Secure Policy-Based Configuration Framework (PBCONF)

Design Document (DRAFT) – Version 1.0

Authors: University of Illinois Urbana-Champaign, EPRI

Innovation for Increasing Cybersecurity for Energy Delivery Systems (I2CEDS) – 2013

DE-OE0000672

June 2014

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THE FOLLOWING ORGANIZATION PREPARED THIS REPORT:

Electric Power Research Institute (EPRI)

Table of Contents

Figures

Tables

Innovation for Increasing Cybersecurity for Energy Delivery Systems (I2CEDS) – 2013

DE-OE0000672

Topic Area

This proposal was accepted for Topic Area 4: Secure Remote Access for the Energy Sector

Summary Information

(1) Project Title:	**Secure Policy-Based Configuration Framework (PBCONF)**
(2) Lead organization submitting proposal	Electric Power Research Institute (EPRI)
(3) Lead organization Category	Industry
(4) Collaborating Organizations	University of Illinois at Urbana-Champaign (U of Ill) Schweitzer Engineering Laboratories (SEL) Ameren
(5) Principal Investigator	Annabelle Lee, EPRI, Senior Technical Executive, alee@epri.com, 202-293-6345
(6) Authorized Representative	David Morrison, EPRI, Senior Contract Manager, dmorriso@epri.com, 865-218-8104
(7) Project Duration in Months	36 months

Project Objectives

PBCONF will be developed as an extensible, policy-based configuration framework to support the secure configuration and remote access of modern and legacy devices from a variety of vendors. The open-source framework will combine a policy engine with a translation engine to address the interoperability challenges of various remote access control methods and provide utilities with a single, organization-wide view of the security configuration for their power delivery devices.

The scope of the project includes the following:

1. The development of an open-source, policy-based configuration framework wherein energy sector devices can be securely configured. The framework will support the management of security related configuration controls (e.g., authentication, authorization, auditing, and access control) and enable secure remote access.
2. The development of a means by which utilities may define a security policy and apply it to heterogeneous devices while providing in-depth information detailing any deviations from that policy.
3. The development of a method for secure remote access to a variety of transmission and distribution substation devices. With the modernization of the electric grid, there is significant new functionality provided within substations. To ensure the effectiveness of the PBCONF, the scope of the initial development effort has been limited and will not include devices such as AMI meters or pole top devices.
4. The development of a common framework that may be used for both legacy and modern equipment.

By building a modular framework, PBCONF will have the necessary flexibility and adaptability for both legacy and new devices. The framework will utilize an ontology that represents the concepts and relationships of the security configuration policy. This is particularly important for the electric sector, with legacy devices that may be 40 years old. The system will leverage distributed architecture concepts to support both centralized and peer-based configuration of the devices to support scalability and resiliency.

The Electric Power Research Institute (EPRI) and the University of Illinois at Urbana-Champaign (U of Ill), with support from Schweitzer Engineering Laboratories (SEL) and Ameren (a utility demonstration partner), will develop an innovative security configuration and remote access system to address the challenges in realizing the high-level vision described above.

Discussion

Incorrect or inconsistent security configuration of the multitude of energy sector devices in the field is a large potential attack vector. By applying uniform security policies across devices in a manner that provides consistency and visibility, this attack vector can be mitigated. Further, both utilities and vendors have indicated the need for security configuration through remote access methods for energy sector devices in a uniform way rather than through isolated applications (stovepipes). Some vendors have standardized their configurations across devices to address this issue. However those solutions are typically only applicable for the respective vendor's devices. A vendor-neutral framework for maintaining security configurations and remote access is needed to further address these problems for the industry.

The Secure Policy-Based Configuration Framework (PBCONF) addresses these needs through its ontology-driven policy, modular architecture, and distributed secure architecture. The PBCONF system can further serve as an audit tool. This allows an organization to maintain a change-managed repository of the remote access methods and security controls implemented on the configured systems. If the remote

access configuration of devices is secured via this mechanism, a utility can also gain efficiency by centrally applying its security policies across all devices or sets of devices in a controlled and verifiable way.

The PBCONF approach provides a model for implementation and deployment that is cost-effective and has the potential to dramatically impact the cyber security of the energy infrastructure. This approach will support not only legacy devices but also future devices that have not come to market The framework will be limited to substation devices, and will not include AMI devices, pole top devices, and related hardware and software. Initial device support is a matter of scope, and there are no technical restrictions on what devices or systems could be supported. The distributed nature of the system provides fault tolerance and increased resiliency and reliability in deploying security configurations and supports secure remote access to the devices. Further, it will support monitoring of the configuration to aid in auditing.

The architecture and tools to be developed will be validated in realistic test environments, demonstrating efficiencies and scalability in secure remote access configuration, auditing, security change management, and support. The technology transfer of results, methodologies, and tools to the utility, industry partners, and research community will follow the framework's initial development.

The following sections describe the approach selected for meeting this critical energy-sector challenge, combining expertise in distributed architectures, automation systems, and cyber security aspects of energy-sector devices. The team members have deep experience, from their respective disciplines, in power and cyber security aspects of grid operations, and a strong track record of research collaboration and technology transfer.

Research Overview

The first phase of the project will include the development of an open-source implementation of PBCONF, a well-specified and open API for modular interfacing with vendor-specific configurations, and a supporting GUI interface. This phase will also include the development of a well-specified and open ontology for describing the security policy and a secure remote access method for brokered maintenance access. The ontology will provide the basis for mapping the deploying organization's security policy to the device-specific configurations. The mapping, verification, and validation of applied, security configurations, security change management and analysis, auditing and alerting, and core functionality will be implemented as part of a reference implementation referred to as a PBCONF node.

The second phase of the work will consist of setting up the demonstration environment and ensuring that the implemented functionality of the framework performs as expected in that environment. The demonstration environment will consist of testbeds at both EPRI and the U of Ill, along with the project's utility partners' location of choice. This phase will also include additional development as necessary and will involve the vendor and utility partners' feedback. Upon completion of the second phase of work, a fully demonstrable architecture and the open-source release of PBCONF will be available for use in corresponding deployment efforts.

Design Statement

All details contained in this document pertain to the design of PBCONF as a system. As a design document, details are subject to change as the project matures and moves into implementation. Any major variations from the design will be noted, with an explanation of why the variance was taken rather than implemented as originally designed. It is anticipated that there will be design deviations throughout the project, as new information and fresh perspectives on the needs of utilities are identified.

Technical Details

As with many open source projects, PBCONF will be leveraging various libraries and other tools throughout the development process. Most of these will be utilized as is and will not be modified. The exception is the data (information) and its supporting structures, which will be created, extended, or modified.

Following are the licenses of various pieces of code that we either anticipate we will be using, or that we are considering for use. This list is not all encompassing at this point in time and it may evolve as the design and implementation is conducted. Also provided is a brief explanation for each of these.

Where necessary, leveraged libraries and existing code modules will be segregated and packaged to limit the impact of their respective licenses on the licensing of PBCONF. This will be accomplished by breaking those components out as standalone applications thereby limiting the areas of code to which the more restrictive licenses apply. An interface and API for the vendor specific translation modules will also be provided to prevent the modules from falling under PBCONFs open-source license. Having the vendor specific modules outside the governance of the open-source license allows the vendors to develop modules that leverage their respective intellectual property (IP) without exposing that IP to the requirements of the open-source license. For example, a vendor may choose to develop a translation module running as a stand-alone application. Such a module will use an externally accessible API for interfacing with the PBCONF node. This module, as a stand-alone application, will not be subject to the licensing applied to PBCONF or any other component of the system.

Development Language and Selected Libraries for Use

- Go: primary development language and runtime executable
  - BSD License
- Git (libgit2/Git2go): golang interface to git-based backend for source control and change management
  - MIT license for git2go
  - GPL v2 with linking exception (libgit2)
- SSH (crypto/ssh extension): golang interface to provide ssh brokered tunnels for remote access
  - BSD License
- Oracle Berkeley DB: backend database for PBCONF configuration and supporting PBCONF metadata
  - Older versions: Sleepycat copyleft
  - Versions >= 12.1.6.0 AGPL v3

Ontology Access and Manipulation

- Redland RDF Suite: ontology interface libraries to read, store, and query ontology
  - LGPL 2.1, GPL 2, or Apache v2
- Gorasqal (go bindings for librasqal – part of Redland): golang bindings for SPARQL and RDQL queries in redland
  - LGPL (although not explicitly stated, inherits from parent)
- Goraptor (Go bindings for libraptor – part of Redland): golang bindings for RDF interfaces in redland
  - LGPL

Front-end Systems and GUI

- Gorilla Web Toolkit (http://www.gorillatoolkit.org/): web framework frontend for golang to simplify web processes
    - New BSD License
- TLS (crypto/tls builtin): golang TLS implementation to provide security layer for web-communications
    - BSD License
- Bootstrap web framework: front end framework to provide base of GUI
    - MIT license
- Backbone js: javascript backend framework to provide structure to web front end
    - MIT license

Information and Data Structures for Modification

- CoEDS (https://github.com/timyardley/CoEDS): cyber security ontology for energy delivery systems
    - Creative Commons 3.0 attribution license
- CPTL (https://github.com/ITI/cptl-power): cyber physical topology language
    - Creative Commons 4.0 for documentation
    - Ontology yet to be released, license unknown at the moment

Target Platform

During development, the target platforms will be a compact form factor machines such as the Intel NUC platform or related derivatives (e.g., Google Chromebox). These machines will provide adequate computation power in a small form factor. If feasible, devices such as a Raspberry PI may also be utilized to aid in prototype creation.

For most field deployments, the target platform should be a substation computer with a rack-mount server being used for the master PBCONF node in the control center. However, a PBCONF node may also operate on a portable computing device, such as a technician's laptop. The project will also verify that there are no inherent issues with deploying on those platforms. During development, measures will be taken to ensure minimal impact to other applications running on a target system. Appropriate protection mechanisms will be evaluated in order to isolate PBCONF node operations (where feasible) from other host platform operations.

