panel (SGIP) activity, coordinated by the National Institute of Standards and Technology (NIST). WAMPAC systems constitute a suite of different system solutions aimed at meeting various wide-area application requirements. The solutions consist of various combinations of common design elements: Intelligent Electronic Devices (IEDs) capable of collecting samples of input waveforms and calculating phasors, sources for a high precision time synchronization reference, various phasor data concentrators, communications, applications, and visualization tools for data presentation. However, the solution designs are not necessarily common across different application domains.

A few properties of the WAMPAC system are shown in Figure 1: WAMPAC Concept. The blue dots in this figure represent measurement points. The callouts represent waveforms sampled synchronously using GPS reference clock and used to calculate synchrophasors, sent to a connecting network. The measurements are collected over a wide area, in the Eastern and Western power grid interconnections, and in ERCOT in Texas, mostly at the transmission level at this time. In the future such an infrastructure may extend to the distribution level as well [2].

The phasor measurements, also called synchrophasors, are provided by variety of types of IEDs, presently most commonly by standalone Phasor Measurements Units (PMUs), shown in Figure 1. While roughly 1000 PMUs are expected to be installed in the USA grid by 2015, there are many other IEDs such as Digital Protective Relays (DPRs), Digital Fault Recorders (DFRs), and Digital Disturbance Recorders (DDRs) that may also provide PMU functionality through a firmware upgrade. As an example, an estimated 8000 DPRs in Texas alone may be enabled to provide PMU functionality through a simple firmware upgrade. Each measurement IED receives a clock signal from the Global Positioning Systems (GPS) satellites through a GPS receiver; hence all the measurements are synchronized to the same reference clock signal. The time signal may also be distributed through the communication network if the GPS receiver resides at a different location than the location of the measurement IED.

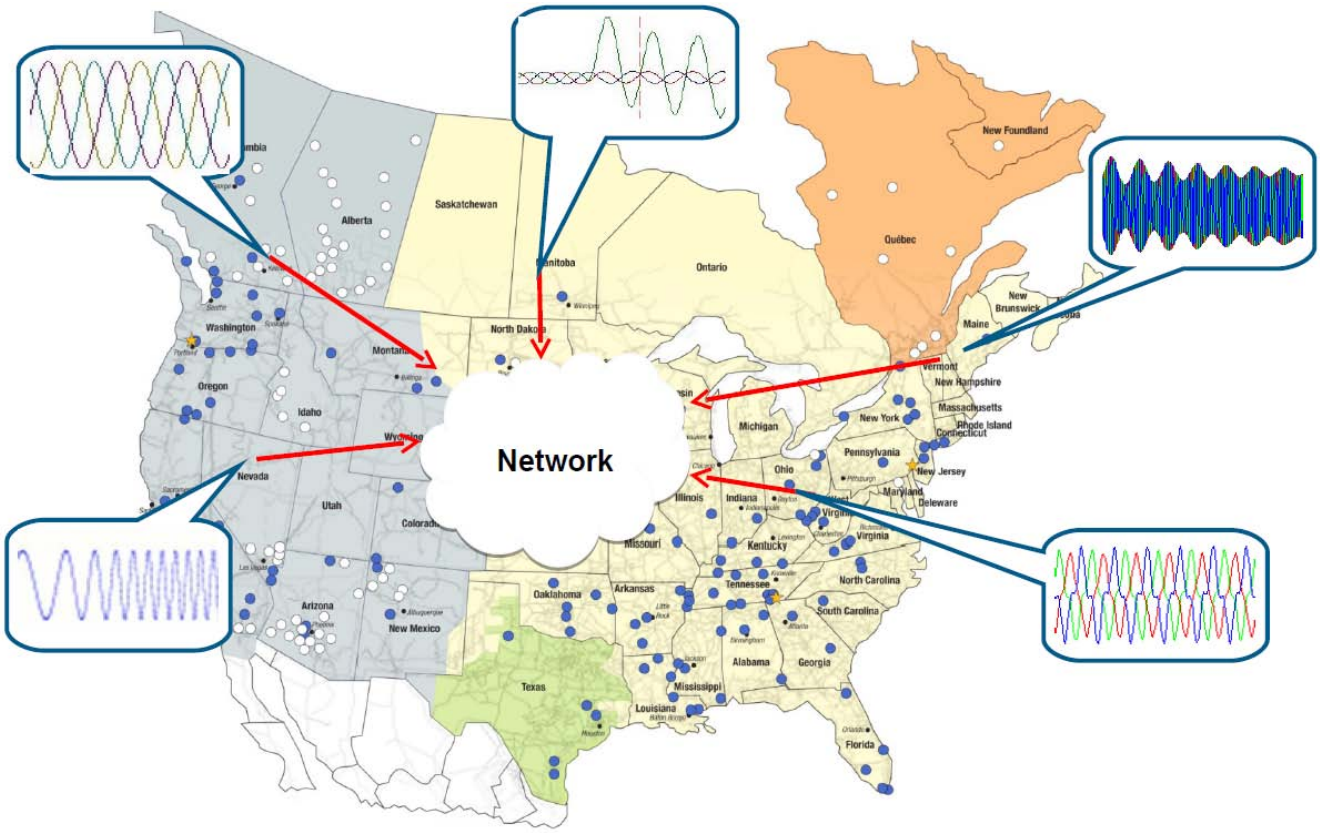


Figure 1: WAMPAC Concept

What characterizes the WAMPAC systems, that are not common to any other measurement infrastructure used in the power grid, are the following:

- The design has high sensitivity to the accuracy of the clock (time) reference supplied through either a physical GPS receiver placed in the substation next to the IED, or a "virtual GPS receiver" located remotely from the substation. The cyber security requirements need to cover both options.
- The end-to-end solutions are typically implemented using hardware/software components acquired from multiple vendors. Hence there is a need for consistency in a cyber security solution design across products from different vendors.
- WAMPAC solutions are used across different personnel groups within a given utility company, as well as across different enterprises such as transmission system operator (TSO) and independent system operator (ISO). This requires consistent cyber security policies across multiple legal entities (enterprises) and perhaps Federal/state jurisdictions.

2.2 End-to-End Solution

An end-to-end WAMPAC solution will span across multiple devices/software modules. As an example, Figure 2 shows a variety of IEDs in a substation collecting field measurements of analog (A) and status (S) signals. The IEDs commonly used in a substation are: Fault Locators (FL), Digital Fault Recorders (DFRs), Circuit Breaker Monitors (CBMs), Digital Protective Relays (DPRs), Phasor Measurement units (PMUs), Remote Terminal Units (RTUs), and sequence of Event recorders (RTUs). Thus an end-to-end WAMPAC solution relies on a number of technologies including synchrophasor technology.

The nomenclature used for the various data categories (operational, non-operational, and situational awareness) designates when and how the data is collected and utilized, and the purpose it is serving. Non-operational data is typically collected when IEDs are triggered by disturbances such as faults and power quality events. These data are analyzed off-line by personnel with specialized expertise focused on interpreting the cause-effect relationship between events and equipment operation. Operational data is collected through regular scans (typically every few seconds), and is used by system operators for monitoring system behavior during normal and emergency situations. Situational awareness data has been recently introduced. It supplements the operational data and is used to track events that are potentially dangerous for power system operation since they may unfold into cascading faults or stability violations.

An end-to-end solution involves not only collecting IED data, but also quite often merging it through integrated solutions and interfacing it to the Energy Management System (EMS). Figure 2 illustrates such an end-to-end implementation that brings together data from multiple IEDs to enhance the operational data.

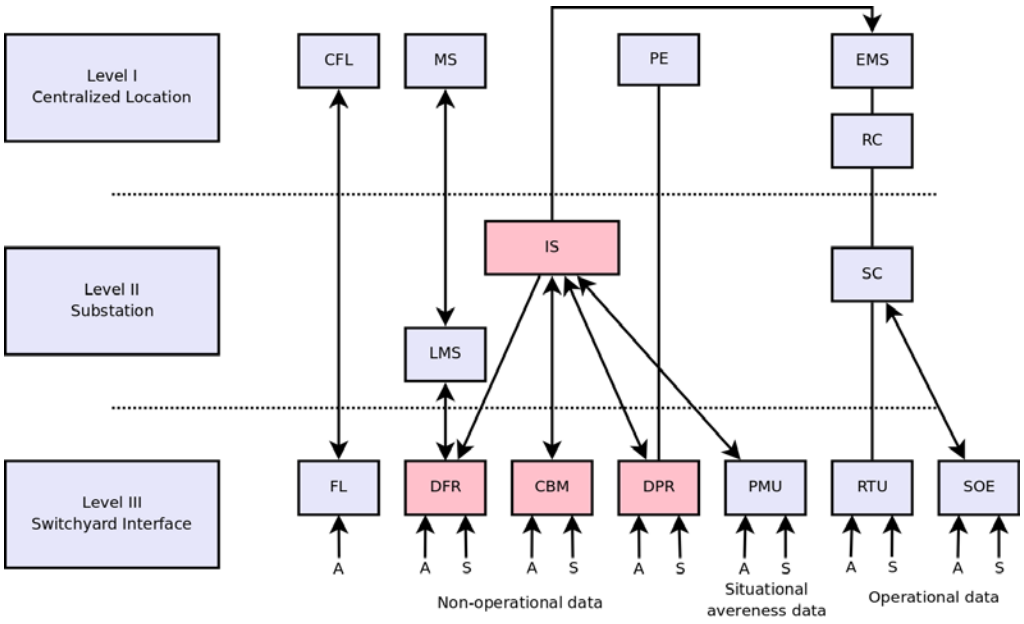


Figure 2: Typical End-to-End Solution with Non-operational Data Highlighted

2.3 Core Elements of WAMPAC Design

The core elements of WAMPAC Design are shown in Figure 3, Figure 4, and Figure 5. Figure 3 shows a typical phasor measurement IED, and Figure 4 shows how such IEDs may be connected in a substation.

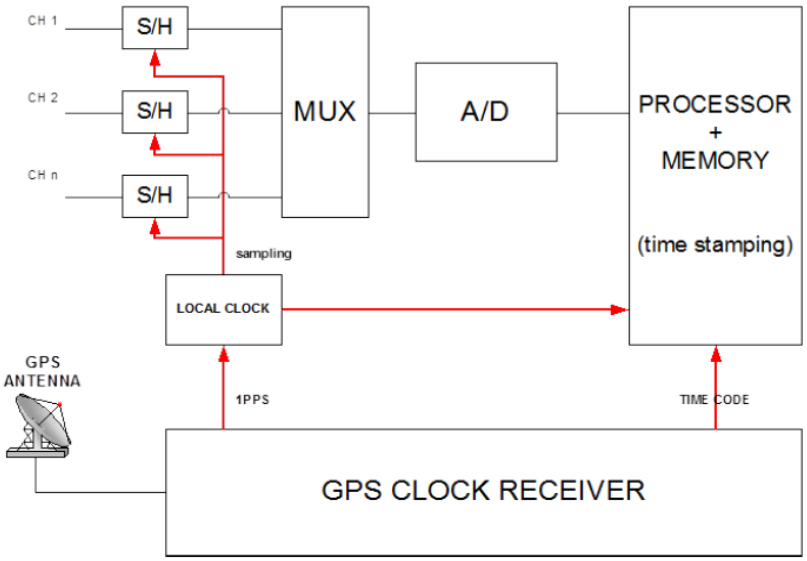


Figure 3: Typical WAMPAC Measurement Device Architecture

The phasor measurement device design shown in Figure 3 describes a distinct feature of the WAMPAC IED, in which it receives a clock synchronization signal (Pulse per second-PPS) and the time code, both provided through GPS receiver. Those timing signals may also be received from a GPS receiver located remotely through a communication network.

Figure 4 shows a typical substation layout where multiple IEDs are interconnected for the purpose of distribution of the GPS receiver signals. Several options for local distribution of GPS receiver timing signals are possible: existence of multiple GPS receivers, some stand-alone and some integrated in IEDs, as well as a variety of scenarios for interconnections. Distribution of the GPS clock signal may happen in the substation control house only, or in some instances between the control house and the switchyard, or between the control house and a remote location where the GPS receiver is placed. The local substation connection between the GPS receiver and phasor measurement IEDs is established using IRIG-B [3], while the connections between the control house and the switchyard may use specialized fiber optic or wireless solutions. The connection to a remote GPS is done through a communication network using IEEE 1588 [4] and its power system application profile IEEE PC37.238 [5].

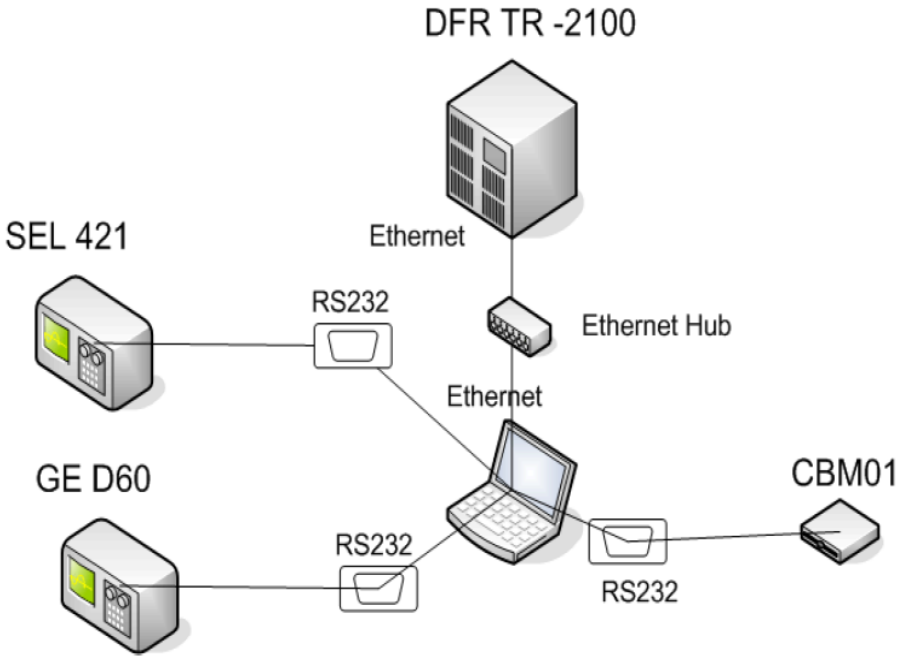


Figure 4: Typical WAMPAC IED GPS Interfaces in a Substation Solution

Besides local connections, a WAMPAC end-to-end solution requires communication among substations, as well as communications between substations and a control center, as shown in Figure 5 and discussed in [1].

