HOW A UTILITY CAN USE ASAP-SG SECURITY PROFILES

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

Draft v0.12 – October 20, 2011

1 Introduction

This document describes several different ways that ASAP-SG[1] security profiles can be used to improve the security of smart grid systems. We assume that the business decision to create or modernize a system has already been made and that procurement will be an important element of the project. We do not assume a particular procurement process or how project responsibilities may be distributed across particular organizational units. Instead, we focus our discussion on elements that are integral to any smart grid project—elements like sets of requirements, designs, and procured or internally developed equipment or systems—and how a security profile can be used (for example) to help create, test, or configure these elements.

ASAP-SG security profiles document recommended security controls tailored to the needs of specific smart grid application areas such as advanced metering infrastructure, distribution management, or synchrophasor systems.[2] Each security profile contains security recommendations that are specific to a particular application area (based on defined functionality, assumptions, and security objectives). Understanding the match between the needs of your smart grid project and those documented in one or more profiles lets you know what is addressed by the profile and what you need to add (or remove) given your specific needs. The keys to effectively using a security profile in a smart grid development project (including procurement) are:

1. Finding the right security profile(s) and determining which portions of the security profile(s) apply. You need to select the security profile(s) that best address your project's smart grid application area. For projects that span application areas, more than one profile may apply.

2. Aligning the security recommendations with the elements of your intended system design. Some security controls will be needed across multiple devices being procured, others may apply to only a few devices, and others still may be handled outside of the new devices being procured (e.g., through the configuration of network segments).

[1] ASAP-SG is the Advanced Security Acceleration Project for the Smart Grid, a utility-driven public-private collaborative effort that develops security recommendations and guidance in support of the UCAIug Smart Grid Security Working Group, and the larger smart grid community.

[2] Synchrophasor systems are also known as wide-area monitoring, protection, and control (WAMPAC) systems.

3. Using the security profile to support the appropriate activities throughout a project's lifespan. The most obvious use of the security recommendations found in a security profile is to include them in Requests for Proposals (RFPs) for new devices and systems. Security profiles also can, and should, support other activities such as design reviews, acceptance testing, commissioning, deployment, and maintenance activities.

Much of the advice found in this document is accompanied by examples taken from the Security Profile for Wide-Area Monitoring, Protection, and Control (WAMPAC)[3], as it represents the most current iteration of the ASAP-SG process and therefore has the richest set of features and attributes to support asset owner efforts to specify, procure, and deploy secure systems.

2 Finding the right security profile(s)

ASAP-SG publishes its security profiles on SmartGridiPedia.[4] As of the writing of this document, four security profiles are available:

- Advanced Metering Infrastructure (AMI)[5] - This document provides guidance and security controls to organizations developing or implementing AMI solutions, and aims to provide prescriptive, actionable guidance for how to build-in and implement security for AMI smart grid functionality. This guidance is neutral to vendor specific implementations and architectures. The scope of this work extends from the meter data management system (MDMS) up to and including the home area network (HAN) interface of the smart meter.
- Third Party Data Access (3PDA) - This document delineates the security requirements for individuals, utilities, and vendors participating in a three-way relationship that involves the privacy and handling of sensitive data. Specifically this document is intended to address the concerns of electric utility customers who want to allow value added service providers to access electric usage data that is in the custody of the customer's utility. Other three-way data sharing scenarios may also be addressed using this profile, as the roles of the three parties have been abstracted in such a way as to support mapping to different environments.
- Distribution Management (DM) - This guideline identifies best practices for securing automated distribution management (DM) functions in a smart grid environment, including steady state operations and optimization. This document addresses concerns related to using

[3] Available on SmartGridiPedia at http://www.smartgridipedia.org/images/5/5e/WAMPAC_Security_Profile_-_v0_08.pdf.