PBCONF Architecture

The PBCONF system is composed of several functional components or subsystems that are contained within a PBCONF node. These nodes combine to provide the functionality of the PBCONF system. A PBCONF node consists of a Web Interface and a Service Container. The Service Container is segmented into subcomponents, which include the:

- SSH connection broker,
- HTTPS server hosting Web-based API,
- Policy Engine,
- Change Management Engine, and a
- Translation Engine hosting the device-specific vendor modules.

Each of the components and subcomponents is detailed further in the following sections.

To support resiliency and reliability, PBCONF will implement a peer-based architecture that leverages a master/slave relationship between the nodes. This will provide a mechanism by which the system can operate under islanded conditions or when the circumstances dictate localized control rather than centralized control.

The master PBCONF node may be a stand-alone instance that directly configures end devices through remote access; it may be an instance that directs subordinate instances; or it may do both. The defining characteristic is that it is the root authority for policy in the hierarchy of PBCONF nodes and would likely be installed at the control center.

A master PBCONF node can have any number of subordinate PBCONF nodes; further, subordinate instances may also have subordinates of their own. In such a configuration, a PBCONF node will act as a client application to the upstream node and as a master to directly connected slaves. The downstream slaves will have no awareness of their master's master/slave relationship with any other PBCONF node. To enable localized control, each PBCONF node (slave or master) will have access to all the details necessary to carry out the application of the policy. Any changes to a device's configuration will be optionally sent upstream to a master node. The master node (top of the tree) will have no parent, thus stopping the propagation. This will also include any conflict management that needs to be handled upstream. The relationship between the master node, slave nodes, and end devices is shown in Figure 1.

Any PBCONF node may be configured to propagate or not propagate a device's configuration upstream. This results in three operating modes.

1. The first (and default) is that every node in the hierarchy will send configuration changes to the next directly connected upstream node. In this mode, every PBCONF node along the path from the device to the master will store a copy of the configuration.

2. The second operating mode is enabled when all of the PBCONF nodes that are directly connected to devices are configured to not propagate device configuration. In this mode, only the PBCONF node that is nearest to a device in the hierarchy will store that device's configuration.

3. The final operating mode is enabled when one or more intermediate PBCONF nodes (PBCONF nodes that are only connected to other PBCONF nodes and are not a master) are configured to not propagate device configurations. In this mode, a device's configuration will propagate up the hierarchy until it reaches a non-propagating node. The configuration will be stored in all PBCONF nodes along the path from the directly connected node to the non-propagating node

Figure 1 shows what an example deployment of PBCONF may look like in the current scoping. This is intended to be illustrative, but not definitive as PBCONF is flexible enough to be deployed in a variety of architectures.

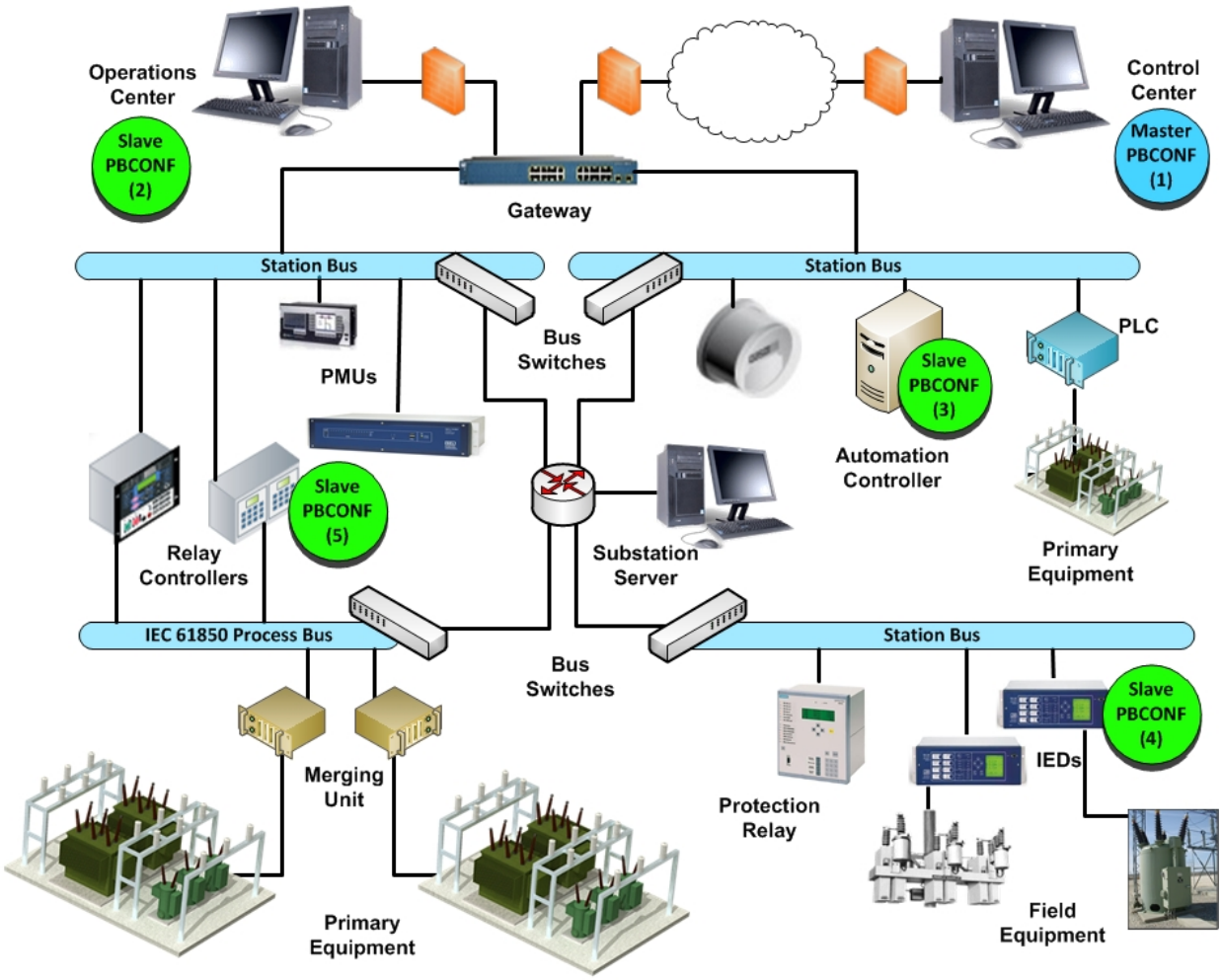


Figure 1: PBCONF Illustrative Example

Architecture Conditions

The architecture of a PBCONF system will be a tree-like hierarchy. At the top of the hierarchy will be the master node. This master node will be able to direct and control the nodes immediately below it in the tree. To ensure that security configuration information is directed along the correct branch of the tree, each PBCONF node will have knowledge of the topology that is below it. However, a higher level node will not communicate directly with any node except those that are directly above or below it in the tree.

This architecture requires communications to be chained. For example, if the Master node (Figure 2) is to send an updated policy to Device 4, the command will be sent to PBCONF Slave 2. Slave 2 will then send the command to PBCONF Slave 4, which will then send the command to Device E4. Likewise, if a field technician makes a security configuration change to Device 4, this change will propagate up the hierarchy (assuming the default operating mode) to the Master Node, where it will be checked for policy compliance. In this manner, the top of the hierarchy is authoritative for the policy, and the node nearest a device is authoritative for the device configuration.

When new devices are added to the hierarchy (a PBCONF node is configured to access a new device), the security configuration existing on the device will be extracted. A notification will be directed to the PBCONF node up in the hierarchy, along with the device's security configuration. This process will continue until the notification and security configuration reach the master node. The master node will

validate the security configuration against the policy, and generate alerts. This ensures that every PBCONF node that contains the new device in its locus of control is notified of the new device, and stores the devices security configuration. In contrast, each PBCONF node may be configured to not store the complete device configurations.

When new PBCONF nodes are added to the hierarchy, the new node will send a notification to its direct upstream parent, indicating that the new node is online and operating, and request the current policy. This notification and request will travel up the hierarchy until it reaches the master. The master will send the current policy down the hierarchy until it reaches the new node. Note: the request may be an indication of the version of the policy that the requesting node currently has. The upstream node may choose to indicate the version the requestor has is up-to-date instead of sending a full policy.

Each PBCONF node will utilize a heartbeat communication to indicate its status, including policy revision. When a heartbeat is received from a slave node, the upstream node will indicate if the policy is up-to-date. The upstream node will store the time (a time reference, not necessarily a time stamp) of the heartbeat. The slave will request an updated policy if the current policy is out-of-date. If a configurable amount of time passes without communication from a slave node, an upstream node (master or slave) will assume the slave is down, and generate an alarm. The hierarchy will begin to operate in a mode where the highest slave in each hierarchy begins to act as a master for that hierarchy. In this mode, propagation of device security configuration will be unaffected with the exception that propagation cannot happen beyond the “acting” master for the hierarchy. The “acting” master will initiate the heartbeat until the acting master node is reconnected to the upstream hierarch. Once the connection issue is resolved, device security configurations will be sent upstream, where policy conflicts are resolved, and the updated policy is propagated down.