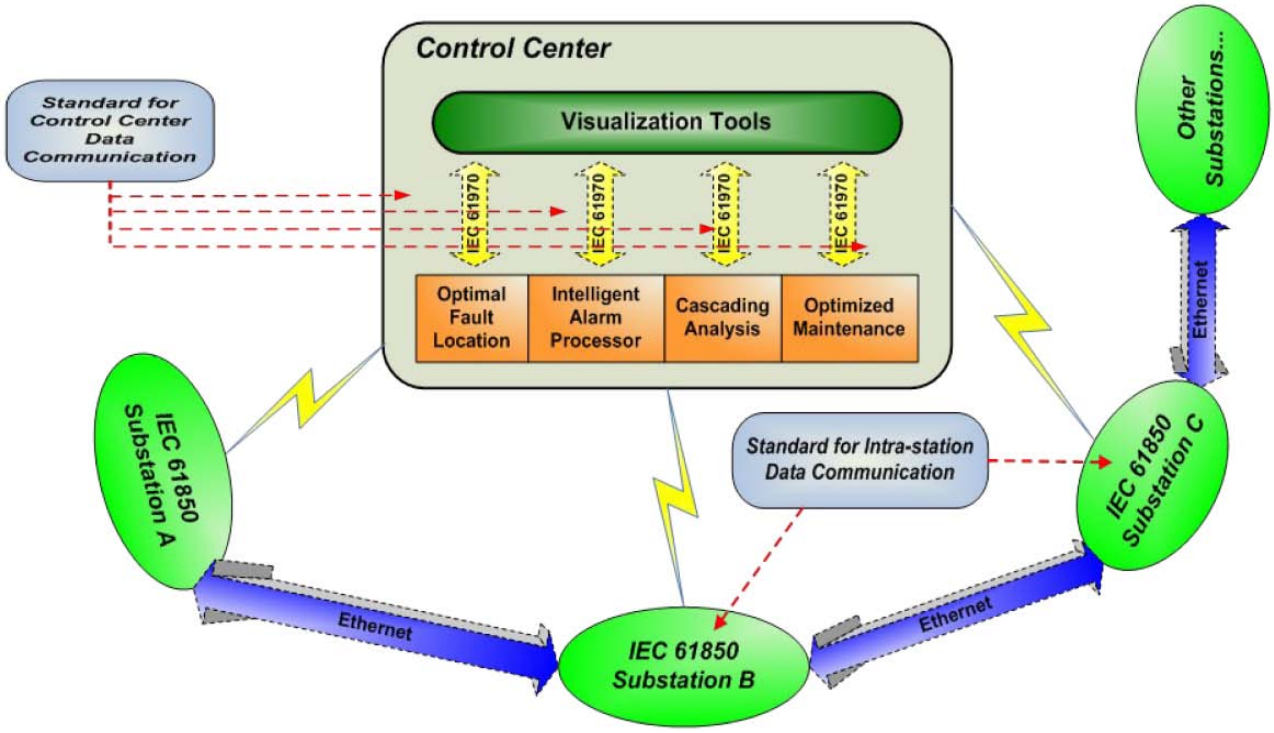


Figure 5: Typical WAMPAC System Solution

Many different standards may be used for such communications but IEC 61850 and DNP3 are emerging as standards of choice [6]. Another important standard for data concentration is IEC 61970 [7], which is used at the control center level to assure consistent presentation of all the data collected by substation IEDs. Due to the efforts in both substation and control center professional communities aimed at defining data in a consistent format, two different standards emerged over a period of time (IEC 61850 and IEC 61970), which need to be harmonized for the purpose of end-to-end solutions [8].

2.4 Future Developments

Multiple trends affecting cyber security issues are expected to emerge as the large-scale WAMPAC systems are developed and deployed:

- Currently PMUs are typically used to support situational awareness applications. However, in the future they may support core reliability functions. Further, they may support these functions for facilities for which NERC CIP would classify associated BES cyber systems as "high impact." When this happens, the determination, according to the most current NERC CIP Version 5 standards, that field measurement equipment is never classified and protected as "high impact," merits reconsideration[1].

- As WAMPAC applications expand beyond situational awareness into the protection and control realm, other performance criteria such as latency and trustworthiness will become prevailing considerations. Specifically, design of System Integrity Protection Schemes

[1] The NERC CIP V5 standards are currently under review and revision.

(SIPS) will require cyber security solutions that do not introduce significant delay or additional risks.

- WAMPAC systems consist of different building blocks supplied by different vendors, hence the cyber security solutions will have to be consistent across the different products, and will have to be sustainable as the products get upgraded, exchanged with products from other vendors, or as WAMPAC solutions expand in the future.

- WAMPAC applications vary in their importance for power system operation. The fact that some are used for critical applications will drive development of their cyber security requirements, which will have to meet minimum latency or other quality of service (QoS) requirements. The WAMPAC solutions are used to act when other systems cannot provide required performance, hence the WAMPAC solution has to maintain its superior performance under all circumstances not hindered by the cyber security design features.

- Future applications will require that data from different substation IEDs be merged, which creates the need to identify when the data is integrated from IEDs that are part of an external critical infrastructure, not under the control of the organization using the data. The types of integrity controls applied and trust afforded to this external data may need to be different than for data whose origin is under the control of the organization using it.

3. INTEROPERABILITY CONSIDERATION

3.1 End-to-End Data Flow

The end-to-end data flow in a typical WAMPAC solution is shown in Figure 6. From the figure it is obvious that WAMPAC solutions consist of many diverse parts: Phasor Measurement IEDs (PMU, DPR, DFR, etc.), Phasor Data Concentrators (PDCs), and many communication, data management and visualization servers acting as gateways, data historians, and data analytics engines. To assure the system meets future interoperability requirements one has to anticipate how the future expansion of the system may unfold.

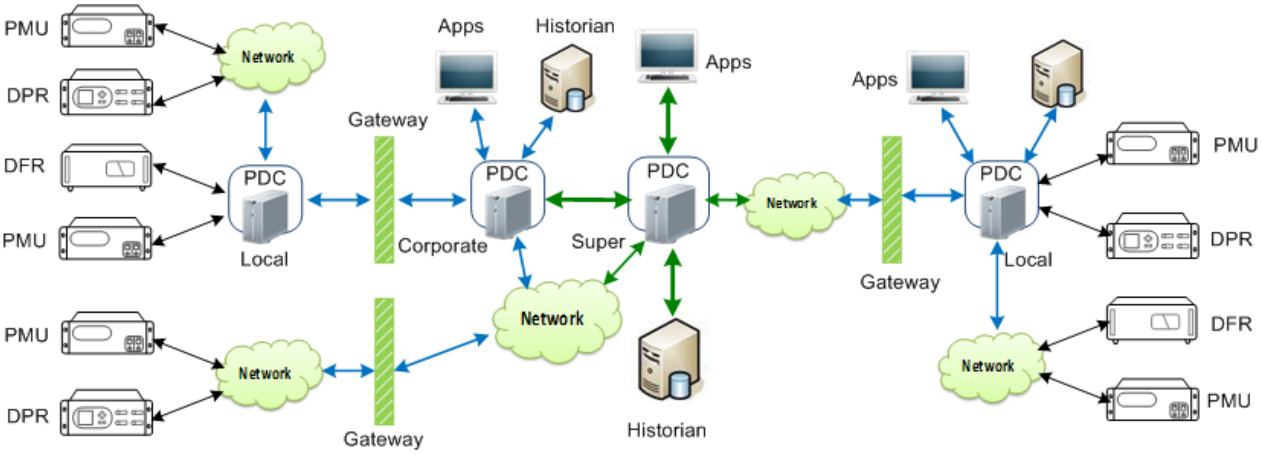


Figure 6: WAMPAC End-to-End Data Flow

3.2 Spiral Life Cycle

As mentioned before, WAMPAC systems are implemented using products from different vendors. As a consequence, it is expected that future development of WAMPAC systems will require exchange of obsolete components at irregular intervals, since the system consists of different types of components with vastly different life cycles.

Hence it is likely that the typical design cycle that includes the stages such as specification, procurement, commissioning, deployment, and decommissioning will repeat in a continuous fashion, leading to another cycle of the same steps, traditionally called a “spiral” design cycle in the Software Engineering field [9]. This will occur due to the interconnection of the components, which will require not only the repeat of the design cycle each time a component is substituted by a new design or new product but also a repeat of the system design cycle since new upgrades will affect or be affected by the rest of the system design.

“The spiral model is based on continuous refinement of key products for requirements definition and analysis, system and software design, and implementation (the code). At each iteration around the cycle, the products are extensions of an earlier product. This model uses many of the same phases as the waterfall model, in essentially the same order, separated by planning, risk assessment, and the building of prototypes and simulations.” [10] and [11].

This lifecycle fits well in environments with changing hardware as well as changing software, as shown in Figure 7.

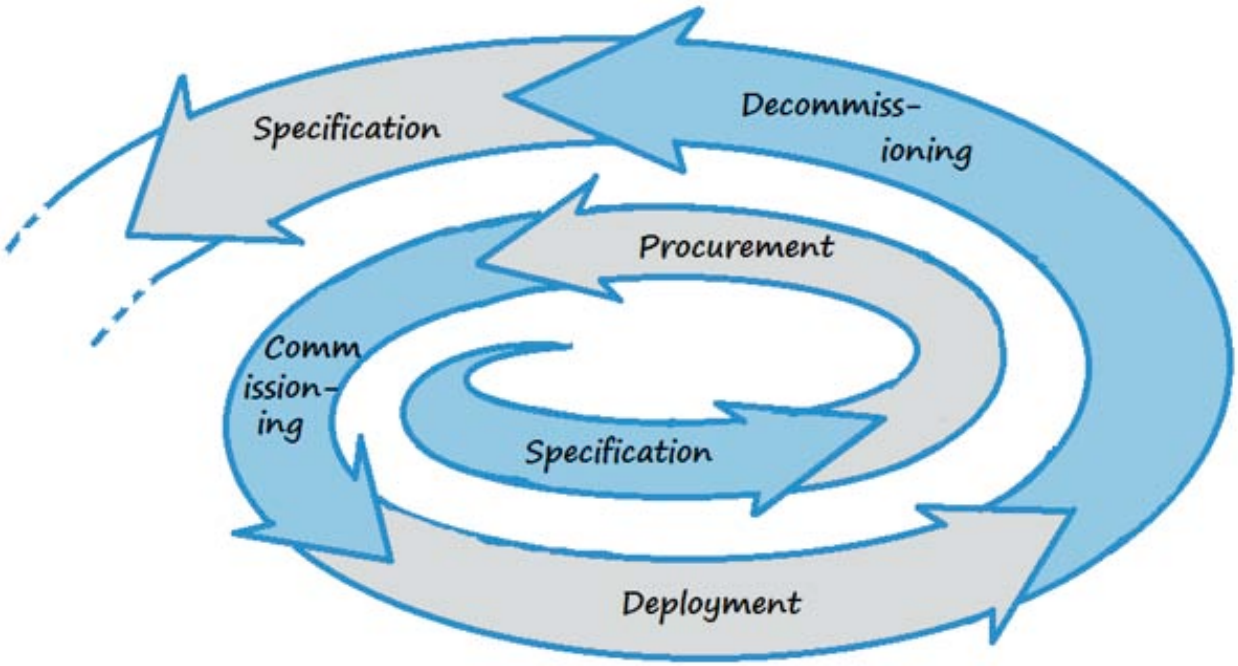


Figure 7: Spiral Lifecycle of WAMPAC Solutions

3.3 Scenarios in WAMPAC implementation

The most likely scenario of WAMPAC implementation is shown in Figure 8 and Figure 9 (a swim lane diagram), where WAMPAC solutions integrate with SCADA systems as well as systems providing non-operational data. The refinements include distinguishing between devices, applications, stored data, and user interfaces, all in relevant locations. The hierarchy of connections are documented as “many to one” where aggregation is applicable and the many optional integrations are clarified with connection points (A) and (B). These WAMPAC scenario diagrams provide more detail, specifying additional device details, data flow, locations, and specific applications not captured in the NISTIR 7628 diagrams. The Voltage Management scenario is used as an application example.

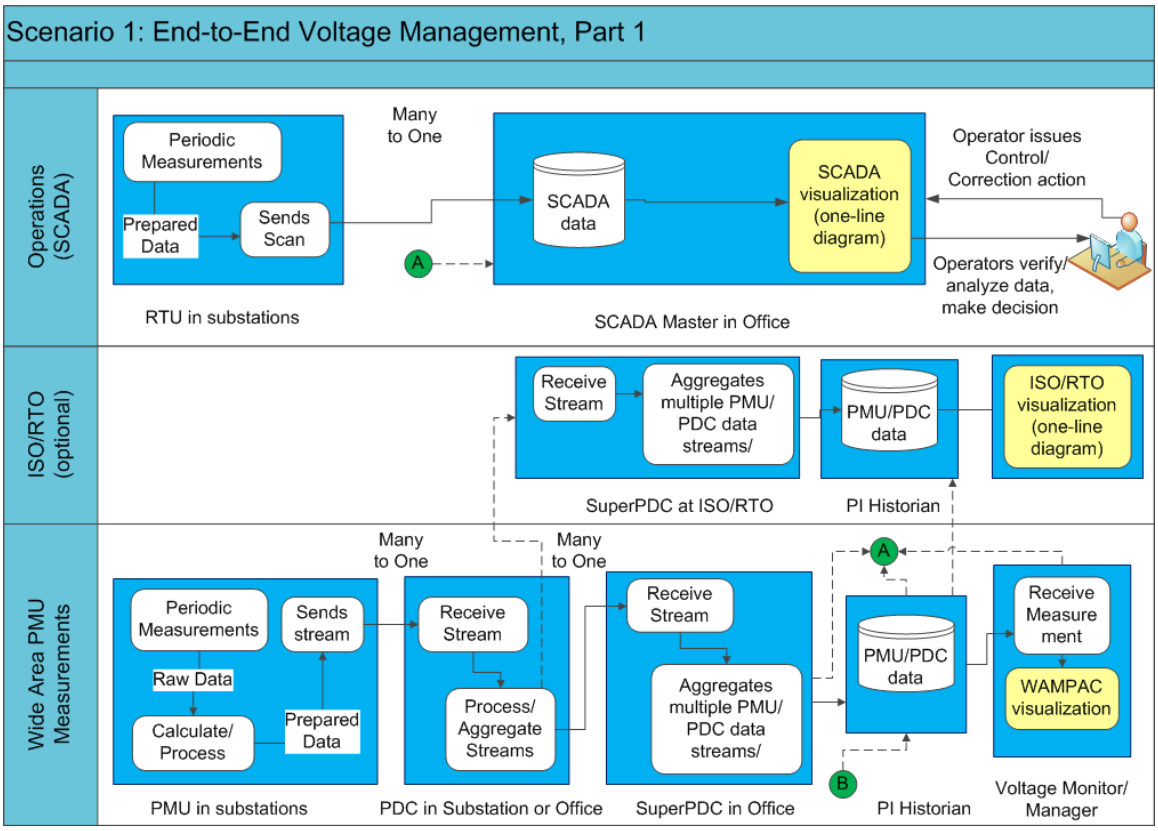


Figure 8: WAMPAC System Interfacing with other Measurement Infrastructures

Figure 8 and Figure 9 are subsets of the same scenario, divided here for readability.