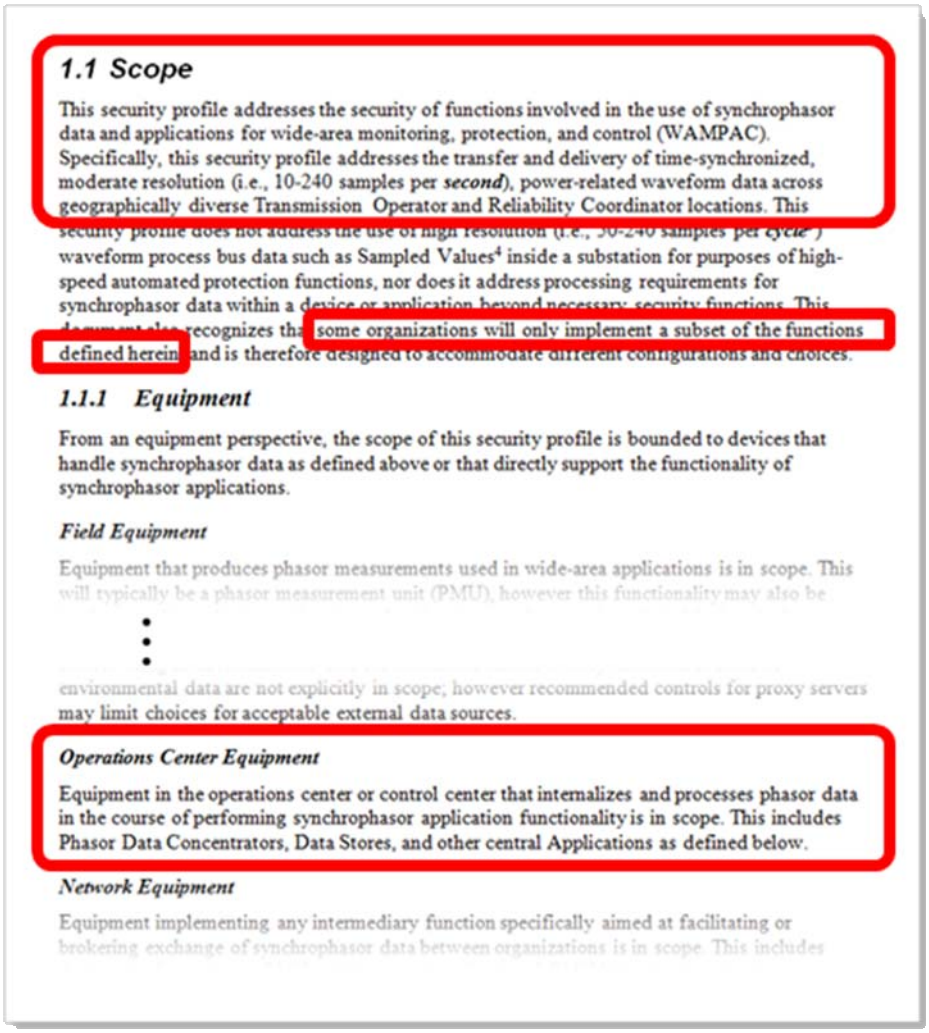
[4] http://www.smartgridipedia.org/index.php/ASAP-SG

[5] This first security profile did not have many of the components described herein, and is being re-worked according to the current ASAP-SG security profile design method by the AMI Security Subgroup within the NIST Smart Grid Interoperability Panel (SGIP) Computer Security Working Group (CSWG).

communications and automation in field equipment that controls the configuration and operation of the electric distribution system. Other electric system operation scenarios may also be addressed using this profile, as the various roles defined herein have been abstracted in such a way as to support mapping to different environments.

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

Each profile addresses different, but interacting, elements of potential smart grid applications. While the names of the profiles are a good indicator of their intended use, each security profile contains a Scope section that defines what is included and excluded from the profile in terms of functionality and key system elements. Figure 1 shows the scope statement for the WAMPAC security profile.



1.1 Scope

This security profile addresses the security of functions involved in the use of synchrophasor data and applications for wide-area monitoring, protection, and control (WAMPAC). Specifically, this security profile addresses the transfer and delivery of time-synchronized, moderate resolution (i.e., 10-240 samples per ***second***), power-related waveform data across geographically diverse Transmission Operator and Reliability Coordinator locations. This security profile does not address the use of high resolution (i.e., 30-240 samples per ***cycle***) waveform process bus data such as Sampled Values[4] inside a substation for purposes of high-speed automated protection functions, nor does it address processing requirements for synchrophasor data within a device or application beyond necessary security functions. This document also recognizes that some organizations will only implement a subset of the functions defined herein and is therefore designed to accommodate different configurations and choices.