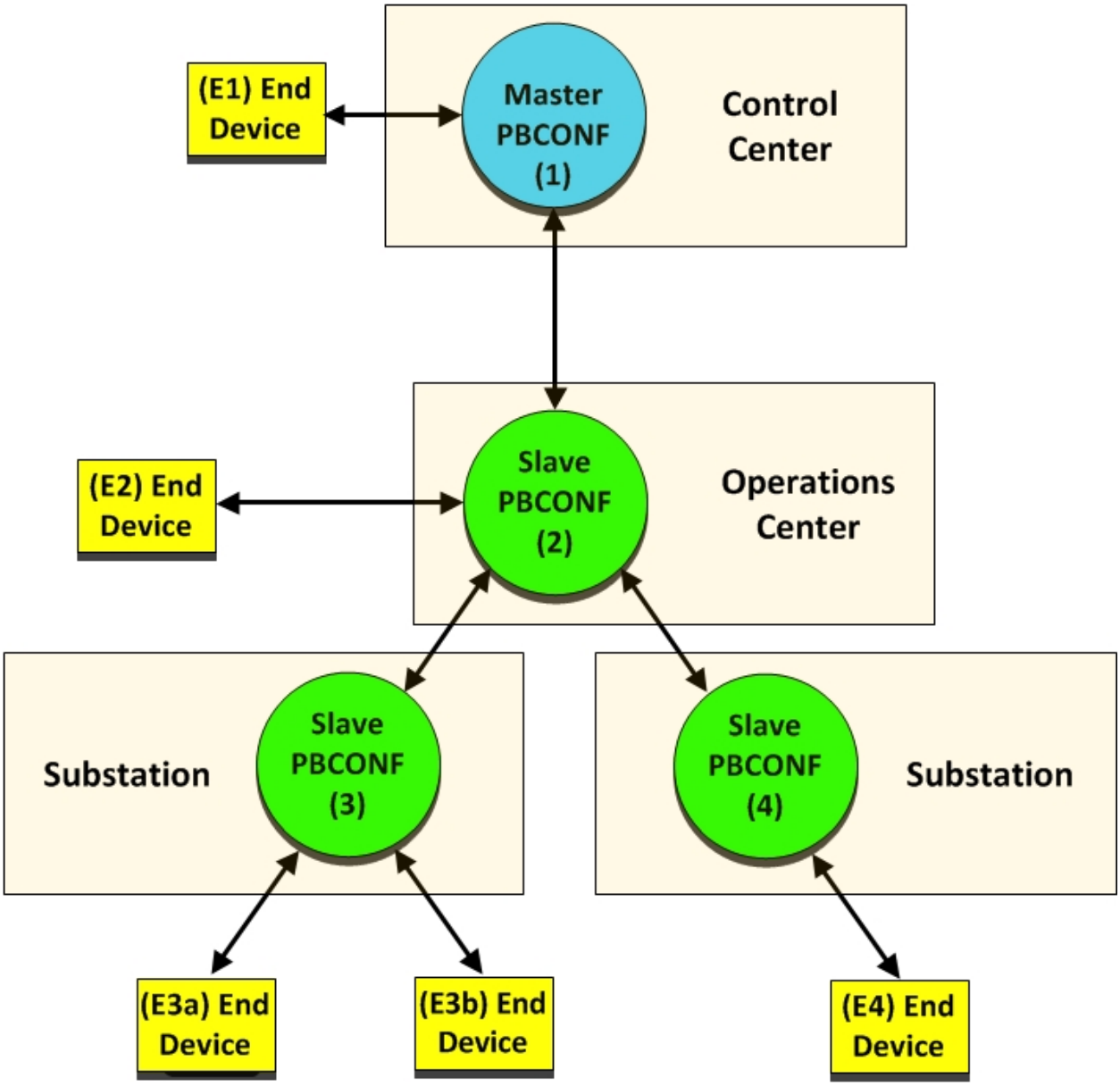


Figure 2: PBCONF Node Relationships

Ontology

While the terms taxonomy and ontology are sometimes used interchangeably, they differ significantly in meaning. Taxonomies are generally limited to describing and classifying relationships based on a subclass hierarchy. However, ontologies, provide a formal representation of the full domain of knowledge that extends beyond the subclass hierarchy to include properties that further define relationships, restrictions, and interdependencies between the expressed concepts. This formal expression and ability to fully represent the concepts in a semantic model are needed to provide policy matching and analysis associated with the expressed policies and device capabilities.

One example of how an ontology is necessary in a security definition domain is associated with certificates. Using a taxonomy definition, a certificate would simply be a type of credential. However,

using an ontology definition, a certificate would be a type of credential that has properties, such as issued timestamp and expiration date that make it possible to provide further information on whether that certificate is an acceptable match.

Security policy definition and application present a difficult challenge. In PBCONF, the ontology definition will be used to capture the definition of the remote access security policy and act as a form of knowledge representation surrounding the policy needs of the energy sector. The scope of the ontology definition will be limited to the security related configuration controls of the heterogeneous devices that allow it to address the necessary attributes for security configuration. PBCONF will not define policy beyond the scope of that configuration, except where necessary to adequately address security needs.

PBCONF will leverage and extend prior work [CPTL, COEDS, NRL2005, HL7SEC] that has built ontologies for aspects of security properties and threat modeling. CPTL focuses on device topology connections, COEDS focuses on actors and assets, NRL2005 focuses on annotation of security capabilities for auto-discovery, and HL7SEC focuses on fundamental security primitives as they map to requirements in the health sector. Leveraging this work will allow PBCONF to build an ontology that is extensible, maintainable, and specific to the needs of the electric sector. In doing so, two definitions will be created:

1) The device capability description associated with the security related features that a device supports (capabilities), and

2) The security policy description that details the actual policy that is to be applied (requirements).

The combination of capabilities and requirements will determine the level of matching available for applying a policy to a device or set of devices. For instance, if the policy requires username and password for access to a remotely connected interface (requirement), and a device has the capability to apply username and password for remote access (capability), then there exists an exact match between the requirement and the capability. If, however, the device only has the option to use digital certificate credentials on remote access interfaces (capability), then there is no match, and operator intervention will be required. Alternatively, if the device does not have any option to apply usernames/passwords to interfaces (capability), then there is also no match, and the policy as stated cannot be applied to that device. In either case when there is no match, the specified policy cannot be applied and the PBCONF system will leverage logging and alerting to notify the operator of the resulting deviations or inability to apply the policy.

Ontologies can be expressed in many ways and there have been several standards formed for the expression of these ontologies. The most appropriate standard to use will be determined based on the underlying implementation technology. The Web Ontology Language (OWL) [OWL2004] is the implementation of choice and will be versioned to help ensure continuity moving forward. Tools such as protégé [PROTÉGÉ] will be leveraged as needed for use in building and assessing the base ontologies. Ontologies may be expressed using formalisms such as the Semantic Application Design Language [SADL] to describe the ontology intent and have it derive the corresponding representation. The implementation for parsing and interacting with the ontology is also important, so openly available libraries will be leveraged such as the Redland RDF suite [REDLAND].

The semantic model approach will also allow for comparison of policies. The query language SPARQL [SPARQL] will provide a mechanism to support a multitude of analysis techniques above and beyond available reports. Advanced analysis techniques will take the form of directed queries initially, but the modular architecture will support the addition of more directed capabilities as desired. If possible, a secure interface will be provided to allow direct SPARQL expression.

The policy representation will be a stored representation of the reasoning around the defined ontology. Mapping the ontologies to their corresponding device commands is addressed in more detail in the policy

engine section of this document. A query builder will be explored as a method to easily describe policies that can then be stored and enforced by the system. The ontology will not be extensible by modules at this time, although that functionality may be supported in the future.

PBCONF Service Container

The core of the PBCONF node is the service container shown in Figure 3. The service container provides a framework on top of which the remaining components of the PBCONF node are built. The service container will provide the underlying internal communication framework for both node-to-node communications and interface-to-engine communications. The service container will host a policy engine for operations surrounding the defined policies and a change management engine for tracking security configuration changes on the end devices. The service container will also host a translation engine that will, with the help of device-specific translation modules, translate a provided ontological configuration into device-specific configuration commands or into the device-specific configuration API. For some vendors, standardized configuration methods may allow a single device translation module to handle a variety of different devices.

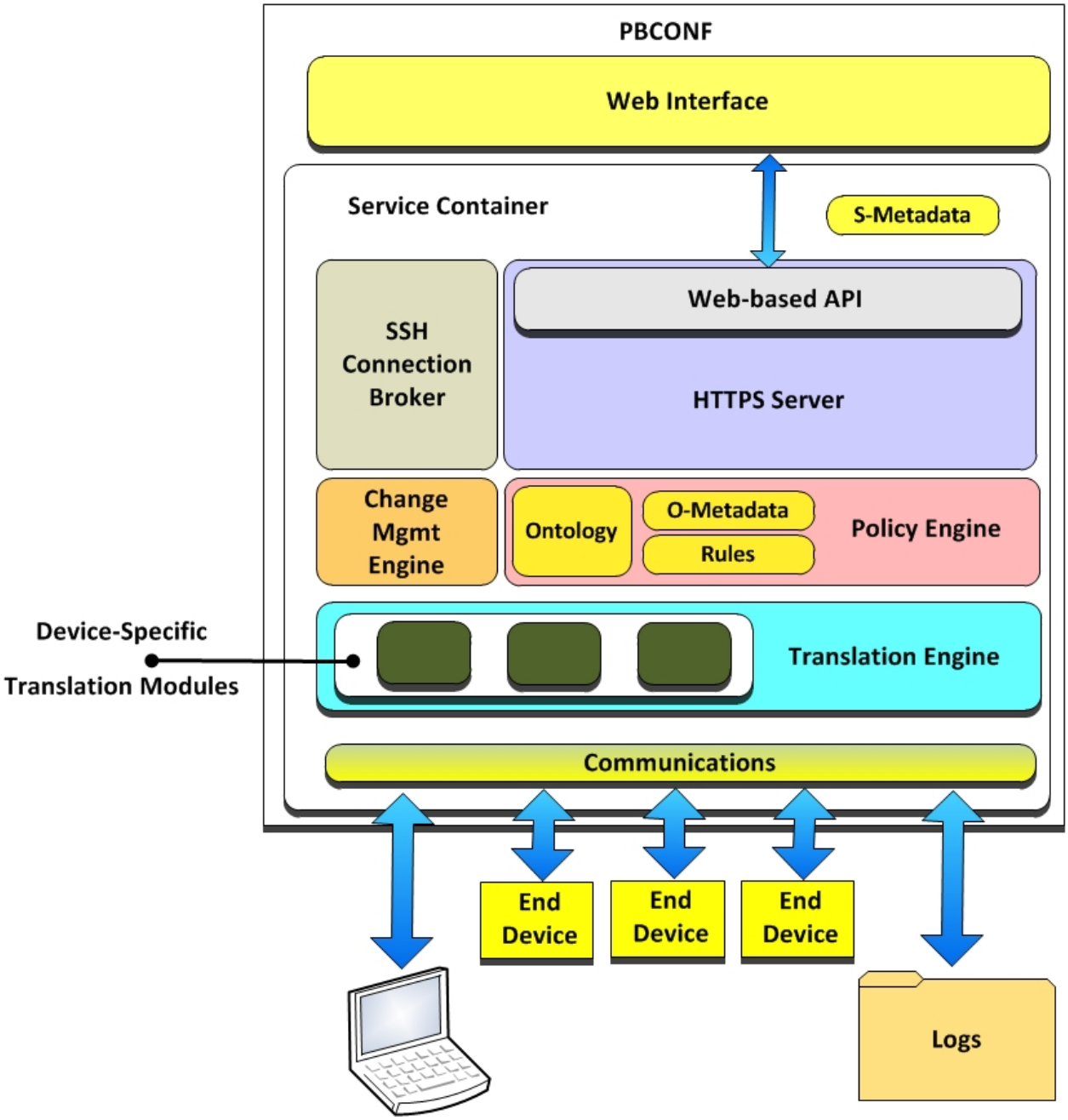


Figure 3: PBCONF Component Diagram

In addition to hosting the communication framework and translation engine, the service container will provide an interface for the policy engine. Upon policy verification via ontological rules and reasoning, the policy engine will submit the requested policy to the service container for mapping to the desired devices via downstream PBCONF nodes. The service container will use a secure communication mechanism to submit the security configuration to all appropriate subordinate PBCONF nodes as well as communicate, via the communication framework, with any directly connected end devices to apply the policy. The applied policy will take the form of a device specific configuration as generated by the device specific translation module.