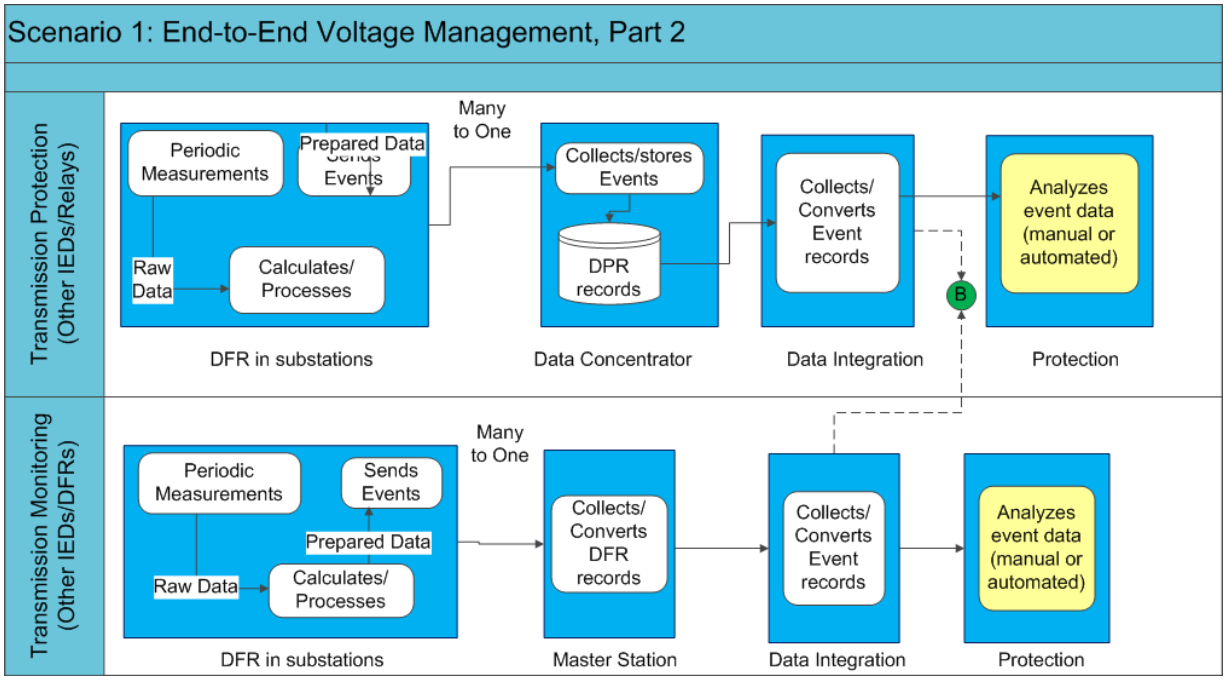


Figure 9: WAMPAC System Interfacing with other Measurement Infrastructures

The Application and Device actors in the WAMPAC Scenario (Figure 8 and Figure 9) that map to the NISTIR 7628 actors are as follows:

Table 1: Actor Mapping between NISTIR 7628 and WAMPAC Swimlanes

NISTIR 7628 Actors	WAMPAC Actors
#31 ISO/RTO Operations	ISO/RTO *swimlane:* SuperPDC, PI Historian, ISO/RTO Visualization
#37 Transmission SCADA	Operations (SCADA) *swimlane*: SCADA Master, SCADA Visualization, PI Historian
#39 Wide Area Measurement Systems	Wide Area PMU Measurements *swimlane*: PDC, SuperPDC, PI Historian, Voltage Monitor/Manager Application
#45 Phasor Measurement Unit	PMU
#46 Transmission DFR/IED	DFR
#47 Transmission RTU	RTU
#49 Transmission Engineering Systems	Transmission Protection *and* Transmission Monitoring *swimlanes*: Master Station, Data Concentrator, Data Integration, Protection

Figure 10 shows how WAMPAC systems feed an Energy Management System (EMS) for the purpose of displaying synchrophasor data to the power system operators for the Voltage Management application.

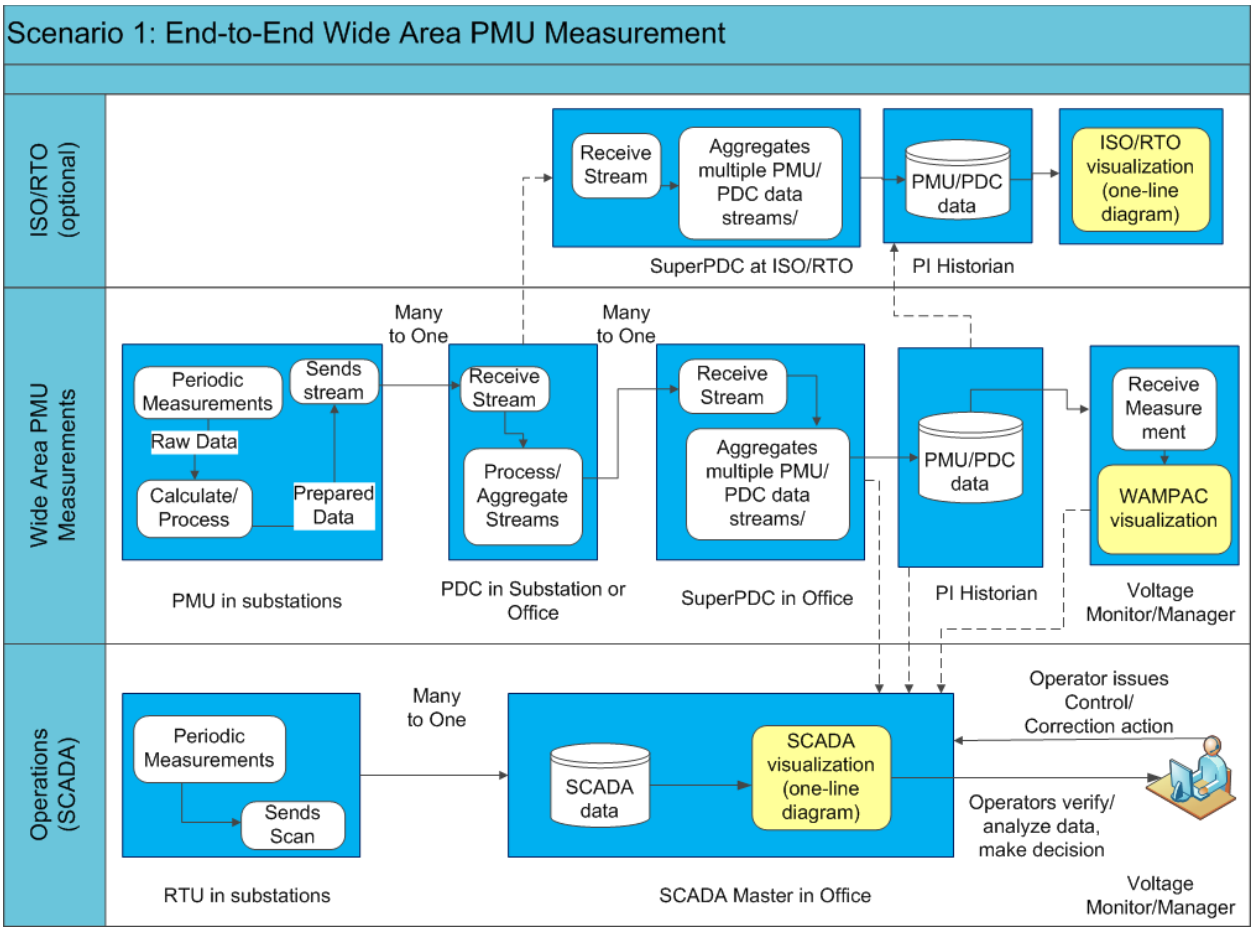


Figure 10: WAMPAC Interfacing with Various Enterprise Solutions

Based on the above scenarios, the following requirements for cyber security implementation may be summarized:

- The cyber security WAMPAC policy may have to extend beyond a single enterprise when WAMPAC systems are used across multiple organizations, which requires a broader stakeholder base when deciding on the use of standards.
- Within the same organization, WAMPAC systems may integrate with infrastructures owned and operated by other utility groups, which may use different cyber security policies due to the different regulatory bodies.

3.4 Interoperability Framework

The last consideration in the previous section relates to the need to enforce interoperability across components of the WAMPAC design. An illustration of the levels of Interoperability, as defined by the Grid Wise Architecture Council (GWAC), is given [12].

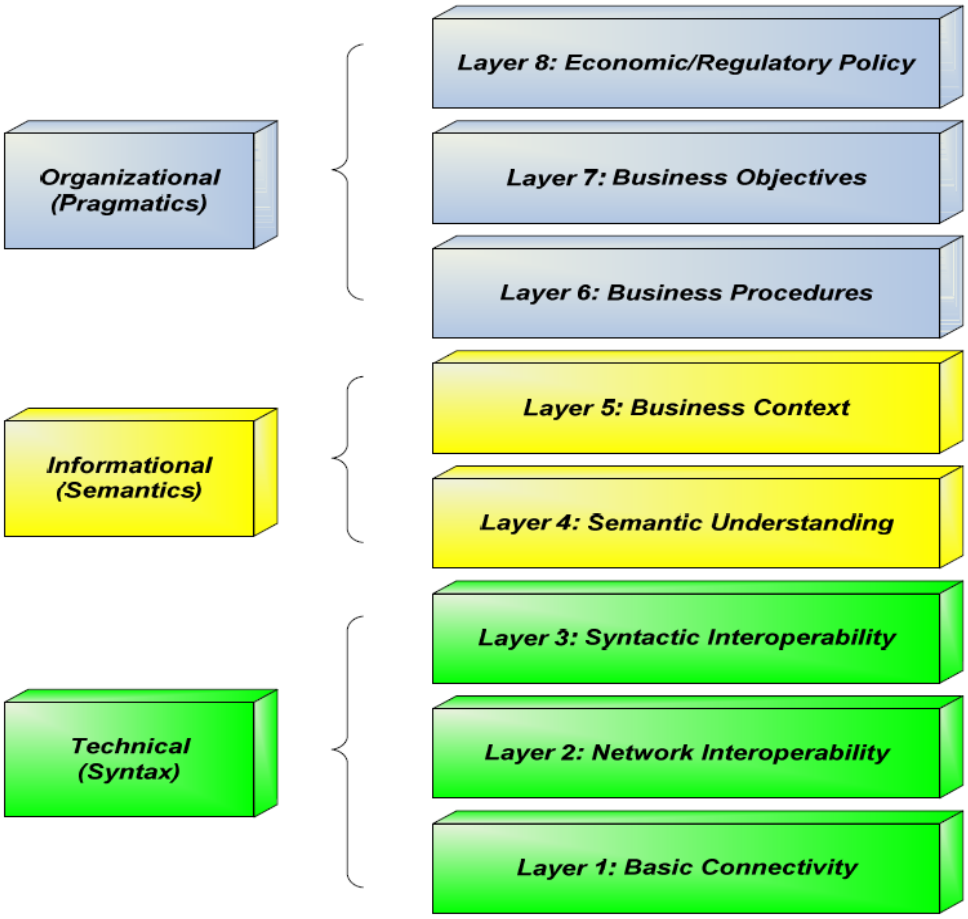


Figure 11: GWAC Stack Interoperability Framework

This implies that the interoperability considerations require not just specification of the physical communication layers, but also the semantic and syntax data layers, as well as organizational layers. The same should extend to the cyber security considerations, where the proposed solutions should be scrutinized at all the interoperability layers. This leads to a concept of cyber security interoperability, which assures that after the WAMPAC system components are replaced, the substitute components still comply with the cyber security design, implementation, testing, and policy requirements. Again, the key to such needs is the fact that the components of the WAMPAC system typically come from variety of vendors that may provide different features to implement cyber security solutions.

4. STATUS OF WAMPAC RELATED STANDARDS

4.1 WAMPAC standards development and coordination

This section provides a review of the WAMPAC related standards as of this date (July 2012). These standards fall into four categories: approved, in the approval process, under development, and other related standards/guidelines. The standards that are assessed in this document are underlined.

Approved standards are as follows:

- IEEE 37.111-1999 “COMTRADE” [13]
- IEEE 37.118-2005 “Standard for synchrophasors for power systems” [14]
- IEEE 37.232-2007 “Recommended practice for naming time sequence data files” [15]
- IEEE 37.239-2010 “COMFEDE” [16]
- IEEE PC37.238-2011 “Standard profile for use of 1588, precision time protocols in power system applications” [5]
- NERC CIP 2-9, Version #5 [17]
- IEC 61850 (90-5), 2012 “PMU logical node” [18]
- IEEE 37.118.1-2011 “Synchrophasor measurement” [19]
- IEEE 37.118.2-2011 “Synchrophasor communications” [20]

Standards in the approval process are as follows:

- IEC version of COMTRADE (IEC 60255-24, Ed 2)
- PC C37. 244 “Guide for Phasor Data Concentrator Requirements for Power System Protection, Control and Monitoring”
- PC 37.242 “Guide for Synchronization, Calibration, Testing and Installation of Phasor Measurement Units for Power System Protection and Control”

Standards under development are as follows:

- PC 37.240 “Standard for Cyber Security Requirements for Substation Automation, Protection and Control Systems”

Other related standards/guidelines are as follows:

- IEC 61850 “Substation Automation” [6]
- IEC 61970 “Common Information Model” [7]

- NISTIR 7628 [21], a guideline, not a standard
- IEC 62351-6: security for 61850 [22]
- IEC 62351: other security considerations [22]
- IEEE 1815-2010 "DNP Standard for Electric Power System Communications"[23]
- IETF RFC6272 "Internet Protocol Standards for Smart Grid" [24]

While this review is not exhaustive, the list already contains 20 standards related to WAMPAC implementation.

4.1.1 Cyber security review of candidates for Catalog of Standards

The Smart Grid Interoperability Panel's Catalog of Standards [25 & 26] has two sections, Approved [25A] standards, and In Process standards (documented in the Review Queue and Tracking Tool [25B]. Reviews started in Oct 2011.

The SGIP subgroups each review the standards before they are approved to be added to the SGIP Catalog of Standards. Priority Action Plan groups (PAP) and Domain Expert Working Group (DEWG) submissions determine review priority. The CSWG is the group that considers cyber security concerns and the WAMPAC team has leveraged their reviews.