1.1.1 Equipment

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

Field Equipment

Equipment that produces phasor measurements used in wide-area applications is in scope. This will typically be a phasor measurement unit (PMU), however this functionality may also be

-
-
-

environmental data are not explicitly in scope; however recommended controls for proxy servers may limit choices for acceptable external data sources.

Operations Center Equipment

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

Network Equipment

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

Figure 1: Excerpt from the Scope section of the WAMPAC Security Profile

Your first step is to determine if portions of your current project are within the scope of any security profile and which portions of applicable security profiles pertain to the current project (i.e., *read the scope and decide if that sounds like the kind of system you're trying to build*). Examining the use cases in a particular security profile will give you further information to help you determine how closely the security profile matches your needs. The profiles are written with the knowledge that some organizations will only implement a subset of the functions described in the profile. Profiles provide traceability to allow an organization to determine which security guidance is applicable to a project's intended functionality.

3 Aligning security recommendations with intended design

Assuming one or more security profiles are applicable to your project, the next step is to determine which guidance applies and to what each piece of guidance applies.

3.1 Which guidance is relevant?

A profile's security controls are derived from the intended functionality of a system (documented in detailed use cases) and high level security and operational objectives. If your smart grid project is intended to perform all of the functions as defined in the scope of the profile, then all guidance applies. If it only includes a subset of the scope, then some guidance may not apply. In such situations, determining which guidance does not apply starts with an examination of the use cases.

Determine which use cases from the profile represent functionality that will be present in your system. All controls that link to these use cases are applicable. Use the traceability information in the profile to find this set of controls. The specifics are a little different from profile to profile, but the essence of the approach is to:

- map real-world system elements to the roles or network segments defined in the security profile
- identify the set of use cases your project will implement and verify the functions each system element will perform as defined by the roles and network segmentation
- look up the controls as they are mapped against the defined roles and network segments
- apply the controls to the system elements that satisfy the corresponding roles or serve as designated network segments

3.2 How does the guidance relate to my project?

Each security control in a profile applies either to roles, networks, or organizations. For example, specific roles must implement some controls while other controls must be satisfied by the manner in which supporting networks are configured. Yet other controls represent organization practices that must be followed.[6]

The different sections of a security profile specify the subject of each control. For the WAMPAC profile, Section 4.3.1 contains a table that lists all controls that must be implemented by individual roles and specifies which controls must be implemented by each role identified in the profile. Section 4.3.2 lists all controls that pertain to network segmentation and specifies which apply to each network segment identified in the profile.

Profile guidance, however, is written against an abstract (or logical) architecture that must also be mapped against the intended concrete architecture being used for the smart grid project. Profiles use abstract architectural concepts because different utilities and vendors package similar functionality in very different ways. For example, the aggregation of readings from different phasor measurement units (PMUs) can be done in the field or in a control center; it can also be stand-alone functionality or packaged with other functionality. The security profiles abstract the essential functionality needed to achieve their particular scope into a collection of "roles." Each role in a profile is clearly defined and one

[6] This varies among the profiles. The WAMPAC security profile does not include organizational security controls.

task for the architect, possibly in conjunction with vendors, is to map the actual equipment being considered into the roles described in the profiles. For example, the control center Alignment role in the WAMPAC security profile is defined to be:

> "The role that executes in the control center, and collects multiple PMU samples with equal timestamps into a single time-aligned super packet. Alignment does not function as a persistent repository, and data is retained (or buffered) only until it is transmitted, discarded, or stored persistently (e.g., if data arrives too late to be collected in a super packet).
>
> The responsibilities of the Alignment role are:
>
> - Aggregate incoming data for the current time period into a super-packet
> - Buffer incoming data until all data has been received
> - Monitor the clock (GPS) and determine when data has reached maximum allowable time lag
> - Send data to the Data Store as appropriate
> - Interact with other roles to ensure the PMUs are correctly configured and that the Alignment is correctly configured to receive the PMU data
> - Interact with PMUs to control their data streams"

The roles defined in a profile are *abstract* or *logical* roles; that is, each role does not necessarily map one-to-one with a device or system. It is possible for a device to implement the functionality of multiple roles. However, it is also possible for the functionality of one role to be split among more than one device. Establishing the mapping between logical roles and devices and systems in the concrete architecture allows security controls applicable to a role to be mapped against the appropriate elements of the actual system that are being developed or procured.