The service container will also host a secure, interactive communication channel allowing remote access to support maintenance or configuration access. This secure communication channel can be used by operators to establish a secure, encrypted, interactive session from their point of origin to the PBCONF node that is most directly connected to the end devices that do not themselves implement secure interactive communication. Where an end device does implement secure communication, the service container will act as a broker, passing the original, secure, communication to the end device. However, when an end device does not implement secure communication, the service container can accept incoming secure connections and leave insecure connections within a reduced "local" footprint bounded by the last hop to the end device.

While Linux will be targeted as the initial reference platform, the service container will be developed as a platform agnostic system. Windows support is expected to be straightforward and will also be provided, in the absence of any unanticipated technical barriers.

Modular Design

The PBCONF system will be designed using a modular architecture. In particular, the service container will be implemented using a modular design approach to support both flexibility and enhanced capabilities. Modularity will allow commercial implementers to replace or supplement many of the subcomponents of the service container while continuing to use the reference implementation of other components and the service container itself.

Modularity will enable vendors to develop device-specific modules that translate the provided ontological basis (pre-parsing of the ontologically defined policy) into device-specific commands while still protecting their intellectual property. This is an important feature due to the open nature of the framework; it will be discussed in more detail below in the section on device-specific translation modules. The modular design will also support extensibility through the addition of new modules, allowing PBCONF nodes to support currently deployed devices as well as future protocols, standards, or devices.

Each submodule will be responsible for implementing an isolated portion of the PBCONF node in such a way as to "plug into" the service container. The service container will likely use a coroutine-based design to manage the submodules and direct subtasks. Coroutines would allow the service container to operate all submodules concurrently, providing further scalability and efficiency.

Secure Communication

The service container will implement two default forms of secure communication: Secure Hypertext Transfer Protocol (HTTPS) and Secure Shell (SSH). While these two communication transport mechanisms will be implemented by the reference implementation of the PBCONF node, the implementation will be modular such that PBCONF is not directly dependent on them; therefore, commercial implementers or end users of the PBCONF node can replace these transport protocols if required. Figure 4 illustrates the communication channels for the components of PBCONF.

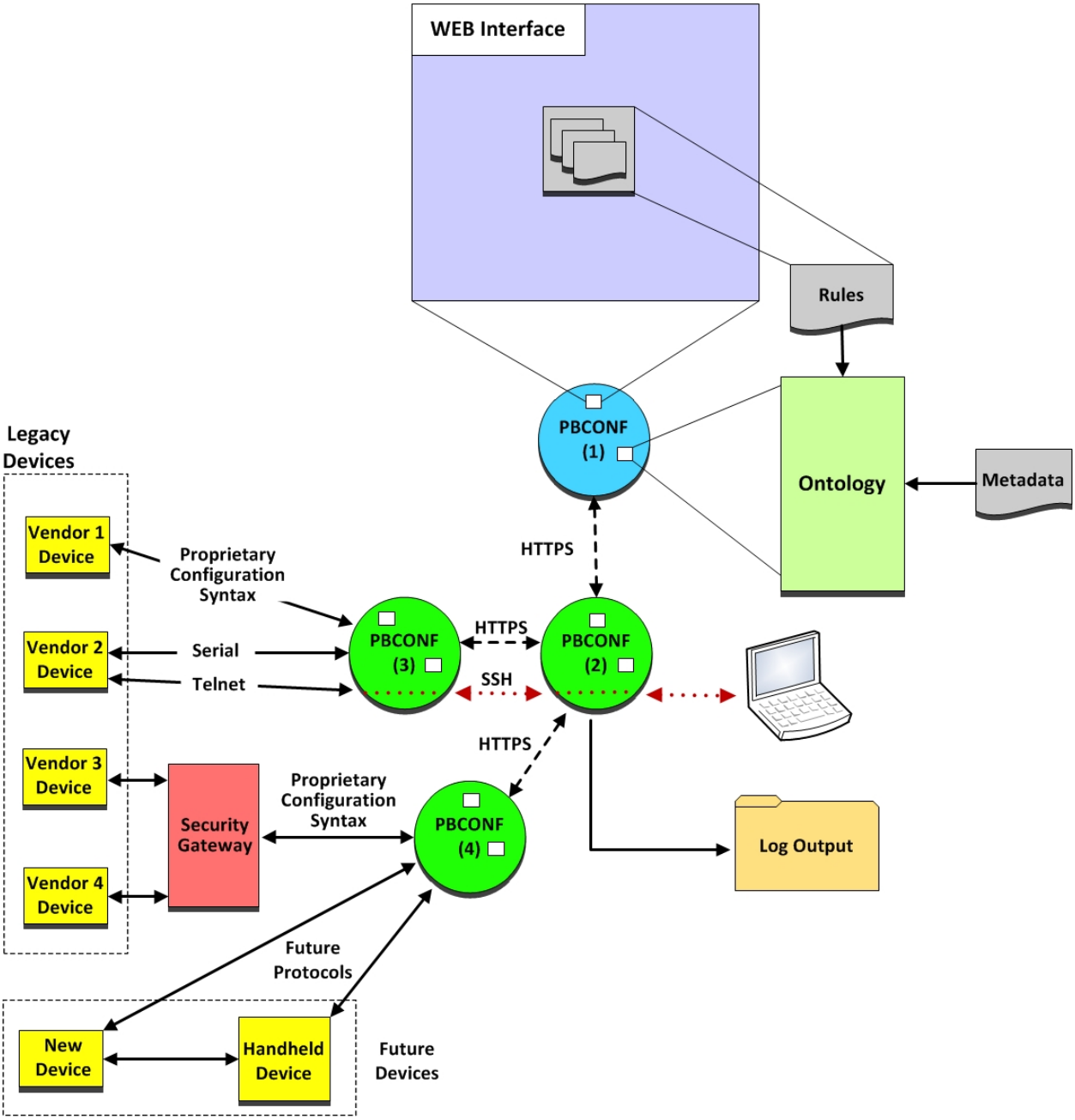


Figure 4: The Composed PBCONF System Overview

Secure Hypertext Transfer Protocol (HTTPS)

Since PBCONF will be communicating critical access credentials, secure communication is mandatory. HTTPS is intended to be an easily portable and broadly flexible transport mechanism that provides both security and flexibility in a well-defined standard. It will lower the barrier to entry for integration while allowing associations of strong security properties with communications. Since HTTPS leverages the SSL/TLS suite, this approach will provide an adaptable framework moving forward. The project will leverage identity verification for mutual authentication of PBCONF nodes by leveraging X.509 identity certificates to validate the communications between PBCONF nodes. X.509 identity certificates are a standardized representation of identities leveraging public key certificates. The use of X.509 will be

modular and could be enabled or disabled. However, the recommended deployment will be having it enabled. A basic access control model with credential store will also be provided as a means to interface with authenticated users (rather than PBCONF nodes mutually authenticating), not mandating that all user entities leverage identity certificates.

Due to known vulnerabilities, such as the Browser Exploit Against SSL/TLS [BEAST], and the Heartbleed vulnerability [HEARTBLEED], only the most recent TLS protocol versions (TLS 1.1 and 1.2) will be utilized. In addition, PBCONF nodes will only allow NIST-approved cryptographic algorithms, modes, and key sizes, to ensure compatibility and secure communication between nodes. The allowed protocols, cipher suites, and other parameters will be documented and specified to allow for easy modification and interfacing with the system. Note, that the system will place a preference on utilizing high security communications mechanisms by leveraging Perfect Forward Secrecy and HTTP Strict Transport Security (HSTS) [HSTS] as applicable for PBCONF communications. HSTS will likely be configured as *Strict-Transport-Security "max-age=31536000; includeSubDomains"*.

SAML and OATH may be explored as potential integration points with external systems, but will likely not be integrated in the scoping of the current project. The authentication systems will be architected to provide the ability to extend in this direction in the future.

Secure Shell (SSH)

SSH will be provided as a means for interactive communication with the end devices. For legacy end devices that do not support SSH, the framework will leverage the network of PBCONF nodes to establish the SSH connection as near to the end device as possible. PBCONF will then locally bridge that connection to an insecure channel (e.g., via telnet or serial) to access the end device. Based on the recommended implementation architecture, this will provide a high level of security on externally visible links and rely on the less secure communications only for the last hop, which is likely to be internal to a substation on a local area network. If end devices support a secure open communication method, that method will be utilized for the last hop. Using this method will create a seamless end-to-end secured communication channel.

Restricted Command Shell

A menu driven command shell will be developed to support interactive use and automated device interaction. The command shell will present the user with a list of options encapsulating common device operations. These operations will enable a user to interactively engage with the devices for operations such as logging in by selecting a single menu option.