The review includes several SGIP entities:

- Working group (Applicable PAP or DEWG)
- Smart Grid Architecture Committee (SGAC)
- Cyber security Working Group (CSWG)
- Testing and Certification Committee (TCC), which is not yet involved in the process but may be soon
- SGIP Governing Board

Table 2 below shows the status of the CSWG cyber security review of WAMPAC related standards as of May 30, 2012. The second column shows current status of the approval process by SGIP. The third column shows the status of the standard with respect to the SGIP's Catalog of Standards, while the fourth shows the status of the CSWG reviews, both as of May.

Table 2: Status of the SGIP Cyber Security Review of WAMPAC Related Standards

Standards	WG Status	Catalog of Standards	CSWG
IEEE C37.238-2011 "Standard profile for use of 1588, precision time protocols in power system applications"	Published	Approved	Reviewed
IEC 61850 (90-5) "substation automation"	Published	Candidate	Reviewed
IEC 62351-6: Security for IEC 61850	Published	Candidate	Reviewed

Standards	WG Status	Catalog of Standards	CSWG
IEC 62351 (-3, -4, -5, -6)	Published	Candidate	Reviewed
IEC 61970 (1-501) “Common Information Model”	Published	Candidate	Reviewed
IEEE 37.111-1999 “COMTRADE”	Published	Up for Candidacy	Not in queue
IEEE 37.232-2007 “Recommended practice for naming time sequence data files”	Published	Up for Candidacy	Not in queue
IEEE 37.239-2010 “COMFEDE”	Published	Approved	Reviewed
IEEE 37.118.1-2011 “Synchrophasor measurement”	Published	Not in queue	Not in queue
IEEE 37.118.2-2011 “Synchrophasor communications”	Published	Not in queue	Not in queue
IETF RFC6272: Internet Protocol Standards for Smart Grid	Published	Approved	Reviewed
IEEE 1815-2010, Std for Electric Power Systems Communications (DNP3)	Published	Approved	Reviewed
NERC CIP 2-9	Published	Candidate	In queue
IEEE C37.244-2012	Not Published	Not in queue	Not in queue
IEEE C37.242-2012	Not Published	Not in queue	Not in queue

A review of Table 2 and other facts surrounding the CoS cyber security review process suggest the following.

- Cyber security review of WAMPAC standards is progressing well, but several WAMPAC related standards are either pending review, or are yet to be nominated for Catalog of Standards (CoS) candidacy and evaluated.
- So far, out of 20 WAMPAC related standards only four are approved, five are recognized as candidates, two are up for candidacy and four are not in the queue yet. The remaining ones are not yet in the process.
- Understanding that the CoS process deals with many other standards that are not applicable to WAMPAC, it may take some time before all WAMPAC related standards for cyber security compliance are considered.
- The current focus of the PAPs/DEWGs, SGAC, CSWG, TCC and the GB is to review the standards on a stand-alone (individual) basis, hence not taking into account end-to-end

solutions, so any cyber security harmonization issues between different standards are not considered.

- The SGIP is transitioning into a new organization (SGIP 2.0) as of January 1, 2013. It is not clear how this will impact the standards review process for inclusion of standards into CoS.
- A formal process for providing cyber security review of WAMPAC standards does not have a direct feedback to the standards development organizations, so newly emerging WAMPAC standards do not have the benefit of a priori guidance to assure cyber security interoperability for end-to-end solutions.

4.1.2 NISTIR 7628 logical Reference Model review

The Logical Reference Model, Figure 12 below, documented in the NISTIR 7628 report is intended to provide a general logical architecture in context of the Guidelines for Smart Grid Cyber Security.

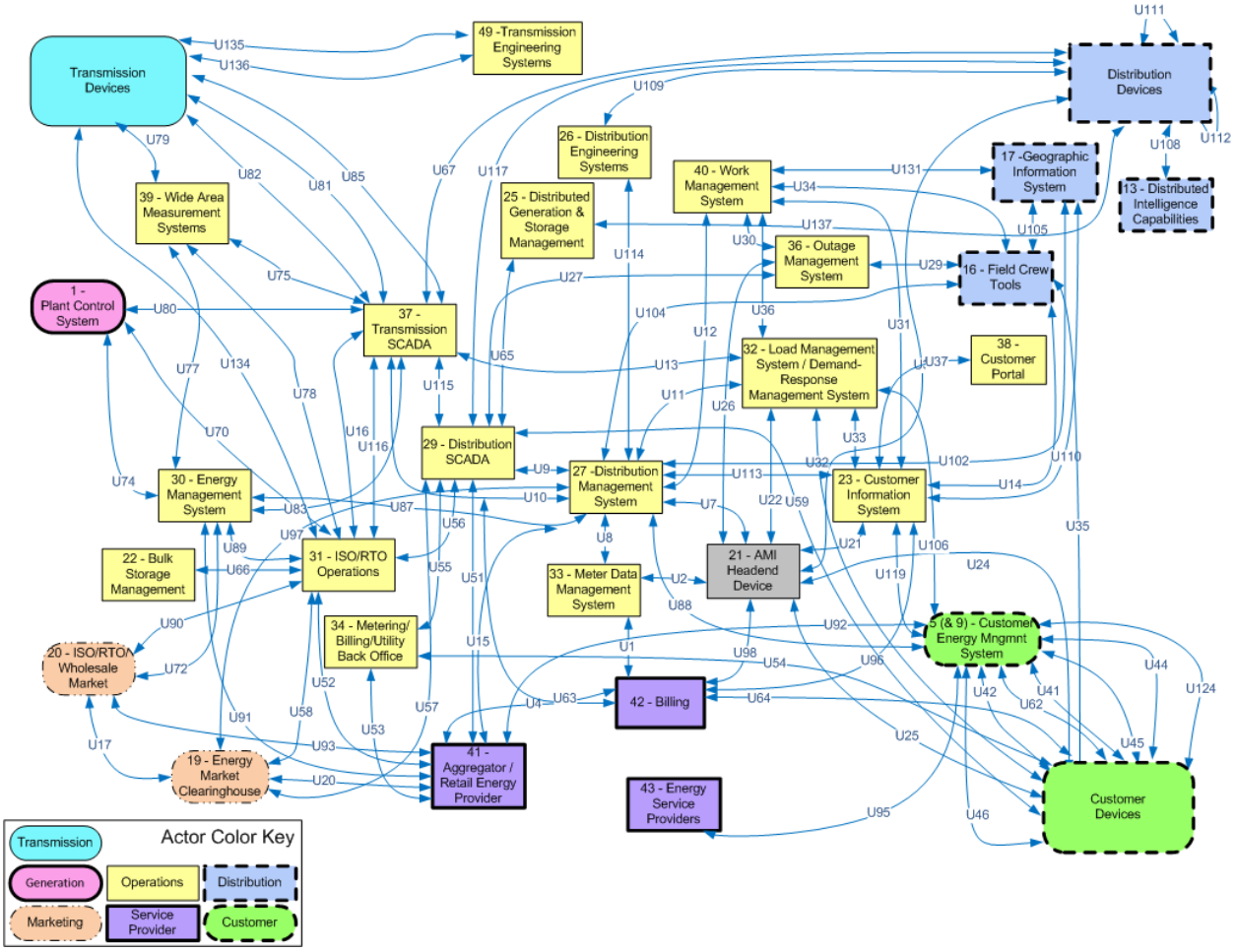


Figure 12: Draft update (May 2012) of the Logical Reference Model, Top Level

The Actors represent Applications and Devices within each of the seven SGIP domains: Generation, Transmission, Distribution, Operations, Marketing, Service Provider, and Customer. The Interfaces define typical integrations between the applications, with more detail in the Logical Interface Categories in the published report (not duplicated here). The Interfaces do not document data flow, or directional integrations. They are also not physical interfaces, but represent the logical level. Note that many physical implementations can map to one generic logical architecture. There are a variety of ways organizations are structured, and this diagram is intended to capture a generic representation based on the SGIP domains.

The NISTIR 7628 has a planned revision in process by the CSWG, and the key updates to this diagram include:

- Removing people and organization Actors from the Logical Reference Model. These will be described in text since there are many variations, which complicate the diagram.

- Creating a hierarchy of diagrams to simplify the top-level diagram, which will contain only Application actors. The Device actors are represented down a level, still showing interfaces to the Applications. There are also many variations in how Devices are deployed, and the intent is to document the generic information that represents many possible implementation architectures.

Figure 12 has the following corrections, the first bullet is from the CSWG F2F meeting in April, and the second is from this WAMPAC project:

- U134 should not connect from #45 Phasor Measurement Unit to a Market application (as shown in the published NISTIR 7628 version) but instead connects to Actor #31 ISO/RTO Operations.

- Actor #39 Wide Area Measurement Systems has been redefined to represent all of the more specific WAMPAC applications, and a mapping is documented in Table 1 above.

The Transmission domain contains the WAMPAC devices, but these devices communicate with key applications within the Operations domain, as shown in Figure 13. The diagrams in this section are the current drafts as of May 30, 2012, containing updates from the published NISTIR 7628 diagrams.

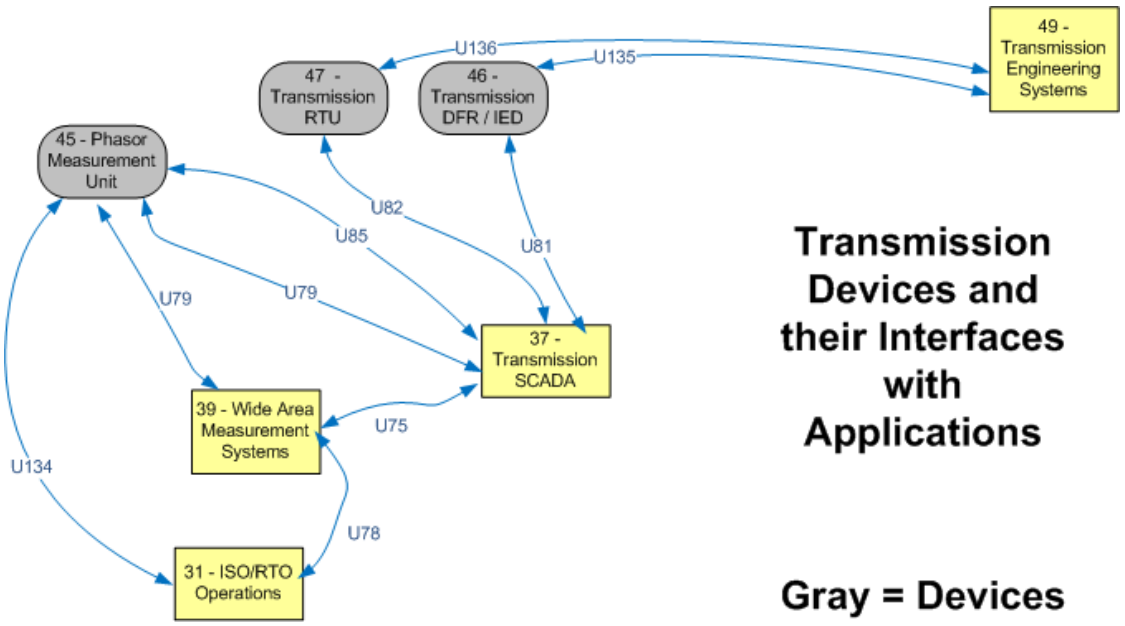


Figure 13: Focus on Transmission Devices showing their Interfaces with Applications (May 30, 2012 draft)

4.2 Summary of Assessments of key WAMPAC Standards

This study documents some of the cyber security issues for some of the most prominent WAMPAC standards:

- WAMPAC issues related to NERC CIP Standards Version 5

- Cyber security for IEC 61850 vs. IEEE 1815 (DNP3)

- IEC 61970: EMS Application Program Interface
- C37.118 IEEE Standards for Synchrophasors in Power Systems
- IETF RFC 6272 Internet Protocols for the Smart Grid

Listed below are major points from the detailed assessments:

4.2.1 WAMPAC issues related to NERC CIP Standards Version 5

- Guidance for mapping WAMPAC usage scenarios and architectures to the proposed NERC CIP impact levels, which does not exist as of today, would assist utilities in incorporating NERC CIP V5 requirements in WAMPAC solutions.
- Under some circumstances, the compromise of the field input data to the WAMPAC analysis process that takes place at the control center could have an impact similar to a compromise of that control center process itself. One such circumstance would be a widespread compromise of WAMPAC data for which there is no reliable method of detecting that a compromise has occurred. Achievement of cyber security for WAMPAC will depend upon a full understanding of such circumstances and their mitigation.
- Multiple ownership of IEDs may be an issue where an ISO owns Dynamic Disturbance Recorders (DDRs) located in substations owned by an operating company. With some labor union contracts, only employees of the operating company may be allowed to access DDRs for installation, repair, and maintenance since the substation is owned by the operator although the ISO is the owner.

4.2.2 Cyber security for IEC 61850 vs. IEEE 1815 (DNP3)

- Adding security to DNP3 has been an active area. DNP3 Secure Authentication (SA) was first released in 2008. The IEEE-1815-2010 incorporated security by including DNP3 SA v2. IEEE 1815-2010 is being replaced by a 2012 version. SA v2 has been superseded by SA v5 [35], which has been approved by the DNP3 user's group and will be part of the upcoming IEEE 1815-2012. SA v5 addresses both discovered vulnerabilities and usability issues for SA v2 as described in [36]. DNP3 SA is fundamentally based on IEC 62351-5. IEC 62351-5 previously included SA v2, and has been updated to SA v5 but not yet approved by IEC.
- For time-critical applications (e.g., 4 millisecond response time), some cyber security requirements may be relaxed. This may not be permissible from a cyber security risk acceptance perspective. Innovative cyber security controls will need to be designed and implemented. This is a challenge for the IEC 62351-6 developers.
- The present study concluded that TCP/IP based implementations of DNP3 and IEC 61850 would likely have equivalent security, since they are both using TLS, including authentication and encryption. Since security of TLS is highly configuration dependent, further study of the details in the standards that address this issue would be of interest.

4.2.3 IEC 61970: EMS Application Program Interface

- This standard has many parts, as listed in the SGIP CSWG review [46] performed for this standard. The standard has not been incorporated into the SGIP CoS. Under the present effort, the study team reviewed in totality IEC 61970-501: Common Information Model (CIM) XML Codification for Programmable Reference and Model Data Exchange. The team concluded that the scope of this standard is limited to knowledge representation—abstract models for information. Thus the team concurs with the CSWG review (October, 2010) of this standard (2.2.2) that it "…does not (and does not need to) address security…"

- The information that the standard is intended to represent however will tend to have related cyber security requirements. The information integrity and in some cases confidentiality will need protection both in transit and at rest. Tampering with such information might allow attackers to influence control center applications to fail. Information about the structure of power system data might enable specialized attacks to be formulated against an implementation.