4 Using a security profile throughout a project's lifespan

The most obvious use of a security profile is as a source of security requirements, which can in turn be used for RFPs. While this is a very effective use of a security profile, profiles can and should support other activities throughout a project's lifespan. The details will, of course, vary based on organization-specific division of responsibility and established engineering practices, which most notably includes procurement.

This section presents an overview of potential ways that security profiles *can* be used in a project's lifespan; however, an organization need not perform them all to gain benefit from a security profile. The ideas underlying these activities are to inform key decisions, validate that guidance is being followed, and to do so as early as feasible in order to reduce risk and potential rework costs.

A typical smart grid project brings together stakeholders from multiple areas of the organization and with different areas of expertise[7] for the common purpose of designing, procuring, and ultimately deploying a system of interest. Figure 2 shows some of the key artifacts involved in such a project:

[7] Examples include project managers, power system engineers, IT specialists, architects, operations, business unit procurement, and corporate procurement.

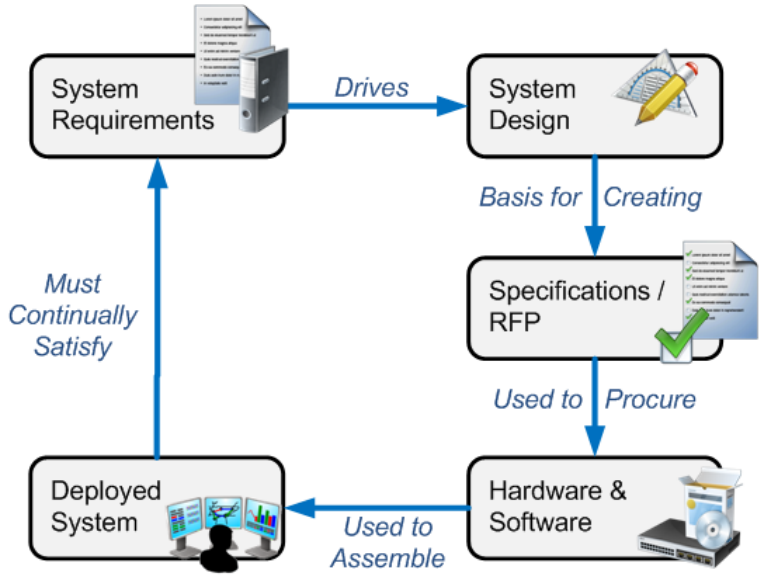


Figure 2: Key artifacts involved in development and procurement activities

- System requirements: These include functional and non-functional requirements (including security) that will drive the design, implementation, and deployment of the system. High level requirements likely exist before the business decision to develop and procure a system is made. These requirements are likely refined as the system design is created.

- Design: This includes architectural and detailed design specifications, which may be created by the utility or vendors. The design must satisfy the system requirements, which often involves balancing multiple concerns (e.g., security vs. risk vs. cost, incorporation of legacy assets, and conformance with regulatory requirements).

- Specifications/RFPs: Each element of the system (e.g., equipment, systems, and software applications) must have its own specifications, including security requirements. These granular specifications must conform to the design and contribute to the resulting system's satisfaction of the system requirements. These specifications are often for elements that must be procured and are collected in Requests for Proposal (RFPs) that are given to vendors.

- Hardware & Software: Each element of the system (e.g., equipment, systems, and software applications) must satisfy its subset of the system specification. Equipment and software must also be configured for the utilities particular needs and maintained over time such that the deployed system satisfies the overall systems requirements throughout the system's lifespan.

- Deployed system: Procured or developed equipment and software are assembled and (typically) integrated with an existing system to create the new deployed system. This new system must be configured and tested to ensure initial satisfaction of the overall system

requirements, and then maintained over time to ensure continued satisfaction of its requirements.