Synchronization

PBCONF nodes will synchronize on an as needed basis with a preference placed on data security (need to know) rather than a focus on full systematic replication. For example, when the policy is modified at a master node, those policy changes will be transferred to applicable slave nodes.

Periodically, master nodes will contact slave nodes with a “heartbeat” command. This is to ensure that slaves are active and operating properly. Failure to reply to a heartbeat will result in an alarm being generated.

Specific data to be synchronized between PBCONF nodes will be determined during development.

Database

Each PBCONF node will implement a security configuration database. The database will store local (to the node) configuration and state information. This information is limited to PBCONF configuration and

information related to connecting to the corresponding devices. For instance, the configuration database will store file paths along with parent and child node connection information. In addition, the database may store access control lists and other device specific system metadata (e.g., IP address, locations), required to access a given device such as local usernames with passwords and connection information for remote user/password stores.

Finally, the database will store the policy definition for the directly connected devices that are managed by that PBCONF node and any child nodes. A PBCONF node will not store the policy definition for peer nodes.

Logging

PBCONF will initially support operational logging via Syslog. Each BPCONF node will report logging information with adjustable (via configuration) levels. The specifics of what information can be logged, and what logging level may be applied to that information will be determined during the development process.

The log level applied to any given message will follow standard Syslog level definitions. This is an eight level scale of increasing intensity. If, for example, a PBCONF node were to be configured to only log level 0 (Emergency) messages, then only messages related to imminent failure of the PBCONF node will be logged. On the opposite end of the scale, if the PBCONF node were to be configured to log at level 7 (Debug), then all possible messages will be logged. The log levels for Syslog are:

- Level 0 – Emergency; System is unstable; Node failure imminent.
- Level 1 – Alert; Immediate action required; Node failure likely.
- Level 2 – Critical; An unrecoverable failure condition has occurred; Node will shut down.
- Level 3 – Error; A recoverable failure condition has occurred. Node will continue to operate, however functionality may be limited.
- Level 4 – Warning; An operationally significant, unexpected event has occurred. Node will continue to operate, however functionality may be limited.
- Level 5 – Notice; An operationally significant, but expected or normal, event has occurred. Node will continue to operate normally.
- Level 6 – Informational; Non-critical informational messages.
- Level 7 – Debug; Information useful to developers and of little value to operators.

Note, the logging system will report messages for all levels below and including the requested level. For example, if an operator sets the log level to 5, then levels 0, 1, 2, 3, 4, and 5 messages will be logged.

Alarms and Notifications

PBCONF will implement an alarming and notification system as part of the service container. This system will be responsible for generating and delivering system critical alarms and notifications to system administrators and operators. PBCONF will initially support two mechanisms for delivering alarms and notifications.

The first delivery method will be via the logging mechanism. All system notifications, such as report completion, will be delivered to the logging system with log level 5 (notice) by default. The system operator may configure the log level used in a production environment. Alarms, which represent an

unexpected operational condition, will be delivered to the logging system with log level 4 (warning). Note, system alarms such as this should not be confused with log level 1 (Alert).

The second delivery method will allow an operator to configure an email address and SMTP server (to be used for delivering the log via email) that PBCONF will use to deliver alarms and notifications. When email notifications are enabled, the notification or alarm will be sent via email in addition to the logging system.

Integration

Each PBCONF node will be able to operate autonomously. In a single node configuration, no other resources, such as user and password information, will be needed for PBCONF to operate. To support future expansion and integration with other enterprise systems, PBCONF will implement hooks to allow other systems to augment PBCONF operations.

Web API

The interactions between service containers will be by way of a web-based API to allow for ease of integration and automation with other systems. Identity verification will be required to access the API, and the API will be implemented to provide the functionality service containers need to intercommunicate, passing well-defined configuration syntax to subordinate service containers. In addition, the web-based API will provide the interface needed by the service container to communicate with other PBCONF nodes.

The service container will implement a built-in HTTPS server to provide access to the underlying functionality and will support a REST-like API utilizing standard operations via that server. Data passed between service containers as well as data passed between the policy engine and master service container will be encoded in a portable format, such as JavaScript Object Notation (JSON). JSON is a lightweight data serialization format that is commonly used for data transfer over HTTP and HTTPS.

The REST-like API will be implemented as a series of HTTP endpoints. An *endpoint* is similar to a function call in a traditional application. An API endpoint is denoted by the URL of that endpoint. For instance, /device/1/config is an endpoint that will return the configuration for the device with ID 1. The returned data is known as an entity. An *entity* is the encoded representation of the data that is returned by an endpoint using a GET method or sent to an endpoint using a PUT method.

The web-based API will implement communications via standard HTTP request methods, as follows.

- **GET**

  Used by subordinate service containers to request updated security configuration data from an upstream master. Get will also be used by the master PBCONF node to request updated security configuration data from the policy engine.

- **POST/PUT**

  Used by upstream masters to “push” new security configuration data to subordinate service containers. Post/put will also be used by the policy engine to inform the master of updated or new security configuration data. Note: PUT requires a complete representation of the receiving entity, and can be used for create operations. POST is for partial resource updates.

- **HEAD**

  Head is used prior to GET operations to determine if any updates are currently available. By utilizing the HEAD method prior to GET, subordinate service containers can avoid requesting

data when currently known data is unchanged. In all instances, HEAD will return only the HTTP headers that would have been sent in response to a GET call [RFC2616]. The HTTP headers return header information that will allow the requester to determine if a GET operation is required to update locally stored state information. While not listed in the tables below, all endpoints that support the GET method will also support the HEAD method.

- **DELETE**

  Delete is used to remove obsolete resources (such as old reports).

Additional HTTP methods may be supported by the underlying HTTPS implementation to comply with HTTP/HTTPS standards and recommendations. The focus will be on providing a robust framework that easily integrates with other systems as desired.

In addition to performing the standard interactions and controls mentioned above, the API will communicate a representation of the defined policy, supporting data for that policy, and any ancillary data (such as data related to auditing, logging, and verification) that needs to be communicated between PBCONF nodes.

As required by the HTTP specification [RFC2616], each HTTP method will return an appropriate HTTP status code with each call. The return code will follow standard REST practices [RESTCODES].

HTTP Status codes are broken down into five categories. Status codes in the range 100-199 represent an informational message from a HTTP server to the client. This range of codes will not be used by PBCONF as they are not fully supported in HTTP/1.0. The 200-299 range of codes indicates that the request completed successfully. The 300-399 range of codes indicates that further action is required by the requestor. The 400-499 range of codes indicated that there was a problem with the request. The 500-599 range of codes indicates that there was an error on the server.

While not a comprehensive list, the following codes (and definitions) will be the most commonly used in PBCONF

- 200 – OK
  Returned by the GET method. Code 200 is a general success code; if no other success code applies, 200 will be returned.

- 201 – Created
  Returned by the PUT method. Code 201 indicates that a new entity (report, device, etc.) was created as a result of the request.

- 202 – Accepted
  Used by the report engine to indicate that a report is still in the process of generating data.

- 400 – Bad Request
  Returned by the PUT method to indicate that the request was incorrectly formed. Specifically, the PUT method requires that a full representation of the entity to be operated on is included in the request body. If the representation is missing or incomplete (POST allows partial representations), then a status code of 400 will be returned.

- 401 – Unauthorized
  Can be returned by all methods if authentication fails.

- 403 – Forbidden
  Can be return by all methods when authorization fails. This will be returned when a node or user attempts to call a method on an endpoint for which they are not authorized.

- 404 – Not Found
  Returned by all methods if a request is made for an entity or endpoint that does not exist.

Versioning

The API will be versioned. That is, every endpoint (except the version endpoint) will be able to utilize an API version number. This feature will enable reliable communication between different versions of PBCONF. For instance, the original PBCONF will support version 1.0 of the API. A newer application may support version 2.0. By versioning the API, the two devices can be assured that a compatible API is present.

The versioning will take two forms. In the URL, you will be able to specify a version number at the end of the URL. Versioning will also be supported via the Accept Header, which makes the URL request transparent across versions.

Namespaces

Each operation area of the PBCONF API will use namespaces to provide separation of responsibility, and to ensure that unique identifiers are tied to the type being referenced. For example, ID can reference most entities. The use of namespaces means that IDs only need to be unique within a namespace, and not globally unique. Use of namespaces will allow non-core features and plugins to extend the API.

PBCONF will initially support the following top-level namespaces

- root(/)
  The root namespace is the top level namespace in the API. The root namespace will expose API endpoints for determining information about the PBCONF node, such as version information, supported sub-namespaces, and sub-namespace version information.

- device (/device)
  The device namespace exposes API endpoints for obtaining information about devices and device configurations.

- namespace (/namespace)
  The “namespace” namespace exposes API endpoints for obtaining information about all of the supported namespaces implemented on the PBCONF node. This namespace is used, primarily, to enable client applications and software to auto-discover node capabilities and to support variations in capabilities between PBCONF nodes.

- node (/node)
  The node namespace exposes API endpoints for adding and removing master and slave PBCONF nodes. In addition, endpoints will be implemented to allow for the configuration of connection properties for master and slave nodes.

- policy (/policy)
  The policy namespace implements API endpoints for working with policy definitions. This includes updating, removing, and adding new policies, as well as initiating validation operations

on a policy definition.

- reports (/reports)
  The reports namespace implements API endpoints for creating, removing, modifying, and running reports.

- ui (/ui)
  The ui endpoint doe not implement any API endpoints. The ui namespace contains the built in web based user interface for the PBCONF node.

Authorization

PBCONF will support a basic authorization framework. Initially, two modes will be defined, a read-only mode and a full access mode. In read-only mode, any endpoint calls that invoke a change will return a 403 code: forbidden response. The full access mode will allow all operations to be performed.

Authentication

Any device or system communicating with a service container is a client of that service container, and will only communicate with the service container if the client already possesses a valid certificate (or certificate chain) for the service container. This provides authentication of the service container. This mechanism ensures that each session is unique and provides authenticity of the requested command. In addition, it allows for future external authentication systems, such as SAML and OAUTH.