4.2.4 C37.118 IEEE Standards for Synchrophasors in Power Systems

- The most security-relevant aspect of C37.118.1-2011 standard is that it sets stringent requirements for temporal accuracy and reporting latency that implementations must meet. These provide potential targets for an attacker wishing to disrupt WAMPAC. Neither this document nor C37.118.2-2011 specify features of an overall system or architecture that would allow it to continue to meet specified accuracy and timing requirements in the face of cyber attack. Examples of such attacks would be spoofing of GPS time signals or flooding attacks that slow down network communications.

- The communication standard C37.118.2-2011 does not have a prescription for cryptographic assurance of authenticity or of confidentiality. The Annexes (E, F) do not subsequently note any of the existing methods of transport security, e.g. IPSEC, TLS. Of particular concern will be the identification of secure communication methods that meet the hard real-time requirements in C37.118.1-2011.

- IEC 61850-90-5 was approved by the SGIP for inclusion in the CoS. The standard makes reference to standards that have not been considered and approved by the SGIP. This "alert" is important for the users since the conclusions may be valid only when all normative (mandatory) references are also approved.

4.2.5 IETF RFC 6272 Internet Protocols for Smart Grid

- RFC 6272 is not specifically focused on security. However every IETF specification needs a section on security considerations (per the guidelines in RFC 3552), and this one has two relevant components. Section 2.2 reviews security goals and threats at the physical, network, transport and application layers. Section 3.1 includes a "security toolbox" - existing building blocks to address threats. This is done largely through reference to other RFCs (although it also cites IEC 62351-3).

- In terms of WAMPAC or any other smart-grid application, the security sections of this RFC serve as a catalog of proven methods to consider in order to meet the security needs

for the application, once these are identified. This standard does not recommend specific methods or combinations of methods for any specific application, other than the illustrative meter infrastructure example in its Appendix A. These conclusions are consistent with the review performed of this document by SGIP CSWG [37].

4.2.6 IEEE 1588-2008

- Precision Time Protocol, IEEE 1588-2008, used in conjunction with the standard profile defined in C37.238 may be susceptible to several cyber security attacks. One attack method is to impersonate the master clock. The next identified attack method is to illegally update the sequence ID in the Sync message. The next attack method is to masquerade the time stamp in the Follow-up message. The final attack method identified is caused by delaying the timing messages.

4.2.7 IEC 61850

- In 61850, for any given function (e.g. distance protection), various attack methods exist due to the communications required among the LNs to execute the function that they compose. One attack method is related to encryption: even if encryption is implemented, given the fast timing and the accuracy of the clock, a DOS attack can be staged involving key exchange mechanisms. The exchange of system parameters (in particular configuration and operational parameters) is may be vulnerable to various cyber security issues/attacks. IEC 61850 application association services may be vulnerable to getting hijacked, aborted, or released even with IEC 62351.

- In 61850-90-5, the first identified attack method is caused by modifying the SCL file. This is caused because the protocol designed for the phasor gateway does not need to check the frequency of SCL file import and the validity of the file's contents. To mitigate this type of attack, the frequency of dissemination of new SCL files can be checked and controlled. The second attack is caused by attacking the PMU configuration data. To mitigate this type of attack, the frequency of configuration data modification should be monitored.

- IEC 61850-90-5 was approved by SGIP for inclusion in CoS. The standard makes a reference to standards that have NOT been considered and approved by SGIP. This "alert" is important for the users since the conclusions may be valid only when all normative (i.e. mandatory) references are also approved.

5. RECOMMENDATIONS AND FUTURE WORK

Background – Cyber Security Objectives

Following are some broad cyber security objectives for WAMPAC systems. The terms that are in italics need to be defined for WAMPAC.

- **Measurement integrity** - Individual measurements values related to specific *authorized measurement points* and points in time, as ultimately available to an operator either as individual measurements or in analyzed/aggregated output, are equal to the values captured in the field by *authorized measurement equipment* at these measurement points at these points in time.
- **Measurement authenticity** - All measurements available to an operator either as individual measurements or in analyzed/aggregated output, are equal to values captured in the field by authorized measurement equipment.
- **Measurement availability** - The operator has timely access to all measurement data and to analysis/aggregations for all *measurement points and points in time that are intended*, based upon the system design and configuration.
- **Analysis integrity** - All analyzed/aggregated output available to an operator represents the intended result based upon the underlying measurements specified for this output.
- **Data confidentiality** - System data such as individual measurements, analyzed/aggregated information based upon measurements, and configurations are protected from disclosure to unauthorized persons or systems to the extent that disclosure of this data would provide an advantage to a threat agent in harming the electric system via cyber or physical means.

These objectives are related to the security principles listed in [39] 3.2.3 in that these are logically higher level goals from which more specific principles are derived (such as the need to verify integrity of data, authenticate, audit, and so on). Starting with higher-level statements and breaking them down logically makes it easier to review the full set of proposed mitigations for completeness.

5.1 Recommendations

Following are several recommendations for future work. These are organized into several categories.

5.1.1 System Definition and Design

1. Develop specific WAMPAC cyber security objectives, including associated definition of terms. An initial draft set of such objectives is included above.

2. Develop guidelines for cyber security requirements for WAMPAC end-to-end solutions that may be applied across all WAMPAC related standards. This is important to achieve interoperability of future WAMPAC solutions.
3. WAMPAC cyber security requirements need to be defined in the overall application context, and not just on an individual standards basis since end-to-end implementation requires harmonization across all involved standards.

4. Further refine the WAMPAC description from a functional and architecture point of view. These will include the NISTIR 7628 and the ASAP-SG WAMPAC security profiles. ASAP-SG security profiles document recommended security controls tailored to the needs of specific smart grid application areas such as AMI, distribution management, or synchrophasor systems. Add additional architectural and functional detail to support a security analysis.

5. A cyber security WAMPAC policy may have to extend beyond a single enterprise when WAMPAC systems are used across multiple organizations. This will require broader stakeholder participation when deciding how to implement a policy.

6. Cyber security policy, design, implementation, and testing need to differentiate between the "standard" approaches that apply to any information technology infrastructure and the requirements imposed by a WAMPAC domain application.

5.1.2 Standards and Guidelines

7. Building upon this document, continue developing a list of standards proposed to be applied for WAMPAC. Document how the various standards would be used within WAMPAC at a high level. This includes identifying the standards that are used on specific links or nodes, and the specific operations. Highlight any conflicts or incompatibilities between the various proposed standards.

8. Document at a high level the extent to which the proposed standards support the specific WAMPAC security objectives. This part of the analysis should also include a mapping from each usage of a standard as identified in #3, to requirements and/or controls in the NISTIR 7628 and the ASAP-SG WAMPAC profile documents.

9. Document the vulnerabilities and objectives that are not mitigated by the proposed standards. This will require some level of analysis of the attack surface of the system. There is a significant amount of work already done on this in ASAP-SG and in the NESCOR failure scenario document. This task would add any new aspects that arise based upon an end-to-end consideration of the security objectives and architecture.

10. Identify unmitigated vulnerabilities that potentially could be addressed by future standards or improvements to some standards. These are potential "standards gaps."

11. The existing version of NISTIR 7628 and its current revision related to WAMPAC representation in the "spaghetti" diagram need to be further refined to achieve granularity shown in some of the WAMPAC "swim lane" diagrams in this report.

12. Future revisions of the NERC CIP Version 5 standards should consider focusing on defining cyber security requirements for WAMPAC implementation cases where measurement devices may be performing multiple functionalities. This is currently not covered by the standards.

13. Cyber security vulnerabilities caused by the use of multiple standards is not considered today when standards are evaluated by the SGIP for cyber security compliance, and future efforts should consider overall end-to-end interfaces.

14. Current WAMPAC related standards are addressing cyber security aspects of data management and communication issues but the issues associated with an attack that affects the time reference signal are not fully explored.

5.1.3 Assessment

15. Mapping of Pen Tests to WAMPAC Failure Scenario Vulnerabilities: under development is a document that maps the Pen Tests that apply to the vulnerabilities in each of the Failure Scenarios. This will include the WAMPAC vulnerabilities, and is only mentioned here since a reference is not yet available. This will result in combining WAMPAC efforts from all three working groups: WG1's Failure Scenarios, WG2's WAMPAC expertise, and WG3's Pen Tests.

    Mapping References:

    1. Electric Sector Failure Scenarios 04-18-012 draft

    2. NESCOR Penetration Test Plan, Version 2.0 Alpha3

16. Penetration testing of WAMPAC solutions for cyber security vulnerability is currently ad-hoc and needs to be fully specified to reflect test scenarios, test methods, test plans, and the metrics for test performance assessment.

    1. Identify cyber security vulnerabilities of WAMPAC solutions. This includes software and hardware vulnerabilities. For vulnerabilities of each component, a corresponding impact on the rest of the WAMPAC solution should be identified.

    2. Assess the risk associated with each vulnerability and correlate to a performance deterioration of the overall WAMPAC system solution. This will lead to a ranking of the vulnerabilities. Since one vulnerability may lead to another, the risk will be

defined as a "nested" concept identifying compounded risk should multiple vulnerabilities be compromised simultaneously.

3. Define metrics for penetration test results under various test conditions. For each type of test, the metric will reflect the level of WAMPAC solution deterioration.

17. The certification process for interoperability of WAMPAC solutions should define clear test procedures for verifying cyber security interoperability for components of WAMPAC end-to-end solutions.

6. CONCLUSIONS

This report's findings point out several areas of further investigation that may be carried out by different groups going forward:

- NESCOR efforts of TWG 1, 2 and 3 may focus on issues regarding WAMPAC end-to-end solutions by studying nested vulnerabilities, certification of cyber security standards interoperability requirements, and penetration test plans and metrics.
- There is an opportunity for TWG2 to develop an overall picture of WAMPAC standards gaps based upon the top down process outlined here. This process leverages NISTIR 7628, the ASAP-SG WAMPAC security profile, the NESCOR failure scenarios for WAMPAC and this initial NESCOR WAMPAC standards study.
- The SGIP efforts regarding the cyber security review of WAMPAC-related standards and NISTIR update of the WAMPAC-related components in the Logical Reference Model ("spaghetti") diagram may be updated based on recommendations from this study.
- Further impacts are expected in the NASPI community that is focused on many implementation aspects including cyber security and WAMPAC solution testing for certification purposes.
- Standards developing organizations, such as IEEE and IEC that are involved in the development of WAMPAC standards could use the discussion of end-to-end requirements to further harmonize the standards. Particularly useful would be incorporating or referencing a common and comprehensive set of cybersecurity requirements.
- The issues raised about the multiple uses of substation IEDs and multiple end users of the synchrophasor data may inform further revision of NERC CIP standards so that CIP requirements are more tuned to various end-to-end solution scenarios.

7. REFERENCES

1. NIST Smart Grid T&D Domain Expert Working Group: *Wide Area Monitoring, Automation, Communications, and Control (WAMACC) for the Bulk Transmission System, Nov 2009* http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/TnD#Wide_Area_Monitoring_Protection. [white paper]
2. FNET description: http://fnetpublic.utk.edu/. [website]
3. IRIG-B: *IRIG Standard 200-98*. Range Commanders Council, May 1998. [report]
4. IEEE Standard 1588-2008: *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, July 2008.* [report]
5. IEEE Standard C37.238: *IEEE Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications, 2011.* [report]
6. Davis, Kathleen: *DNP3 vs. IEC: Skirmish in the Substation, Electric Light & Power, POWERGRID International, 2011.* http://www.elp.com/index/display/article-display/361183/articles/utility-automation-engineering-td/volume-14/issue-5/features/dnp-vs-iec-skirmish-in-the-substation.html. [website]
7. IEC Standard 61970-501:2006(E): *Energy management system application program interface (EMS-API) Part 501: Common Information Model Resource Description Framework (CIM RDF) schema.* Commission Electrotechnique Internationale (www.iec.ch.) Geneva, Switzerland, 2006-03. The 61970 standard has several sub parts in addition to this specific part studied by the team. [report]
8. EPRI Report #1020098: *Harmonizing the International Electrotechnical Commission Common Information Model (CIM) and 61850 Standards via a Unified Model: Key to Achieve Smart Grid Interoperability Objectives*. EPRI, Palo Alto, CA: 2010. [report]
9. Boehm, B.: *A Spiral Model of Software Development and Enhancement*, ACM SIGSOFT Software Engineering Notes, ACM, 11(4):14-24, August 1986. [report]
10. Spiral Model: http://en.wikipedia.org/wiki/Spiral_model. [website]
11. NASA-GB-8719.13: *NASA Software Safety Guidebook*. March 31, 2004, p.56-57. [book]
12. GridWise Architecture Council: *GridWise Interoperability Context-Setting Framework, March 2008*. http://www.gridwiseac.org/pdfs/interopframework_v1_1.pdf. [website]

13. IEC Standard 60255-24 ed1.0: *Common Format for transient data exchange (COMTRADE) for power systems.* Commission Electrotechnique Internationale (www.iec.ch.) Geneva, Switzerland, 2001-05-04. [report]

14. IEEE Standard C37.118-2005: *IEEE Standard for Synchrophasors for Power Systems.* IEEE, New York, NY, March 2006. [report]
15. IEEE Standard C37.232-2007: *IEEE Recommended Practice for Naming Time Sequence Data Files.* IEEE, New York, NY, August 2007. [report]
16. IEEE Standard C37.239-2010: *IEEE Standard Common Format for Event Data Exchange (COMFEDE) for Power Systems.* IEEE, New York, NY, Nov 2010. [report]
17. Draft NERC CIP Version 5 standards: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_Version_5_CIP_Standards_.html. March 26, 2012. [website]
18. IEC/TR 61850-90-5 ed1.0: *Communication networks and systems for power utility automation - Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118, 2012-05-09.* [report]
19. IEEE. Std C37.118.1-2011: *IEEE Standard for Synchrophasor Measurements for Power Systems*. IEEE, New York, NY, Dec 2011. [report]

20. IEEE. Std C37.118.1-2011: *IEEE Standard for Synchrophasor Measurements for Power Systems.* IEEE, New York, NY, Dec 2011. [report]

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

22. DNP3 Secure Authentication:v5 2011-11-08 draft: http://www.dnp.org/Lists/Announcements/Attachments/7/Secure%20Authentication%20v5%202011-11-08.pdf. [website]

23. IETF. RFC 6272: *Internet Protocols for the Smart Grid*. Baker, F. & Meyer, D., 2011-06. https://tools.ietf.org/html/rfc6272. [website]

24. Cleveland, Frances: *IEC TC57 Security Standards for the Power System's Information Infrastructure – Beyond Simple Encryption, Xanthus Consulting International.* June 2007. [white paper]