A smart grid project includes a number of activities involving these elements. Requirements and designs have to be created. Equipment and systems must be procured (or developed), configured, deployed, and maintained. Most every element must be reviewed or tested at some point to ensure that it meets the needs defined in previous steps, and again periodically to ensure it continues to meet those needs throughout the life of the system. In the remainder of this section, we describe how security profiles can be used to support (not replace) these kinds of activities (a high level overview of this support is shown in Figure 3). Note that we do not prescribe a particular order for the activities, nor which stakeholders must be involved in the activities. Individual organizations will have to decide how much resources to commit (and when) based on factors like available budget, schedule, staff expertise, and risk tolerance.

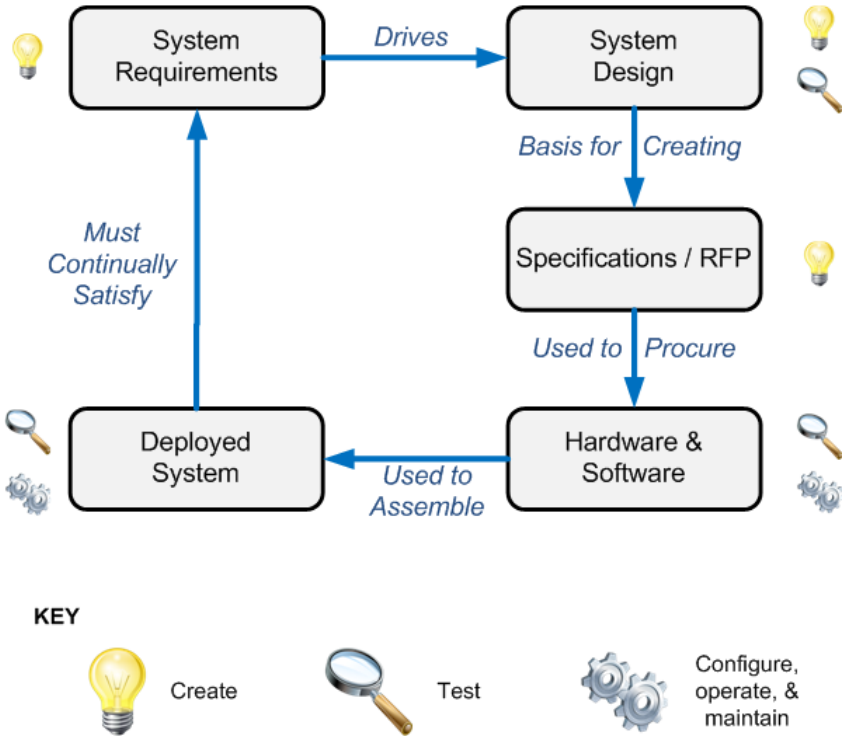


Figure 3: Security profile support for development and procurement processes

4.1 Creating or refining system requirements

Some of the core elements found in a security profile are the lists of security principles and objectives. These lists and the assumptions they reflect form the basis for the decisions made in selecting security controls, and they should be consulted during creation or refinement of system requirements to ensure alignment with organizational objectives. While an organization may have goals beyond those in a

profile, a typical system requirements document should at least cover[8] those found in any relevant profiles. Discrepancies between organizational objectives and those in the profile should be examined carefully to identify risks associated with a dismissed objective, as gaps at this level are likely to have significant impact. If security requirements (even high level requirements) are not identified and agreed upon early, subsequent design and implementation activities may include decisions that are detrimental to system security.

Security profiles also contain much more detailed, fine-grained security controls. These controls are often defined at a level suitable for individual pieces of equipment or software, though some are at more of a system level (e.g., controls affecting network segmentation). Many of these controls may be too specific for early system requirements work, but should be consulted as system requirements are refined into more specific and enforceable statements. At whatever level system requirements are expressed, they should be complete enough to imply a need for each of the specific controls found in applicable profiles. For example, abstract system requirements should reflect all of the concerns addressed by the specific controls so that later refinement to such specific controls does not introduce new security needs.

In some cases, reference to a profile as a whole may be an appropriate use – for example, if an organization intends to select a primary vendor[9] and delegate creation of system requirements to that vendor. In such situations, it is imperative to address *all* of a project's requirements and goals, including security and other non-functional attributes, as part of the selection process. Specifying that the vendor is expected to at least satisfy the security controls specified in a particular security profile is one way to accomplish this (at least, with respect to security). It is also a good idea to request that the potential vendor provide evidence-based assurance that those requirements have been or will be satisfied.