- ALL HTTP request method operations should return 401 if the Authorization header is missing or authentication fails.
- ALL HTTP request method operations should return 403 if the Authorization header is included, the authentication is successful, but the authorization fails.
- Issuance of ANY HTTP request methods not defined will return a 405 error.

In addition to the endpoints identified below, additional endpoints may be identified during development and testing. As such, the following lists should not be considered final.

Global Endpoints (/)

Global endpoints are API endpoints that are implemented in the root namespace. These API endpoints provide versioning information about the PBCONF node.

Endpoint	Method	HTTP Status Code	Return	Comment
/version	GET	200	List of namespaces and API versions	Returns a list of the implemented namespaces and the API version associated with each
/version/<namespace>	GET	200 404	API version for the named <namespace>	404 status will be returned if <namespace> does not exist

User Interface Endpoint (/ui)

The ui namespace does not define any additional endpoints. A request to the ui endpoint should return the built in json/html web interface. The user interface will utilize the same REST APIs as any other application that would interface with the system.

Other Endpoints (non-global)

Endpoint	Method	HTTP Status Code	Return	Comments
/device	GET	200	List of devices	
/device/<id>	GET	200 404	Device specific information for device <id>	404 status will be returned if <id> does not exist. This may include information such as the device name, IP address, etc.
/device/<id>/config	GET	200 404	Configuration information for the device indicated by <id>	404 status will be returned if device <id> does not exist
/namespace	GET	200	List of namespaces	
/node	GET	200	List of known subnodes, and current state of each subnode	
	POST	200 201	The updated or created entity	A call to POST must contain a complete representation of the entity to be updated or created. REST semantics dictate that the updated/created version of the entity be returned. The 201 status will be returned if a new entity was created; a 200 status will be returned if an existing entity was updated
/node/<nodeid>	GET	200 404	The state of <nodeid>	The 404 status will be returned if node <nodeid> does not exist
/node/<nodeid>	PUT/POST	200 400 404	The updated version of <nodeid>	Equivalent to POST/node/, except that the entity to be updated is specified in the request URI instead of the request body, and PUT does not support entity creation. Note: The PUT method requires a

Endpoint	Method	HTTP Status Code	Return	Comments
				full representation of the entity to be created. The 200 status will be returned if an existing entity is updated; the 400 status will be returned if the request body does not contain a full representation of the entity to be updated and PUT was used; the 404 status will be returned if node <nodeid> does not exist.
/node/<nodeid>/config	GET	200 404	Configuration of a specific PBCONF node	The 404 status will be returned if node <nodeid> does not exist.
/node/<nodeid>/config	PUT	200 400 404	The updated security configuration	The 400 status will be returned if the request body does not contain a full representation of the security configuration; the 404 status will be returned if <nodeid> does not exist
/node/<nodeid>/config	POST	200 201 404	The updated or created configuration element	Used to create new configuration elements. The 200 status will be returned if an update is successful; the 201 status will be returned if a new element is created; the 404 will be returned if node <nodeid> does not exist
/node/<nodeid>/config /<config element>	GET	200 404	Specific element of a specific PBCONF node	The 404 status will be returned if either node <nodeid> or <config element> does not exist.
/node/<nodeid>/config /<config element>	PUT/POST	200 400 404	The updated configuration element	The 400 status will be returned if a complete representation of <config element> is not included in the request body and PUT was used; the 404 status will be returned if node <nodeid> does not exist
/reports	GET	200	List of available reports	This will probably include the id, name, and a description for each report
/reports	POST	200 201	The update or created report	Update or create a new report. The 200 status will be returned if the report is successfully updated;

Endpoint	Method	HTTP Status Code	Return	Comments
				the 201 status will be returned if a new report is created
/reports/<report id>	GET	200 404	The report identified by <report id>	Retrieve a specific report definition. The 404 status will be returned if report <report id> does not exist.
/reports/<report id>	PUT/POST	200 400 404	The updated report	Update report <report id> The 200 status will be returned if the report is successfully updated; the 400 status will be returned if the request body does not contain a full representation of the report and PUT was used; the 404 status will be returned if report <report id> does not exist.
/reports/run	GET	200	List of existing executed or executing reports	
/reports/run/<report id>	POST	201	The report being run	Run a report
/reports/report/<report id>	GET	200 202 404	Report data	The 200 status will be returned if the report is complete; the 202 status will be returned if the report has not yet completed; the 404 status will be returned if <report id> does not exist

Policy Engine

The policy engine will accept a set of policy rules and supporting data that are defined by the ontology and apply them to a selected device or set of devices via the device-specific translation modules. The policy rules will define constraints that a security configuration must meet.

The supporting data can come in several forms and are documented in the Ontology. The data is expected to contain items such as user credentials, identity certificates, and access control information. The supporting data may be provided as part of the policy, a local secure data store, or referred to by the policy and sourced from another location via available APIs.

The policy engine will implement an HTTPS server for secure communication between client applications and the policy engine. The internal HTTPS server will also be used to enable the master PBCONF node to request updated security configurations. In addition, the policy engine will implement an HTTPS client to enable the master PBCONF node to provide notification of new or updated security configurations.

Policy Definition

As mentioned earlier, the policy representation will be a stored representation of the reasoning around the defined ontology. A query builder will be explored as a method to easily describe intended policies that can then be stored and enforced by the system. The ontologies will not be extensible by modules at this point in time, although that functionality may be supported in future releases.

SADL may allow for some additional flexibility associated with policy definition. The intent behind leveraging this would be to explore the "human readable" SADL query language and rule definition as a mechanism by which policies could be defined. For those that are versed in ontological queries, use of SADL may not be necessary. However, there are a limited number of individuals that have this expertise, therefore, so simplification of queries is being explored. SADL also supports test suits, which can be thought of as unit tests for a created ontology definition. This allows verification that any modifications to the ontology still adhere to the constraints intended. For example, if the definition of a device is changed in the ontology, a previous instance of that device should always be classified as that device in the new ontology definition, regardless of the changes to the device definition (i.e., once a device, always a device). By leveraging SADL, test cases can be provided that allow for the validation that those properties hold after updates are made to the ontology definition. For example, a password should continue to be classified as a password even after changes are made to the definition of a password (e.g., such as adding a character set).

At this time, there is no intent to create automated policy definitions. Such a capability would allow policy to be driven by connectivity, capabilities, and device functions. For example, a CIM model could be utilized as a definition of some aspects of policy. Further, a machine based definition of CIP policy could be created such that a mapping of CIP compliance constraints can be expressed in relation to the ontological policy and would allow for automated compliance checks. No direct automated interface with CIM/CIP or any other systems will be created at this time, and instead human interfacing and reasoning will be leveraged to build the policies.

/policy (External API)

Endpoint	Method	HTTP Status Code	Return	Comment
/policy	GET	200	List of policies	
/policy	POST	200 201	The updated or created policy	The 200 status will be returned if the policy is successfully updated; the 201 status will be returned if a new policy is created
/policy/<policy id>	GET	200 404	The policy identified by<policy id>	The 404 status will be returned if policy <policy id> does not exist
/policy/<policy id>	PUT/POST	200 400 404	The updated policy	The 200 status will be returned if the report is successfully updated; the 400 status will be returned if a full representation of the policy is not included in

Endpoint	Method	HTTP Status Code	Return	Comment
				the request body and PUT was used; the 404 status will be returned if policy <policy id> does not exist
/policy/<policy id>/validate	POST	201 404	The validation record	Initiate validation of <policy id> The 201 status will be returned if the validation has been successfully started; the 404 status will be returned if <policy id> does not exist
/policy/<policy id>/validate/<validation id>	GET	200 404	The validation record identified by <validation id>	The 404 status will be returned if policy <policy id> or if <validation id> does not exist
/policy/default	GET	200	The default policy definition	
/policy/default	PUT/POST	200 400	The default policy	The 200 status will be returned if the new default is successfully set; the 400 status will be returned if the full representation of the new default policy is not included in the request body and PUT was used

Device-Specific Translation Modules

The service container will provide an API that vendors will use to implement device-specific translation modules. These modules will translate the ontological configuration into device-specific configuration commands and apply the configuration parameters by interfacing with end devices directly, using the devices' native communications or configuration APIs, or via a security gateway configured to act as the gatekeeper for the devices behind it. Any translation modules that are vendor provided will be installed as libraries for PBCONF to access. The device-specific translation modules are shown in Figure 4.