25. Smart Grid Interoperability Panel (SGIP) Catalog of Standards: *25A Approved*. http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPCoSStandardsInformationLibrary. [website]
26. Smart Grid Interoperability Panel (SGIP) Catalog of Standards: *25B Candidates*. http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CoSStandardsReviewQueueAndTrackingTool. [website]

27. *Communication Networks and Systems in Substations – Part 1: Introduction and Overview*. IEC 61850-1, IEC/TR 61850-1:2003(E). [report]
28. NESCOR FS: *EPRI NESCOR, Electric Sector Failure Scenarios and Impact Analyses, version 0.1. January 30, 2012*. www.smartgrid.epri.com/nescor.aspx. [website]

29. *Tools and Methods for Hardening Communication Security of Energy Delivery System (ADEC-G: Adaptive, Distributed, and Extensible Cybersecurity for the Grid).* DE-OE0000518 (funded by DOE OE). [report]

30. *Communication networks and systems in substations – Part 7-1: Basic communication structure for substation and feeder equipment – Principles and models.* IEC International standards, IEC 61850-7-1:2003(E). [report]

31. Narain ,S., Talpade, R., Levin, G. *Network Configuration Validation*. Chapter in Guide to Reliable Internet Services and Applications, edited by Kalmanek, Chuck (AT&T), Yang ,Richard (Yale) and Misra, Sudip (IIT). Verlag ,Springer, 2010. [report]
32. McMorran, Alan W [McMorran]. *An Introduction to IEC 61970-301 and 61968-11: The Common Information Model*. University of Strathclyde, January 2007. [report]

33. IETF. RFC 6272: *Internet Protocols for the Smart Grid*. Baker, F. & Meyer, D. June 2011 https://tools.ietf.org/html/rfc6272. [website]

34. SA v2: *DNP3 Vol2-Supp1 Secure Authentication v2 July 7th, 2008*. Included in IEEE-1815-2010, cited above. [report]

35. SA v5: *DNP3 Secure Authentication v5 August 11th, 2011*. Draft. http://www.dnp.org/Lists/Announcements/Attachments/7/Secure%20Authentication%20v5%202011-11-08.pdf. [website]

36. SA v5 Info: *Further Information Regarding the Release of DNP3 Secure Authentication Version 5 (SAv5)*. December 1st, 2011. http://www.dnp.org/DNP3Downloads/DNP3%20SAv5%20Further%20Info%20Announcement%2020111201.pdf. [website]

37. CSWG 6272: *CSWG Comments on PAP01: Role of the Internet Protocol Suite (IPS) in the Smart Grid, 2010-10.* [report]

38. CSWG 61850: Smart Grid Interoperability Panel Cyber Security Working Group Standards Review. *CSWG Standards Review Report: IEC 61850, 2010-10.* [report]

39. PROFILE: *Advanced Security Acceleration Project for the Smart Grid, Security Profile for Wide-Area Monitoring, Protection, and Control*. Version 0.08. May 2011 [report]

40. IEC 60870-5: *Telecontrol equipment and systems - Part 5: Transmission protocols, 2007-10*. This standard has several sub parts which are not listed individually here. [report]

41. *Power systems management and associated information exchange – Data and communications security, Part 1: Communication network and system security – Introduction to security issues.*

42. ASAP-SG: SmartGridipedia. *http://www.smartgridipedia.org/index.php/ASAP-SG*. [website]

43. CSWG STDS: SGIP CSWG Standards Subgroup Wiki Page. *http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGStandards*. [website]

44. NERC CIP: Draft Version 5 standards dated March 26, 2012. http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_Version_5_CIP_Standards_.html. [website]

45. IEC Technical Specifications, IEC/TS 62351-1, 2007(E). [report]

46. CSWG 61970: Smart Grid Interoperability Panel Cyber Security Working Group Standards Review. *CSWG Standards Review Report: IEC 61970, 2010-10.* [report]

47. DNP3 OVER: Triangle MicroWorks, Inc. *DNP3 Overview, Revision 1.2, February 22, 2002*. [report]

48. IEC. 61850: *Communication networks and systems for power utility automation*. This standard has several sub parts that are not listed individually here. [report]

49. IEC. 62351: *Information Security for Power System Control Operations*. This standard has several sub parts that are not listed individually here. [report]

50. *Harmonization of IEEE C37.118 with IEC 61850 and Precision Time Synchronization (IEC 61850-90-5)*. Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG) Standards Review, Priority Action Plan (PAP) 13. April 28, 2011. [report]

51. *Power systems management and associated information exchange – Data and communications security, Part 6: Security for IEC 61850.* IEC Technical Specifications, IEC/TS 62351-6, 2007(E). [report]

52. *NIST SGIP CSWG Standards Review, Phase 1 Report*. October 7, 2010. http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGStandards/StandardsReviewPhase-1Report.pdf. [website]

53. Guidelines for Smart Grid Cyber Security. Computer Security Division: *NIST Interagency Report NISTIR 7628, August 2010.*National Institute of Standards and Technology. [report]

54. IEEE. Std 1815: *IEEE Standards for Electric Power Systems Communications – Distributed Network Protocol*. IEEE, New York, NY. IEEE 1815-2010 has been published. IEEE 1815-2012 is pending publication as of the date of this report. [report]

55. CSWG 1815: Smart Grid Interoperability Panel Cyber Security Working Group Standards Review. *CSWG Standards Review Report: IEEE 1815, 2010-9.* [report]

7.1 Acronyms

AH	Authentication Header
ASAP SG	Advanced Security Acceleration Project for the Smart Grid
BES	Bulk Electric System

CBM	Circuit Breaker Monitor
CIM	Common Information Model
CIP	Critical Infrastructure Protection
CIS	Component Interface Specification
CMS	Cryptographic Message Syntax
CoS	Catalog of Standards
CRC	Cyclic Redundancy Checks
CSWG	Cyber Security Working Group
DDR	Digital Disturbance Recorder
DEWG	Domain Expert Working Group
DFR	Digital Fault Recorder
DNP	Distributed Network Protocol
DOE	Department of Energy
DPR	Digital Protective Relay
EAP	Extensible Authentication Protocol
EMS	Energy Management System
EPRI	Electric Power Research Institute
ERCOT	Electric Reliability Council of Texas
ESP	Encapsulating Security Protocol
F2F	Face to Face
FERC	Federal Energy Regulatory Commission
FL	Fault Locator
GB	Governing Board
GPS	Global Positioning System
GWAC	Grid Wise Architecture Council
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPS IP	IP Protocol Suite

IPSec IP	IP Security
IRIG	Inter-range Instrumentation Group
ISO	Independent System Operator
LAN	Local Area Network
MMS	Manufacturing Message Specification
NASPI	North American Synchrophasor Initiative
NERC	North American Electric Reliability Corporation
NERC CIP	NERC Critical Infrastructure Protection
NESCOR	National Electric Sector Cyber security Organization Resource
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
NTP	Network Time Protocol
OAuth	Open [Standard for] Authorization
PANA	Protocol for Carrying Authentication for Network Access
PAP	Priority Action Plan
PDC	Phasor Data Concentrator
PKIX	Public Key Infrastructure using X.509
PMU	Phasor Measurement Unit
RDF	Resource Description Framework
RFC	Request for Comments
QoS	Quality of Service
RFC	Request for Comments
RTO	Regional Transmission Organization
RTU	Remote Terminal Unit
SA	Secure Authentication
SCADA	Supervisory Control and Data Acquisition
SGAC	Smart Grid Architecture Committee
SIPS	System Integrity Protection Scheme
SGIP	Smart Grid Interoperability Panel

S/MIME	Secure Multipurpose Internet Mail Extensions
SSH	Secure Shell
TC	Technical Committee
TCC	Testing Certification Committee
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSO	Transmission System Operator
UDP	User Datagram Protocol
UML	Unified Modeling Language
VPN	Virtual Private Network
WAMPAC	Wide Area Monitoring, Protection, and Control
WG	Working Group
XML	Extensible Markup Language

A APPENDIX: REVIEW OF SELECTED STANDARDS

This section includes assessments of the standards referenced throughout this report.

Related Work

The SGIP CSWG Standards subgroup performs a task they describe on their public web page [43] as follows:

- "…assesses standards and other documents with respect to their cyber security requirements…"
- "During these assessments, the subgroup determines if a document does or should contain cyber security requirements, correlates those requirements with the Catalog of Cyber Security Requirements found in the NISTIR 7628, and identifies any gaps. Finally, recommendations are made for further work to develop the missing cyber security requirements."

This NESCOR effort focuses on the cyber security requirements for WAMPAC, while the CSWG addresses cyber security for all the domains of the electric sector. This report has leveraged the results of CSWG standards reviews where such reviews were available for standards that may be applicable to WAMPAC. Among the standards discussed in this report, CSWG reviews were available for IEC 61970, IEC 62351, IETF RFC 6272 and an earlier version of IEEE 1815. This report also considers standards expected to have significant impact on WAMPAC deployments for which the CSWG has not posted reviews as of the publication of this report. These standards are the NERC CIP version 5 drafts and IEC C37.118.

ASAP-SG has carried out a cyber security study specific to WAMPAC entitled: "Wide-Area Monitoring, Protection, and Control Security Profile" [39]. As described on the ASAP-SG web site [42], "This document was developed … in order to accelerate the development of security requirements and standards. This document defines security requirements for wide-area monitoring, protection, and control of the electric grid, specifically leveraging synchrophasor technology…" Thus part of the purpose of the profile document is to facilitate studies such as the present one. The profile document does this by proposing the scope of cyber security requirements for WAMPAC, which in turn might be met by standards such as those reviewed in this report.

NERC CIP Version 5 Drafts

Application to WAMPAC

The current NERC CIP standards 002-009 [44] describe cyber security requirements on Bulk Electric System (BES) cyber systems. These standards are in active use and have been through several revisions. In particular, a second comment period on the Version 5 CIP Standards recently closed on May 21, 2012. This working version as posted for comment by NERC is considered in this report, and is referenced as NERC CIP V5. The NERC CIP standards have

been identified by SGIP as a candidate for review and inclusion in the SGIP Catalog of Standards (CoS) but have not yet been reviewed.

Under NERC CIP V5, different requirements are to be applied based upon whether a system is designated as high impact, medium impact, or low impact per criteria defined in NERC CIP V5 002. Therefore, to assess how these standards would apply to WAMPAC, a utility would need to assess particular functions supported and architectural characteristics of their WAMPAC usage scenario. This would allow the utility to determine the impact level of the associated cyber systems.

A further consideration is that a utility may install equipment with one function, such as voltage monitoring on a small scale. Later, measurements from this same equipment may be used for other more critical functions, such as primary monitoring and control decision-making, covering a broader area. Thus is very possible that the impact level of the same cyber system could change over time. However, deployment planning for the initial equipment may consider only architecture and equipment features for the initial impact level.

To avoid these potential problems, utilities have to consider when implementing WAMPAC components (1) the initial impact level but whether this will be different in the future and (2) whether the initial implementation meets NERC requirements for the initial impact level, but also whether the components can evolve in a technically feasible and cost effective manner to an impact level that may be required in the future. Guidance for mapping WAMPAC usage scenarios and architectures to NERC impact levels would assist utilities in performing this task.

Example

Utilities may purchase devices that function both as a protective relay and as a collector of phasor measurement data. The utilities have interpreted NERC CIP V5 to mean that if the protective relay function is used, then the equipment will be classified as high impact. If a utility also wants to use the data collection capability, the utility will need to secure the measurement and configuration data flow using the high impact level requirements. These are significant requirements. A utility might elect not to use the measurement capability so that these requirements do not apply.

Discussion with NERC

The study team that prepared this report initiated a discussion with NERC to begin to address the questions framed above. The team framed the initial query as follows:

“We would like to understand how NERC would apply its draft classification guidelines for high, medium and low impact (reference CIP 002-5 draft March 26, 2012), for the following cases of cyber assets:

- Device dedicated to a wide area application
- Device that does protection as well as being used for a wide area application
- Device that provides data for wide area protection, monitoring and control (WAMPAC)

The device might be a digital fault recorder (DFR), a phasor measurement unit (PMU) or a protective relay.

As a start, we observe that protection systems fall under Dynamic Response Operating Service per page 26, and field data sources fall under Balancing Load and Generation Operation Service per page 27 of the latest posted redline version NERC CIP 002-5."

The response to this question from a NERC representative was:

- In the current draft, high impact (as specified by the "bright-line" criteria in NERC CIP 002-5, Attachment 1, Section 1) only applies to equipment in control centers, and does not apply to data source instrumentation such as DFRs or PMUs.
- Likewise, since a protective relay is not in a control center, it would not be classified as high impact.
- These assets would therefore be given a medium or low rating, which would depend upon the bright-line criteria defined in the standard (as specified in CIP 002-5 Attachment 1, Sections 2 and 3).

The scope of NERC CIP is BES cyber systems. According to the terminology section of the NERC CIP standards, to qualify as a BES cyber system, a cyber system must perform a reliability task. The bright-line criteria in NERC CIP V5 002-5 are defined based upon the characteristics of power system assets with which a BES cyber system is associated. Examples of power system assets and characteristics mentioned in the standard are the Real Power capability of a generating facility, the voltage level, number of connected substations, and the presence of interfaces to nuclear power plants for a transmission facility, and the scale of an automated load shedding capability.

In the above example of a protective relay that incorporates a PMU function, these functions would be classified as either medium or low impact. Based on the current NERC CIP V5 drafts, the protective relay and the data collection function could have different NERC impact levels. The overall impact level is at the device or system level. The level would be the highest of the various levels. This could occur because the application using the data from the DFR might not meet the bright line criteria for medium impact, but the protective relay might. Further, classifications of either of these sub-elements of a device might change over time as their roles change. This might happen for due to changes in grid connectivity or the scope and nature of the WAMPAC application being supported by the data from the DFR.

Under some circumstances, the compromise of the field input data to the WAMPAC analysis process that takes place at the control center could have an impact similar to a compromise of that control center process itself. One such circumstance is a widespread compromise of WAMPAC data for which there is no reliable method of detecting that a compromise has occurred. Achievement of cyber security for WAMPAC will depend upon a full understanding of such circumstances and their mitigation.

Cyber Security for IEC 61850 vs. IEEE 1815 (DNP3)

The status of each of these standards is briefly summarized and then the cyber security aspects are assessed.