4.2 Creating or evolving designs

Security profiles contain detailed use cases describing the functional behavior of smart grid applications. Study of these use cases during the design process will help ensure that the functions presumed to be part of the system in the security profile map to the functions that the organization intends to deploy.

- The designers of the system should determine how each use case from the relevant security profile(s) maps to the desired functionality that the organization intends the deployed system to provide.

[8] A security objective can be "covered" by including it directly or by providing a more general statement that is at least as strong as the objective.

[9] A primary vendor could be one that will coordinate and integrate the design, procurement, integration, configuration, deployment, and maintenance of the equipment, services, systems, and software applications needed to the construct the supporting technology infrastructure for the project. The primary vendor could also be responsible for subcontracting with other vendors to provide needed technology and services for the project.

- Where the functionality as documented in the security profile matches how the organization wants the system to work, the security profile use cases can be incorporated into the system's design.

- Where the organization's desired functionality differs from the use cases in the security profile, these differences will have to be examined to determine if they imply a need for additional security controls. Security controls identified in the security profile are intended to cover failures of the use cases. So if additional functionality is built into the system, that functionality should also be examined for potential failures and corresponding need for additional controls.

Security profiles also contain logical architectures that depict roles that must be present in the system to provide the functionality described in the use cases. These roles match those used to document the included use cases. As described in Section 3.2, security profiles describe the logical architecture in terms of abstract roles. On the other hand, the system implementer will likely describe the design in terms of more concrete elements (e.g., due to specific technology, vendor, or product decisions). Those using the security profile as a basis to examine the security needs associated with a system's intended functionality should perform a mapping between the system elements as referenced in project documentation and the logical roles[10] as referenced in the security profile. The user should then compare the actual system design (through the lens of the mapping) to the logical architecture to ensure that all potential interactions from the profile are included in the design. The details of these interactions can be found in the use cases, which should also be examined through the lens of the element-to-role mapping.

Intended network architectures should also align with the network segmentation prescriptions contained in the security profiles. Profiles describe how networks should be segmented, which segments different roles are allowed to be deployed in, and provide security controls that should be implemented in the network infrastructure. The network architecture (or view) of the design should conform to this guidance. In fact, it may be helpful to use this guidance as a starting point for the design of the network architecture.

4.3 Reviewing designs

The entity ultimately responsible for the system should review and analyze all designs for fitness,[11] whether the designs were created in house or developed by a vendor or contractor. Part of this review

[10] Security profiles also include examples of such mappings, which can be consulted to see some of the options that have been used elsewhere.

[11] Fitness of a design includes satisfaction of many criteria, such as feasibility, cost, and compatibility with existing systems. In this document, we are concerned with security issues. In this context, fitness means that if the design is correctly implemented, then the resulting system will satisfy our security goals and requirements. If the design is too vague on security issues, this is difficult to achieve.

should explicitly address security, and security profiles contain a great deal of information that can be used as review criteria.

- Designs should be analyzed to determine if they provide sufficient guidance to ensure that the security principles and objectives found in the relevant profiles will be satisfied. This task is simplified if the design contains evidence-based arguments to this effect (e.g., documented evidence demonstrating security control fulfillment).

- Designs should be reviewed to determine if all intended functionality is protected. Security profiles document functionality with use cases. The profiles correspondingly document protection of that functionality with controls required of the roles participating in those use cases.

- The design's network architecture should be reviewed for conformance with the profile's prescribed network segmentation and network controls. The network architecture should also ensure that the deployment of system elements in network segments conforms to the allowable deployment of roles to segments in the profile.

- All controls that are required by the profile should be allocated to the appropriate elements of the system design. In most cases these controls are allocated to abstract roles in the profile, so design elements must be mapped to these abstract roles such that the controls may be allocated to the corresponding design element(s). Other controls are allocated to the network or other infrastructure in the profile, so the user must identify the corresponding design element(s) (e.g., subnet or firewall) to allocate the control.