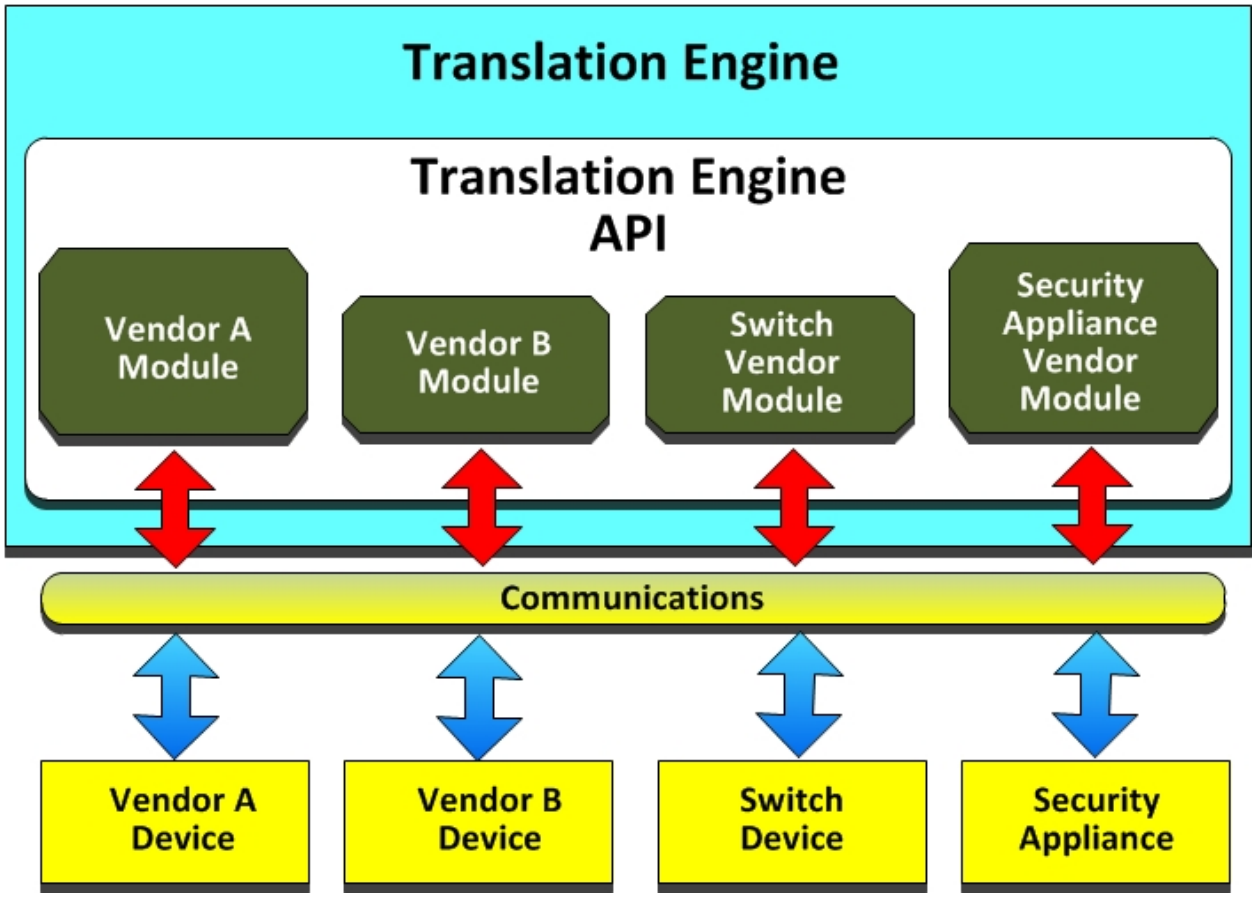


Figure 4: Example Device Specific Configuration Modules

The service container will provide a mechanism that the translation modules can use to compare an existing device configuration with the configuration generated based on the ontological policy for auditing, change control, and validation. The generation of these configurations must be deterministic to provide a valid comparison. The translation engine will ensure that the deterministic property is maintained by maintaining the order that commands were requested. Further, the deterministic translation will be designed to minimize the impact to the PBCONF and instead concentrate the bulk of the work in the device modules themselves.

Capabilities will be explored surrounding the notion of device state. Devices could be set in a state that does not allow the modification of configurations, only monitoring. If the device supports differing access levels, the authentication with the device will leverage the concept of least privilege to accomplish a given goal. For example, if the PBCONF node is only checking the configuration, it would likely not need to be in a mode that allows the changing of the configuration.

Because of the modular nature of the service container, the device modules may remain closed-source to protect any intellectual property the vendor views as proprietary. By leveraging a modular design and providing a well-defined interface for the modules, vendors can avoid exposing confidential configuration syntax, methodology, algorithms, or other functions while interacting seamlessly with other open- and closed-source modules and the service container itself. To ensure that vendor-developed translation modules can be relied on to accurately represent the requested policy as a proper device configuration (e.g. does not configure elements of the device that are not represented in the policy), all vendor translation modules will require a cryptographically secure digital signature. The translation engine will

verify this signature prior to loading the translation module. If signature verification fails, the translation engine will refuse to load the module. The details of the signature format, signing, and verification process will be developed during translation engine development.

As part of PBCONF, several framework-based supporting functions will be written. This will include a general communication framework that will implement the most common transport layer communication methods. For example, both TCP and serial communication capabilities will be implemented. As with other aspects of the PBCONF system, these transport implementations can be replaced or modified, and additional transport modules can be implemented. In addition, some device-specific translation modules will be created. Those pieces will be released as open-source, but there are no restrictions on allowing the use of any externally created modules.

Initially, translation modules will be developed for several model devices. This does not preclude other devices from being selected, nor does it limit the capabilities of other modules being created. The PBCONF system will be open source and extensible, and the translation module API will interface with the system in a way that allows for IP protection of any information that the vendor deems as proprietary in configuring their devices.

Translation Representation

Mapping the ontology to the corresponding class-derived commands will be done by creating a representation of the intended command that is presented to the translation module. These representations will likely be derived from ontological definitions of either object or data properties associated with classes in the ontology. The command-set will be determined as the project moves into implementation and the ontology is fully engineered. An example of a command may be “adduser” with a provided data structure of the supporting user information (e.g., username, password) needed to add a specific user.

The command data structure will be defined in a generic way and represented as a JSON object structure to the supporting translation module. This will allow for flexibility in data representation and extensibility to add additional fields without complication.

The outputs of the translation engine will take the form of accept, reject, success, or error to represent that the device is capable of mapping the command (ACCEPT), unable to map the command (REJECT), ran into an issue executing the mapped command (ERROR), or succeeded in executing the command (SUCCESS).

It is yet to be determined how every potential translation module will function, but it is intended to create a flexible system that will accommodate several modes of operation. For example, in configuring some devices, you may be required to issue all configuration commands on the device rather than being able to only incrementally issue commands that change particular settings. In such cases, the modules will be able to specify their required mode of operation so that the PBCONF communications layer can interface with the translation module appropriately.

At this point in time, anything that cannot be represented in the ontology will not be configurable using PBCONF. This means that any device command set capabilities that are not defined by the ontology cannot be executed independent of the defined command set. As a result, there will be no immediate way that arbitrary commands can be sent to a device, except to send them as raw device-specific commands. A mechanism will be provided to support issuing these raw commands; however some limitations may be put in place to limit the application of arbitrary commands to the device. These limitations may be expressed as rules on a raw class object in the ontology.

New Protocols for Secure Device Access

As part of PBCONF, the team will explore the implementation of a module to support the configuration of the password-changing protocol [TCIPGPASS] work that has been conducted as part of TCIPG's research. The goal of that effort is to investigate a robust, scalable, and automated password-changing protocol framework to ensure unique authentication of personnel in the presence of widespread use of remote access, and to ensure secure access to data inside the handheld and telemetric resource-constrained devices along with secure delivery of data over the wireless network in the field in real-time under varying maintenance scenarios.

The password-changing protocol work has been prototyped, and refinement of the approach is continuing based on feedback and strong interest from the energy sector. As the protocol is still at the research refinement stage, there are still no manufacturer-based implementations. However, PBCONF is expected to support its configuration to demonstrate the adaptability of the framework.

Configuration Auditing and Change Management

The service container will implement a change management engine. The engine will give the PBCONF node the ability to track security configuration changes as well as maintain a log of security configuration changes applied to end devices. The change management engine will likely be backed by the Git distributed revision control system.

Each PBCONF node instance will maintain a single Git repository that contains all the devices under its locus of control. The engine will store the filtered device configuration information from the device and compare it to the security configuration generated by the policy. Any changes will be compared and tracked via the Git repository, which includes an audit log and time stamping. That will provide the foundation of the change management system. Where PBCONF must maintain a copy of the entire device configuration (when a device does not support incremental configuration changes), only those device configuration options that can be represented by the ontology will be written to the repository. Due to the device authoritative nature of PBCONF, however, the repository audit log may include changes outside of the scope of device security configuration options that are managed by PBCONF.

The master will use subtrees to represent the other nodes in the system. The master node will have a global view of all the subordinate nodes, and their corresponding change managed information. Each subordinate node will only have the visibility of its subtree. This helps provide data isolation and segregation while controlling the sizes and histories of each individual repository.

An operator will be able to use the web-based API to request the change log for a device or devices from a PBCONF node. The PBCONF node will retrieve the audit log from the Git repository, including recorded security configuration changes from any point in time after the PBCONF node began managing a device.

Configurations will be stored in the Git repository in both a well-defined, JSON-encoded, deterministic format and in their native command format or parameters, when available. Storing configurations deterministically will enable the PBCONF node to quickly and reliably isolate security configuration changes, and generate reliable audit logs. By storing the actual configuration commands or parameters, operators will have a way to inspect the translated commands for further assurance.

/node & /device (External API)

Endpoint	Method	Request Parameters	HTTP Status Code	Return	Comment

Endpoint	Method	Request Parameters	HTTP Status Code	Return	Comment
/<namespace>/log	GET		200	Raw Git log	
/<namespace>/search	GET	Query string	200	Results of searching the Git log for <query string>	Searches for a string
/<namespace>/diff	GET	Old Revision New Revision	200	The contents of the diff between the two revision	Return the differences between two revisions

Configuration Validation

Before it applies the security configuration to an end device, the PBCONF node will validate the end device's current configuration against the stored configuration. Inconsistencies will be reported to the operator, and will require further action prior to application of the new requested configuration. The service container will aid in that functionality to ensure that the comparison is done correctly and uniformly across devices.

After applying a requested security configuration to an end device, the PBCONF node will request the current security configuration from the device. That configuration will be compared to the requested configuration to ensure that the requested configuration was successfully and properly applied. If that validation fails, the operator will be notified. Further errors will result in that device's being marked as noncompliant.

Reports

PBCONF will provide several forms of reports. Pre-defined reports will cover several common reporting needs. For example, PBCONF will include a predefined report listing all PBCONF alerts generated over various periods of time. Other possible pre-defined reports may include device lists, security configuration actions, and policy conflict reports.

The reporting engine will support periodic execution of predefined reports. In these instances, an operator will set a schedule on a report, and the PBCONF system will execute the report based on that schedule. In addition, an operator may set a report to create a notification upon completion. When notification is enabled for a report, PBCONF will utilize the alert and notification system to issue a notification that a report has completed.

In addition, PBCONF will implement an interface for operators to define, save, and execute new reports. Using a query language, such as SPARQL or SADL, operators will be able to define a new report to be executed by the reporting system. The specific queryable parameters will be determined during development; however, at a minimum it should include all configuration elements of device configurations (live and stored) if possible.