IEEE 1815 (DNP3)

Per the IEEE description of IEEE 1815: IEEE Standard for Electric Power Systems Communications -- Distributed Network Protocol (DNP3) this standard provides the following:

> *The DNP3 protocol structure, functions, and application alternatives and the corresponding conformance test procedures are specified. In addition to defining the structure and operation of DNP3, three application levels that are interoperable are defined. The simplest application is for low-cost distribution feeder devices, and the most complex is for full-featured master stations. The intermediate application level is for substation and other intermediate devices. The protocol is suitable for operation on a variety of communication media consistent with the makeup of most electric power communication systems.*

The DNP3 protocol can be used over a serial physical layer or Ethernet. DNP3 defines communication up through the application layer. DNP3 is an IEEE derivative of IEC 60870-5. Quoting an overview of DNP3 [47]:

> *DNP3 is an open, intelligent, robust, and efficient modern SCADA protocol. It can:*
>
> - *Request and respond with multiple data types in single messages,*
> - *Segment messages into multiple frames to ensure excellent error detection and recovery,*
> - *Include only changed data in response messages,*
> - *Assign priorities to data items and request data items periodically based on their priority,*
> - *Respond without request (unsolicited),*
> - *Support time synchronization and a standard time format,*
> - *Allow multiple masters and peer-to-peer operations, and*
> - *Allow user definable objects including file transfer.*

Adding security to DNP3 has been an active area. DNP3 Secure Authentication (SA) was first released in 2008. The IEEE-1815-2010 incorporated security by including DNP3 SA v2. IEEE 1815-2010 is being replaced by a 2012 version. SA v2 has been superseded by SA v5 [35], which has been approved by the DNP3 user's group and will be part of the upcoming IEEE 1815-2012. SA v5 addresses both discovered vulnerabilities and usability issues for SA v2 as described in [36].

IEEE 1815-2010 was reviewed by the SGIP CSWG and the need for the upcoming SA v5 enhancements was documented in that report [55]. IEEE 1815-2012 has been identified by SGIP as a candidate for further review and inclusion in the SGIP Catalog of Standards.

SA v5 is an application layer protocol for communication between DNP3 master and outstation. It is based upon IEC 62351-5 (Power systems management and associated information exchange

- Data and communications security - Part 5: Security for IEC 60870-5 and derivatives). The threats addressed by this protocol are:

- Spoofing
- Modification
- Replay
- Eavesdropping - on exchanges of cryptographic keys only, not on other data

Both directions of communication are considered. The approaches used to address these threats are:

- Challenge/response for authentication
- Pre-shared keys plus remote rekey method.

This method can be used alone on serial links, or in combination with TLS (Transport Layer Security) on TCP/IP connections.

IEC 61850

IEC 61850 is a family of standards and includes a communications protocol similar to the DNP3 protocol. However, the IEC 61850 family of standards is broader in scope, and describes other features NOT addressed in DNP3. These are: real-time services and protocols, self-description services, many information models, and System Configuration Language. As a communications protocol, DNP3 is designed to focus on inexpensive endpoints and low-bandwidth communication channels while IEC 61850 is designed for high-bandwidth communication channels with a richer, wider range of features.

The IEC 61850 family been reviewed by the SGIP CSWG [38] and many parts of it are included in the Catalog of Standards. IEC 61850-90-5 relates specifically to the application of 61850 to WAMPAC. It has been reviewed but is not yet included in the CoS. It is discussed elsewhere in this NESCOR report.

Comparison of Security Features

The IEC TC57 WG15 on Security Standards for data communications within the Power Industry is standardizing security features for both 61850 and the international version of DNP3, IEC 60870-5. The following table lists the security standards that apply for these two protocols and all are in the IEC 62351 series. The IEC 62351 family of standards has been reviewed by the SGIP CSWG [49]. This family of standards is not yet in the CoS.

Table 3: Security Standards Applicable to IEC 61850 and IEC 60870-5

	Standards for Security of Networked Implementations	**Standards for Security of Serial Implementations**
DNP3	IEC 62351-3: Communication Network and System Security (TCP/IP) IEC 62351-5: Data and Communication Security (Other	IEC 62351-5: Data and Communication Security

	networked)	
IEC 61850	IEC 62351-3: Communication Network and System Security (TCP/IP) IEC 62351-4: Security for Profiles that Include MMS	IEC 62351-6: Data and Communication Security

IEC 62351-3 specifies how to provide confidentiality, tamper detection, and message level authentication for SCADA and telecontrol protocols that make use of TCP/IP as a message transport layer. This part of IEC 62351 specifies how to secure TCP/IP-based protocols through constraints on the specification of the messages, procedures, and algorithms of Transport Layer Security (TLS) so that they are applicable to the telecontrol environment of IEC TC 57.

IEC 62351-5 specifies messages, procedures, and algorithms for securing the operation of all protocols based on or derived from the standard IEC 60870-5: Telecontrol equipment and systems – Part 5: Transmission protocols. This specification applies to all least those protocols listed in the table below:

Table 4: IEC 62351-5 Standard and Applicability to Other Standards

Number	Name
IEC 60870-5-101	Companion standard for basic telecontrol tasks
IEC 60870-5-102	Companion standard for the transmission of integrated totals in electric power systems
IEC 60870-5-103	Companion standard for the informative interface of protection equipment
IEC 60870-5-104	Network access for IEC 60870-5-101 using standard transport profiles
DNP3	Distributed Network Protocol (based on IEC 60870-1 through IEC 60870-5 and controlled by the DNP Users Group)

IEC 62351-4 addresses IEC 61850 for the MMS profile. IEC 61850-8-1 makes use of MMS in a 7-layer connection-oriented mechanism. IEC 61850-8-1 is used over either the OSI or TCP profiles.

IEC 62351-6 specifies messages, procedures, and algorithms for securing the operation of all protocols based on or derived from the standard 61850. This specification applies to at least those protocols listed in the table below.

Table 5:IEC 62351-6 Standard and Applicability to IEC 61850

Number	Name
IEC 61850-8-1	Communication networks and systems in substations – Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO/IEC 9506-1 and ISO/IEC 9506-2) and to ISO/IEC 8802-3
IEC 61850-9-2	Communication networks and systems in substations – Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3

IEC 61850-6	Communication networks and systems in substations – Part 8: Configuration description language for communication in electrical substations related to IEDs

Both TCP/IP and DNP3 have defined security for serial implementations, addressing authentication and integrity, but not confidentiality. The assumption underlying this approach is that confidentiality is neither strictly necessary nor feasible for many of the serial applications of these protocols. This report does not evaluate these assumptions; it is most appropriate to evaluate them for a specific application scenario. The present effort has not performed a detailed technical comparison of the DNP3 and IEC 61850 security approaches for the serial case.

IEC 61850 Series

The conclusions below are based on the review of [50], [45], [41], [51], and [52] include the following.

Logical interfaces with remote protection (teleprotection of bay-level units), as well as logical interfaces with remote control centers (for remote control of functions/applications), are beyond the scope of the 61850 series ([50], pages 11 and 13). Alternatively, distributed functions require communication of Logical Nodes (LNs) with one another to execute specified tasks (in particular from an end-to-end perspective of WAMPAC applications). As such, potential cyber security vulnerabilities over these two interfaces need to be addressed as well.

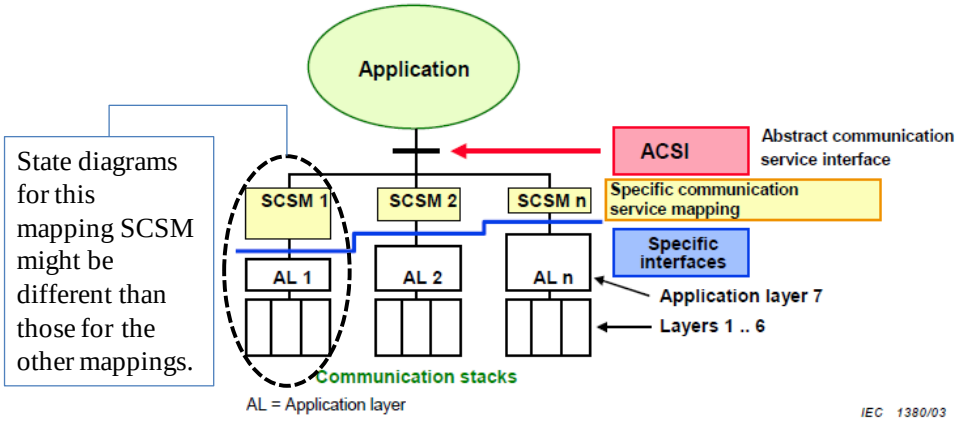
For any given function (e.g., distance protection), various attacks exist due to the communications required among the LNs to execute the function that they compose. For instance, expected reaction from an LN residing on a different physical device may be blocked to stop proper execution of that function. Cyber security considerations for 61850 are delegated to 62351, but this is not sufficient to stop various attacks that take advantage of the dependencies among various LNs (such as the general class of attacks just noted involving blocking of responses) or the protocol states composing these LNs. Therefore, state diagrams describing the internal of how 61850 LNs and functions act, as well as those of potential attacks being specified, need to be identified to better understand these attacks and how to mitigate them.

Furthermore, IEC 62351 specifications may not be sufficient for mitigating certain attacks, for instance those involving gained-access to a substation IED, those that are in the clear (e.g. GOOSE, GSSE, or SMV messages for the most part) which support real-time applications (hence their importance) (e.g. see [51] page 53), or those that rely on disrupting proper association establishment and/or closing by launching a Denial of Service (DoS) attack.

An example is the resource limitations of the substation IEDs: As noted in IEC 62351-1, substation IEDs are typically resource limited [45]. These limitations include constraints involving narrowband communications, processor speed, and memory size. These limitations pose an operational challenge to implement cryptography in IEDs to meet real-time requirements of GOOSE, GSSE, or SMV messages (e.g. those under 4ms of response time) [41]. Thus, these messages are exchanged as clear text without encryption (as suggested in IEC 62351-6, see section 4.1 in [41]), which exposes them to “man in the middle”, “tamper detection/message integrity”, and “replay” attacks broadly speaking. To mitigate this, 62351-6 suggests using a Message Authentication Code (MAC) to ensure message integrity (see section 7.2.2.1 in [41]), as

well as tracking of time by each 61850 client (whereby certain messages are denied by monitoring the timestamp properties, e.g. those exceeding 2min skew). However, these are not strong mechanisms to mitigate "replay" attacks and the like. Enabled by such clear-text messages, an adversary could alter the state number within a GOOSE message and preempt an existing legitimate message. Due to the clear-text nature of GOOSE, GSSE, or SMV messages, many other attacks can be staged (e.g. flooding of multicast GOOSE messages).

In addition, since actual sequence of messages implementing the desired applications (e.g. protection schemes) is beyond the scope of 61850 (e.g. see [51] page 54) and may differ from one vendor to another, an adversary could take advantage of these differences; for instance, potential repetition of GOOSE multicast messages could help their detection and "replay". Another attack would be blocking enable and/or disable messages for subscriptions by using a DoS attack, where an attack on enable hinders start of subscription and attack on disable subscription (with buffered reporting) can lead to data flooding and eventually hindering other



messaging– see Figure 144 in [51] for the buffered reporting mechanism. Specifics of such an attack depend on the SCSM being used for the application, which in and of itself raise another issue (that we note next). Similar attacks can be noted also for the log control mechanism (e.g. see page 40 in [51]).

Another attack is related to encryption: even if encryption is implemented, given the fast timing and the accuracy of the clock, a DOS attack can be staged involving key exchange mechanisms, which is also pointed out on page 6 in the PAP 13 report involving TimeToNextKey [50].

Since the focus of the 61850 family of standards has been on interoperability and interchangeability, as noted in [50], mapping of defined Abstract Communication Service Interface (ACSI) services onto actual protocols is not unique and will allow for the adoption of multiple protocol stacks (e.g. MMS over OSI stack or directly on Ethernet). Actual implementations of device interfaces to ACSI are outside the scope of 61850 ([50], page 18). While the use of various different SCSMs (Specific Communication Service Mapping) allows for implementation flexibility and diversity, potential cyber security attacks (even those of the same kind) manifests themselves differently since the internal state-diagrams (as noted previously) of different 61850 SCSMs would be different due to the mapping. Further, only applications using the same SCSM (i.e. those specified in 61850-8-x and 61850-9-x) would actually be interoperable ([50], pages 18 and 19), which somewhat defeats one of the main purpose of 61850. We would need to generate The state diagrams noted in the previous diagram for each SCSM need to be generated. While ACSI is independent of the SCSMs ([51], page 23),

the progression of protocol functions and hence cyber security attacks are dependent on these mappings.

Exchange of system parameter (in particular configuration and operational parameters) is also susceptible to various cyber security issues/attacks. While the syntax, semantics, and requirements of parameter exchanges are specified in 61850-6 [53], related cyber security vulnerabilities need also be addressed. It is well known that the majority of the cyber security vulnerabilities are due to misconfiguration of networked devices [23]. Therefore, there is a need to focus on configuration management in 61850 series and associated vulnerabilities. This will become even more important in the near future when WAMPAC applications, and the associated substation resources (e.g., for communication services), need to adapt to the power-system dynamics much more frequently and intelligently with large-scale penetration of renewables (such as wind power-plants).

IEC 61850 application association services are also vulnerable to getting hijacked, aborted, or released even with IEC 62351. This can be done be, for example, by terminating and re-establishing the involved TCP/IP sessions.

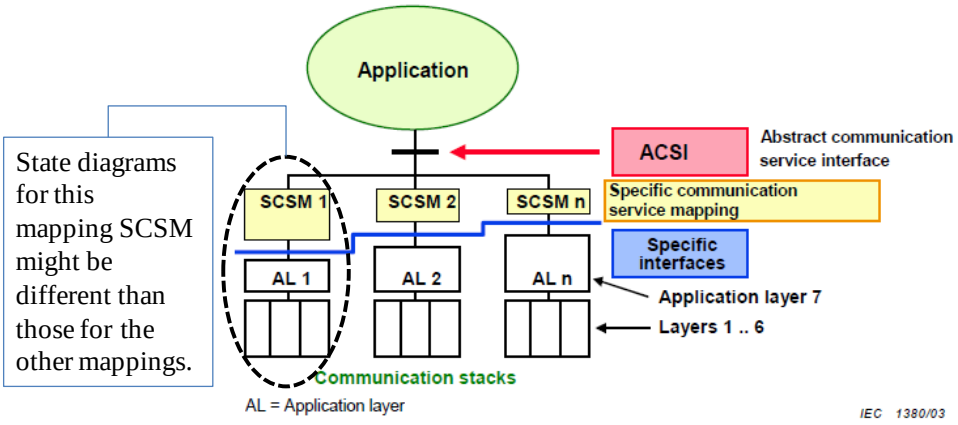


Figure 14: State diagrams for protocol actions and/or potential cyber security vulnerabilities differ from SCSM being adapted.

The most recent NIST CSWG report [52] presenting a review of potential cyber security vulnerabilities involving 61850 series is brief and only points out to specific subsections in 61850 series where cyber security requirements are specified.

IEC 61850-90-5 Series

The following describes attacks of IEEE C37.118 when synchrophaser information is transmitted using IEC 61850.