Any risk analysis that is performed as part of the design or part of review of the design should incorporate the failures documented in the security profile. Security profiles also associate security controls with the failures that they address. This information can also be incorporated into the risk analysis, assuming the security controls from the profile are also incorporated into the actual system design.

4.4 Creating requirements and RFPs

System designs may be comprised of several different design elements, including equipment, software, infrastructure (e.g., networks), or other interacting systems. Any of these elements that do not already exist must be built or procured. As such, each must have a set of requirements (sometimes captured in an RFP) that the element must satisfy.

Most security requirements found in a security profile are security controls mapped against logical roles. These controls can be included verbatim in requirements documents or RFPs for system elements. To find the appropriate set of technical controls:

1. Identify a design element to be built or procured.

2. From the security profile, identify the abstract role or roles that are to be provided by that design element.

3. Find the set of technical controls allocated to each identified abstract role (usually found quickly by looking in a table in the security profile, such as Table 15 – Controls Mapped to Roles in the WAMPAC security profile).

4. Combine all controls identified in step 3 to form the complete set of security controls for the design element (removing any duplicates, of course).

Note that the mapping between roles and system elements may not be one-to-one. For example, the software (e.g., an application) and the hardware on which it is deployed (e.g., a server) that together implement a role may be acquired separately. In such cases, determine which security controls are to be implemented in each element and ensure that all controls are allocated to at least one.

Other security requirements in a security profile are security controls mapped against network segments. These controls may not be mapped against individual design elements, instead being mapped against collections of design elements. One of the primary ways collections of design elements are characterized is by how multiple elements are deployed and connected (e.g., partitioned into network segments). As above, mapping design elements to abstract roles will also be necessary in order to include the appropriate controls for each design element.

4.5 Testing hardware and software

Each piece of hardware and software that is built or procured should be tested to ensure that the appropriate security requirements are satisfied. Testing of hardware and software may be performed at different times. This testing may be done

- during product or vendor evaluation (i.e., prior to a procurement decision)
- as part of an acceptance test (e.g., on product delivery)
- after being configured for how the element will be used in the system (e.g., in an isolated test environment, prior to deployment)
- upon deployment
- each time the element is patched or updated
- periodically, as part of a regular security review

Tests for such hardware and software elements should address security requirements, as well as functional requirements. Appropriate sets of security controls for different hardware and software elements can be found in security profiles. To identify the appropriate security controls for a specific piece of hardware or software, follow the steps in Section 4.4.

The definition of each identified security control should be used as input for constructing one or more tests to determine if the control has been satisfied by the element.

4.6 Configuring, operating, and maintaining individual hardware and software elements

Some security requirements are not satisfied by system elements in their default configurations. Instead, such elements often need to be configured in specific ways in order to satisfy security requirements. For example, good security practices require that default system passwords be changed and that unnecessary services be disabled before a system element is used in a live environment. These requirements, however, are not always satisfied "out of the box," and may require additional work by utility personnel or system integrators.

Security profiles include controls that identify the need for such configuration changes, but the precise configuration changes to be made can only be determined with knowledge of a delivered system element. In some cases, a vendor (if provided with appropriate security requirements) may notify a utility that satisfaction of some requirements requires utility configuration. Otherwise, using a security profile to generate test cases for hardware and software (as described in Section 4.5) is a means to identify such cases.

1. Examine all test cases that are not initially satisfied.
2. Review product documentation (or speak with the vendor) to determine if there exist configuration settings that would change the system element in way that would pass the tests.[12]
3. Configure the system element and repeat the tests.
4. Note any configuration changes required to ensure that security requirements are satisfied. It is important to ensure that these settings be maintained over the life of the system element (or changed appropriately in response to security notifications by the vendor or advisories from authoritative security organizations). Such configuration settings may make important checklist items for current and future employees.

Some security profiles also includes operational security controls (e.g., setting maximum periods between malware scans) that should be followed in day-to-day operations. These controls are typically called out in a separate section of the profile and can be used as input to utility policies and procedures.

Security is an ongoing effort, and it is important to revisit these actions (as well as those in Sections 4.5, 4.7, and 4.8) whenever hardware, software, and other system elements are patched, upgraded,

[12] Of course, this step can be done without Step 1, and is often more efficient, particularly for experienced engineers.

replaced, or reconfigured. The security controls found in a security profile should continue to be satisfied throughout the operational lifetime of the system, not just when first deployed.