The first identified attack is caused by modifying the SCL file. Unlike “online access” mode, the phasor gateway configures the client in dependently of the PMU by importing an IEC-61850 Substation Configuration Language (SCL). This is called “offline access”. By intercepting the SCL file and sending the modified version to the phasor gateway, the PMU data frame can be misinterpreted by the phasor gateway. To launch this type of attack, the malicious node to

intercept the SCL file generated by the phasor manager. The intercepted or snooped copy of the SCL file is modified by the malicious node. Afterwards, the modified SCL file is sent to and imported by the phasor gateway. The phasor gateway processes the configuration data in the SCL file to prepare for receipt of the specific PMU's data stream. The modified SCL causes the phasor gateway to erroneously interpret the specific PMU's data stream. This is caused because the protocol designed for the phasor gateway does not need to check the frequency of SCL file import and the validity of the file's contents. To mitigate this type of attack, the frequency of dissemination of new SCL file can be checked and controlled. Also, the content of the SCL file needs to be inspected at the phasor gateway side.

The second attack is launched by attacking the PMU configuration data. For the 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. The phasor gateway sends the configuration request directly to the PMU. The PMU then sends that configuration data to the requesting client. The phasor gateway requires the PMU configuration information to process a new or re-configured PMU data frame. The PMU configuration data in the phasor gateway should match the current PMU configuration. A malicious node can initiate a request to provide the current configuration data from a specific PMU to a phasor gateway 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 that has been reconfigured and thus requires new configuration information to be provided to the phasor gateway. When the phasor gateway receives a request to update its configuration data for a particular PMU, it sends a request to the PMU for its current configuration data. For implementing utilizing the IEC-61850-90-5 standard, this consists of the phasor gateway reading the appropriate control block. The configuration data returned by the PMU after it receives the request is intercepted by the malicious node and modified. The phasor gateway receives the modified configuration data from the malicious node. It processes the configuration data to prepare for the specific PMU's data stream. Some validation, such as if the expected PMU responded, may be done as part of this processing. Once the phasor gateway has processed the PMU configuration data, it is now ready to receive the specific PMU's data stream. From the compromised configuration data, the phasor gateway will interpret the specific PMU's data stream incorrectly. To mitigate this type of attack, the frequency of configuration data modification should be monitored. The root cause of this attack is that the protocol is designed for the phase gateway to accept the configuration data as long as it is expecting the data from the PMU.

IEC 61970: Energy Management System Application Program Interface

This (2006) standard offers a common information model (CIM) and component interface specification for energy management systems within and between control centers. It specifies UML-based ontology with RDF indicated for data exchange.

This standard has many parts, as listed in the SGIP CSWG review [46]. The standard has not been incorporated into the SGIP CoS. Under the present effort, the study team reviewed in totality IEC 61970-501: Common Information Model (CIM) XML Codification for Programmable Reference and Model Data Exchange, and reviewed the publicly available abstracts from the remaining parts of the standard. Based upon this review, the team concluded that the scope of this standard is limited to knowledge representation—abstract models for

information. Thus the team concurs with the CSWG review (October, 2010) of this standard (2.2.2) that it "…does not (and does not need to) address security…"

The information that the standard is intended to represent however will tend to have related cyber security requirements. Its integrity and in some cases confidentiality will need protection both in transit and at rest. Tampering with such information might allow attackers to influence control center applications to fail. Information about the structure of power system data might enable specialized attacks to be formulated against an implementation.

For example, for PMU data to be available to remote applications, the measurement points (CIM terminals) are registered with a PMU registry, indicating identities, locations, and types of measurements produced. This registration information is sometimes modified thereafter to reflect changes to a previously registered PMU. The security profile minimally demands that no incorrect information is stored in the registry and that no unintended modifications or deletions occur. An attacker knowledgeable in the CIM might tamper with the registration message (e.g. as a man-in-the-middle) to declare an inaccurate measurement type or location or to alter the identity of an update to overwrite an existing (accurate) registration. These changes might cause subsequent transfers of measurement data to be misinterpreted at a central analysis site.

The identification of these specialized attacks depends upon the technology and architecture used to implement this standard. Specific implementations that reference the CIM or CIS will thus need appropriate safeguards, but nothing about such safeguards is prescribed by this standard.

C37.118 IEEE Standards for Synchrophasors in Power Systems

The Power System Relaying Committee of the IEEE Power & Energy Society sponsored this standard covering the measurement and communication of phasors in power systems. The original C37.118-2005 was a single standard. It was split into two parts: Part 1 covers measurement requirements and Part 2 covers real-time communications. The IEEE-SA Standards Board approved both parts in December 2011. These standards have not been reviewed by SGIP CSWG or identified as a candidate for the CoS. (However, IEC 61850-90-5 refers to this standard, and has been considered by SGIP.)

C37.118.1-2011 Synchrophasor Measurements for Power Systems

This standard defines synchrophasor measurement terms, performance requirements for measuring them, and means for evaluating compliance under various conditions. It does not address cyber security issues for communications or storage and refers to Part 2 (C37.118.2-2011) for all discussion of communications and recording. The most security-relevant aspect of this (Part 1) standard is that it sets stringent requirements for temporal accuracy and reporting latency that implementations must meet. These provide potential targets for an attacker wishing to disrupt WAMPAC. Neither this document nor C37.118.2-2011 specify features of an overall system or architecture that would allow it to continue to meet specified accuracy and timing requirements in the face of a cyber attack. Examples of such attacks would be spoofing of GPS time signals or flooding attacks that slow down network communications.

C37.118.2-2011 Synchrophasor Data Transfer for Power Systems

This standard defines messages, data types, and formats for communications between phasor measurement units, phasor data concentrators and related applications. Section 5 sets out a

simplified network architecture with local, corporate, and regional entities sharing data from PMUs (Figure 2 of the standard). This includes the roles of the phasor measurement unit and phasor data concentrator. Section 6 describes a messaging framework that encompasses data, configuration and header information messages from PMUs/PDCs, and commands sent to PMUs/PDCs. A CRC checksum is specified for frame transmission error detection (Annex B), however the framework implements no error or retransmission messages. There is no prescription for cryptographic assurance of authenticity or of confidentiality.

Annexes E and F (informative) of this standard discuss communications methods involving the serial and IP protocol suite. Multicast UDP is noted as having particular value in this application since it allows numerous clients to receive the same set of frames while minimizing transmission load; clients may come online or go offline randomly. Annex F contains the principle reference to cyber security in the standard:

> *Cyber security must be addressed with the communications used to transport synchrophasor data. This annex describes only methods that have been implemented to date and does not attempt to prescribe measures that may be applied in the future. Users of these methods need to be aware of the risks of unsecured communications and should consider adopting more secure methods.*

The Annexes (E, F) do not reference any of the existing methods of transport security, e.g. IPSEC, TLS. The annexes also do not describe the types of attacks that might be mounted by spoofing command or data frames, sniffing traffic, or meddling with intermediate routers. Of particular concern will be the identification of secure communication methods that meet the hard real-time requirements in C37.118.1-2011.

C37.238 (with Precision Time Protocol, IEEE 1588-2008)

The following describes the attacks of PTP (Precision Time Protocol, IEEE 1588-2008) used in conjunction with the standard profile defined in PC37.238.

The first attack vector is to impersonate the master clock. In PTP, the best master clock (BMC) algorithm performs a distributed selection of the best candidate clock based on the following four clock properties: identifier, quality, priority and variance. An identifier is a universally unique numeric one for the clock. This is typically constructed based on a device's MAC address. The quality of a clock is quantified based on expected timing deviation, technology used to implement the clock or location in a stratum schema, although only V1 knows a data field stratum. PTP V2 defines the overall quality of a clock by using the data fields "clockAccuracy" and "clockClass". The priority of a clock is an administratively assigned precedence hint used by the BMC to help select a grandmaster for the PTP domain. IEEE 1588-2008 features two 8-bit priority bits. The variance is a clock's estimate of its stability based on observation of its performance against the PTP reference. IEEE 1588-2008 uses a hierarchical selection algorithm based on the following properties in the order indicated: Priority 1, Class, Accuracy, Variance, Priority 2, Identifier (for tie-breaker). By stealing the current master clock's identity, the rogue clock can force the slave clock to switch to itself and disrupt the clock system of the slave clock. Assumed here was that the adversary possesses capability to intercept and modify the PTP Sync messages while residing inside the domain.

The rogue clock first snoops the communication from the legitimate clock to other slave clocks. The Sync messages are carefully snooped to retrieve the grandmaster's clock information such sequenceId or Uuid. Once this information is intercepted, then the rogue master clock sends a "best" Sync message to the slave clock. The Sync message wins other Sync messages from legitimate master clocks. The victim slave clocks will run the BMC election process and pick the rogue master clock as their master clock, then switch to the rogue master clock. By forcing the victim slave clocks to switch to a rogue clock master, their clock synchronization mechanism is disrupted and produces incorrect timing information. To mitigate this kind of attack, the frequency of new master clock election and the identity of a newly elected master clock should be carefully monitored. This type of attack is made possible because the protocol is designed for the slave clock to switch to a different master clock whenever the master clock wins the BMC election process.

The next identified attack is to illegally update the sequence ID in the Sync message. A slave clock performs the synchronization with the master clock first by inspecting the sequence ID of a Sync message. If the sequence ID contained in the Sync message is lower than the number last seen, it discards the Sync message. By continuously sending a legitimate Sync message with a higher sequence ID to the victim slave clock, the victims slave clock will not process the Sync messages from the legitimate clock master. To launch this attack, the rogue clock master sends a Sync message with a sufficiently higher sequence ID than the legitimate sequence ID. The victim slave clock will updates its last Sync ID to this wrong sequence ID. When the legitimate master clock sends a Sync message with the next sequence ID, this message is rejected by the victim slave clock since the sequence ID contained in the Sync message is lower than the sequence ID recorded from the rogue clock master's Sync message. By continuously sending Sync messages by incrementing the sequence ID sufficiently, the legitimate clock master cannot keep up the speed the sequence ID is increased in the slave clock, which prevents the slave clock from ever synchronizing with the legitimate master clock. This type of attack may be preventable if the sequence ID increment is inspected from any clock master. It should be detected that any such increments continuously keep other master clock from synchronizing other slave clocks. This type of attack can be performed the protocol is designed for a slave clock to update its next expected sequence ID based on the sequence ID recorded in the incoming Sync message.

The next attqack is to masquerade as the time stamp in the Follow-up message. The time synchronization in PTP is performed based on the timestamp information contained in the timing-related messages such as Sync, Sync Follow-up, Delay request, Delay response messages. The slave clocks determine the offset between themselves and their master. The master periodically broadcasts the current time as a message to other clocks. Under IEEE 1588-2008, up to 10 messages per second are permitted. Not all masters have the ability to present an accurate time stamp in the Sync message. It is only after the transmission is complete that they are able to retrieve an accurate time stamp for the Sync transmission from their network hardware. Masters with this limitation use the Follow-up message to convey the time stamp information. By masquerading the timestamp information in the Follow-up message, the incorrect time synchronization can be legitimately performed by the victim slave clocks.

To launch this attack, the rogue clock master can put wrong time stamp information in the "originTimestamp" field of Sync messages. Modification of the time message can be achieved by blocking the transmission of the original message, and subsequently injecting the modified message back into the communication channel. By tempering within the timestamp fields in the

Sync message, the rogue clock can cause an incorrect resynchronization of the slave clock(s) or a miscalculation of the network latency. To mitigate this attack, the time stamp fields in the Sync message should be monitored and the time stamp value that exceeds some threshold needs to be inspected. This type of attack can be launched because the protocol is designed for a slave clock to use the time stamp value in the Sync message without checking the valid range of the value.

The final attack identified is caused by delaying the timing messages. The time synchronization in PTP is performed based on the packet arrival time of timing messages such as Sync messages. The slave clocks determine the offset between themselves and their master based on arrival these messages. By delaying the arrival of messages at the recipient nodes, the rogue node can cause an increase in the values used in the offset and one-way delay calculation. To launch this type of attack, the rogue clock master intercepts the timing messages between the master and slave nodes and later re-injects the intercepted messages into the communication channel. By intentionally delaying the reception time of the Sync message by the slave clock, the attacker may dramatically increase the offset of the slave clock with respect to the master clock, setting the slave clock off synchronization with the rest of the system. Delaying the reception of the Follow-up message at the slave clock can also cause a timeout of the synchronization event. If this condition continues, it may lead to the slave clock being denied synchronization with the master. The slave will either pick the wrong clock on the subnet to synchronize with, or operate based on its local clock, eventually drifting from the true master clock. To mitigate this type of attack, an abnormal delay of timing messages should be determined. If this abnormality is found for an extended period of time, validation of the data against other neighboring nodes should be performed. This type of attack is possible because the protocol is designed for a slave clock to record the arrival time of timing messages without checking its valid range.

IETF RFC 6272 Internet Protocols for the Smart Grid

This 2011 IETF informational RFC (request for comments) discusses the potential applicability of the IP-based protocol suite (IPS) to applications in the smart grid. The IPS is quite extensive and much of it has been heavily tested and hardened by field use. This RFC covers many protocols, but none of them in great depth. It is best considered as a road map with extensive references for further study. The smart-grid orientation is broad, and was not aimed specifically at WAMPAC. For example, the RFC notes the NTP time protocol, but does not consider whether it is a good match to the stringent performance requirements of WAMPAC. While the bulk of the RFC was written from a general data communications perspective, Appendix A describes a smart grid specific example: an advanced metering infrastructure based on IPS. This application is more directly applicable to customer end points than to grid-wide measurement.

RFC 6272 is not specifically focused on security. However, every IETF specification needs a section on security considerations (per the guidelines in RFC 3552), and this one has two relevant subsections. Section 2.2 reviews security goals and threats at the physical, network, transport and application layers. Section 3.1 offers a “security toolbox” - existing building blocks to address threats. This is done largely through reference to other RFCs (although it also cites IEC 62351-3). The subsection on authentication, authorization, and accounting refers to RADIUS, Diameter, EAP, PANA and 802.1X. The subsection on network layer security cites IPSEC (including ESP, AH, and IKEv2). At the transport layer, this RFC cites TLS, a protocol familiar to most web users, but with broad applicability. At the application layer the RFC cites CMS, the cryptographic message syntax, a signing and encryption standard that influences

various other standards. For example, CMS may be used to protect the firmware packages embedded in field devices (RFC 4108). Specific application protocols noted include PKIX, Kerberos, OAuth, SSH, and S/MIME.

In terms of WAMPAC or any other smart-grid application, the security sections of this RFC serve as a catalog of proven methods to consider to meet the security needs for the application, once these are identified. This RFC does not recommend specific methods or combinations of methods for any specific application, other than the illustrative meter infrastructure example in Appendix A. These conclusions are consistent with the review performed of this document by SGIP CSWG [37]