4.7 Testing a system

Like individual pieces of hardware and software that are procured or built for the system being developed, the integrated system itself must be tested. Likewise, this testing may be performed at different times, including

- as part of an acceptance test (e.g., on system delivery)
- after being configured for use (e.g., in an isolated environment, prior to deployment)
- upon deployment
- each time the elements of the system are patched or updated
- periodically, as part of a regular security review

Of course, system testing may not always encompass the entire system, but rather portions thereof (e.g., early integration testing of portions of the system).

This testing may repeat the testing of individual hardware and software elements, though in the context of other system elements rather than a test harness. Such tests should address security requirements as well as functional requirements. As described in Section 4.5, requirements for security tests and their applicability to different system elements can be found in security profiles.

Additionally, some security requirements span multiple roles or heavily depend on infrastructure configurations (for example, security requirements regarding how system elements are deployed on a network or which network segments are allowed to be connected to each other). Security profiles also contain such security requirements, which can be used to generate additional system-level security tests. To identify such security controls, find all security controls that are allocated to network segments, rather than individual roles (in the WAMPAC security profile, these are summarized in Table 16).

4.8 Configuring, operating, and maintaining a deployed system

Like individual system elements, the system as a whole must be properly configured, operated, and maintained in order to continue to satisfy security requirements. Security profiles contain guidance that can be used to assist in this mission. This task at the system level is similar to the equivalent task at the individual system element level (as described in Section 4.6).

In particular, security profiles contain controls constraining the configuration of network segments. Many of these controls can only be satisfied by a conforming configuration of network assets. Network assets should be assigned to network segments that are designed for specific and tightly-scoped purposes. A recommended minimal decomposition of network segments is provided in the

corresponding security profile, although more complex arrangements may be necessary depending on the size and mission of the system in question. At a minimum however, the system owner should:

1. Ensure that no single network segment serves more than one purpose as defined in the security profile.
2. Map network assets to the roles as defined in the security profile.
3. Ensure network assets are allocated to the appropriate network segments as constrained by the network segmentation controls in the security profile.
4. Ensure each network segment satisfies the required security functionality as defined by the network segmentation controls in the security profile.

For systems in initial deployment or substantial re-configuration, owners and operators can use the security profile to help establish a secure initial configuration and minimal functionality. For static systems, owners and operators can ensure the continued security of their deployed systems by routine evaluation of their systems against the set of controls in the corresponding security profile.

In the event that the systems in question were not originally deployed using a security profile, the system owner will need to perform a mapping of system components against security profile roles as well as a mapping of network architecture against security profile network segments – all as described in Section 3 Aligning Security Recommendations with Intended Design. Provided the system architecture is relatively stable, this mapping exercise is essentially a one-time effort that may be re-used in subsequent evaluations.

5 Conclusion

The advice in the above sections draws on the evolutionary experience of the ASAP-SG team in developing security profiles, starting with the AMI Security Profile ratified by the UCAIug Smart Grid Security Working Group in 2009 and revised in 2010, and culminating most recently with the first public draft of the Security Profile for Wide-Area Monitoring, Protection, and Control (Synchrophasors) in May 2011. While these documents vary in features and attributes, they all are designed to support asset owner efforts to specify, procure, build, and deploy secure systems.

This guidance is provided without the assumption of a particular procurement process or how project responsibilities may be distributed across particular organizational units. A security profile provides guidance that is applicable to the fundamental elements of any smart grid project within that profile's scope and can be used to help create, test, or configure these elements, among other tasks.

Each security profile contains security recommendations that are specific to a particular smart grid application area based on defined functionality, assumptions, and security objectives. Matching the needs of your smart grid project to those documented in one or more security profiles lets you know what is addressed by the profile(s) and what you need to add (or remove) given your specific needs.

Once you have selected the security profile that addresses the smart grid application area of your concern and aligned the security recommendations with the elements of your intended system, the security profile may be used to support a wide variety of activities throughout the project's lifespan, and should provide a substantially traceable and reusable basis for ensuring the long-term security of the system.