Web-Based GUI

In addition to the service container, there will be an example policy and configuration management web interface. The interface will require authentication and will tie into a basic access control system that will delineate functionality of the interface. The web interface will interact directly with the policy engine. Operators will use the web interface to define global and device-specific policy rules, which will be sent to the policy engine via the same web-based API that the policy engine uses to communicate with service containers. An operator will also use the web interface to define ontological configurations, which will also be submitted to the policy engine for evaluation and subsequent submission to master PBCONF nodes.

Defined User Interfaces

The web interface will provide several areas for interacting with the PBCONF system. For example, the web interface will implement an administration area. This area will contain options for various administrative tasks such as setting connection properties for slave PBCONF nodes. The administration interface will also allow operators to update and configure security certificates and view system alerts. Further, there will be at least basic access levels defined for user interface capabilities (e.g., administrator versus view only mode).

The web interface will also contain a report builder interface. This interface will enable operators to create and edit reports using a query builder. In addition, operators will be able to run reports, view past reports, and export reports in several formats, including PDF and HTML.

Other interfaces will be assessed as the project moves forward with implementation.

Operational Considerations

Node Discovery and Connection Management

When provisioning a new PBCONF node, the new node must be informed of its place in the hierarchy. The new node must be granted permission to connect to other nodes that may be upstream, downstream, or parallel. The new node must be configured with the connection information for any directly connected nodes. A new PBCONF node will need three pieces of information to make a connection to another node. First, the new node will need to be configured with the connection information. Second, the new node will need the neighbor node's public certificate or certificate chain, which will be used to authenticate the neighbor node. Finally, a new node will require its own X.509 identity certificate. The certificate will be used to authenticate the new node and encrypt communications.

In addition, the neighbor nodes will require the first two pieces of information about the node that is being added. Once all information is entered, the new node will request policy and device security configuration updates (see synchronization section for details).

The new node must also be granted permission to connect to end devices.

Policy Rules and Operation

New policy rules can be added to the system in one of two ways. Users may directly enter policy rules using the web based GUI. This should be performed using a master node.

When a policy update has been entered, the node that received the new policy will contact any directly connected downstream nodes and update that node's policy using the API.

Device Discovery and Management

When adding a new device to a hierarchy, the directly connected node needs to be notified of the new device. This is done using the web based GUI or the API (the web based GUI uses the API). PBCONF needs to be configured with all of the information required to connect to the device. The details of this connection information are device specific, but may include connection mechanism (telnet/serial/ssh/etc) and parameters associated with the connection mechanism (e.g., baud rate for serial or IP address for telnet) and the type of device (to select the correct translation module).

Once the device has been configured in PBCONF, the node will request the device's security configuration parameters, and create an initial version of the configuration on the node. When the master initiates the synchronization process, the node will send the end device security configuration to the master. The security configuration may be revised based on the policy in the master.

PBCONF Use Cases

As described earlier, PBCONF supports the secure configuration of heterogeneous devices. This section provides an example of how PBCONF will support that operation using the architecture previously discussed.

Leveraging PBCONF for Enhanced Security and Increased Compliance

PBCONF brings value to the energy sector in many ways, including assistance with NERC CIP compliance, auditing and logging of changes to security-related configuration of heterogeneous devices, and the streamlined application of security policy on energy sector devices. It further adds value by leveraging the framework to secure remote communications for maintenance access and pushing the envelope of security further inside the utility boundary, providing defense in depth. To illustrate, an example application of PBCONF is provided that represents a scenario typical in the energy sector. Note that this is just one example of many ways the system could be utilized.

In current practice, many of the mechanisms for accessing and configuring energy sector devices are isolated from each other, and policy configuration is done manually. The following scenario shows how the current practice would differ from the proposed use of PBCONF.

Scenario

A utility's chief security officer (CSO) would like to evaluate the security policies associated with the energy sector devices under the control of the utility. The CSO requests a report that shows what the current security policy is and which devices are in compliance with that policy.

Current Approach

The Operations IT (OIT) group would gather the information on the security policies that have been defined for their devices. Those policies may require assessment of the configuration parameters set on each device and a determination of why they were set. Once those configurations have been determined for each manufacturer, the OIT group would then need to access every device that is configured to gather the devices' configurations. It is likely that this step would involve the need to access every field device (potentially in an insecure way) or send field technicians to check the configurations of devices in the field where localized access is required to check the configuration. Once the data has been collected manually, it has to be assessed for variance from the policy for those devices. The assessment may be error-prone and may not guarantee of accuracy. Once any variances have been determined, the report can be finalized and delivered to the CSO. The process may a significant amount of time to execute for a utility with a large service territory.

PBCONF Approach

With PBCONF, the OIT group would open the web interface of the master PBCONF node and select the policy or set of policies they are interested in looking at. Next, they would request that a compliance check be run by the system, which would then automatically securely connect to each of the remote devices, verifying the current configuration and determining whether it is in compliance with the selected policy. The report would include the applied policy, the devices that were out of compliance, and the devices that were in compliance. It would further include any data the PBCONF system has regarding when that policy was applied to each device and when the last security policy update on that device occurred. Any variances that are detected could be corrected automatically if the OIT group chooses to have the system push an approved version to the remote device. Further, any of the devices that are out of compliance could be explored in more detail to reveal the configuration differences, or could be remotely connected to in a secure way to allow further exploration of the device configuration. Once the report has been generated, it can be printed or saved to share with the CSO. The process would be expected to take minutes to hours, depending on the methods of access, and would provide machine-assisted formalisms for comparison rather than a potentially error-prone manual assessment.

Use Case Categories

- Case 1: Secure change management
- Case 2: Monitoring for security configuration changes
- Case 3: Auditing and reporting
- Case 4: Secure remote access
- Case 5: Global policy application
- Case 6: Authorization and non-repudiation

Included in the appendixes to this design document are use cases, NESCOR failure scenarios, and use case repositories. All are being assessed for applicability to PBCONF and will be selected and tailored, as appropriate and allocated to the appropriate use category listed above.

Scientific Validation

Validation Methods

Validation of the configuration architecture described in the previous sections will take place in two stages, described below.

Stage 1: Lab Testing

The PBCONF nodes and energy sector devices that will be supported under the demonstration will be set up in a lab environment. Several example policies that are derived from utility input will be defined and configured for the application. The devices under management will have their configurations modified manually to verify that the system has the ability to detect those modifications (and optionally correct them). Similar testing, including a security assessment, will be performed to exercise the base functionality of the system prior to more distributed deployment.

Stage 2: Distributed Deployment

Once any system deficiencies discovered during Stage 1 testing have been corrected, Stage 2 testing will begin with distributed deployment to the teaming partners. That will entail distributing PBCONF nodes

among the teaming partners that have been configured with the master at U of Ill. Those nodes will then exercise control over a set of devices behind them. Functionality assessments similar to those in Stage 1 will be conducted, with attention paid to any differences resulting from the distributed layouts of the locations. The core team (U of Ill and EPRI) will work with Ameren to ensure that the product meets utility deployment and usability requirements and provides security and communication characteristics that are within the utility's constraints for operational deployment.

Platform Specifications

The implemented architecture will be deployable on any modern computing infrastructure since the expected computational requirements are minimal. However, a typical deployment is anticipated to consist of a mid-level server as the central master node, with hardened or embedded systems as the slave nodes. One suggested specification for the central master node would be a Dell R720 2U rack mount server with a dual-processor, 8-core hyper-threaded architecture. This would provide a single machine that could offer 32 effective processors, scalable storage, and a large RAM capacity to ensure both high reliability and sufficient processing power to handle thousands of devices under the control of that node. The slave PBCONF nodes will likely be deployed on existing substation-hardened platforms, such as SEL-3354 substation computers or other similar embedded devices. It may be possible to deploy these nodes on low-cost hardware, such as the Raspberry Pi or hardened Gumstix platform, although that equipment is not certified for substation deployment.

Project Validation Efforts

Technical Approach and Project Management

The foregoing discussion outlines elements of the technical approach in the areas of secure configuration and remote access. The approach can be summarized as follows:

1. Configuration Architecture. A distributed architecture is a natural response to the need to integrate both legacy devices and future devices. It provides the ability to push the security as close to the end devices as possible. The approach allows for a hybrid approach, letting the system use a pure centralized approach if necessary, but with weaker security guarantees.

2. Applied Configuration Example. The project will show a realistic application of the PBCONF technology to address secure configuration and remote access for the energy sector. Note that the provided example will be only one of many applications, and that the distributed configuration architecture design will be flexible enough that it can be extended to address many future applications.

3. Validation. The architecture will be validated both in a lab environment and with one or more partners in a distributed architecture. The project will demonstrate that the communications and policy requirements are adequately met by the distributed configuration architecture. The findings will be disseminated to stakeholders and the research community at large with the goal of transitioning the technology.

The project will have two phases: 1) research and development and 2) demonstration.

The research and development phase will develop the ontology, PBCONF node, ontology logic, and distributed architecture. PBCONF will be designed to support heterogeneous device configurations both for existing legacy devices and for new digital devices that will have new functionality. The focus of the PBCONF will be on providing secure and interoperable security related configuration controls (e.g., authentication, authorization, auditing, and access control). When devices have been configured securely but do not support a secure access method for maintenance or engineering, the distributed configuration

framework can broker a secure channel for that access up until the last hop. Further, since this framework will be dealing with selective configuration of devices, it has the ability to act as an audit component, keeping track of applied configurations and any variance from global policy.

The project will develop and demonstrate a reference implementation for the PBCONF, with support for heterogeneous device configurations. The core team will work with the partner organizations to carry out the demonstration in Phase 2. The demonstration will highlight the features of the system and will both leverage and exercise those features throughout the demonstration to configure, audit, and monitor the security related configuration of the devices.

The reference implementation will be open-sourced, and the vendor-specific modules will access the framework via an open, well-defined API, but the vendor-specific modules themselves will not need to be open-source. That will allow the vendors to protect any intellectual property regarding the configuration of their devices that is important to them. PBCONF will build upon the successful automation tools developed internally at U of Ill for testbed automation and configuration.

The project participants will move PBCONF towards deployment by working on vendor adoption via working/interest groups via outreach efforts, by doing an open-source code release, and by holding workshops related to the development, architecture, and implementation of the framework that will be organized by EPRI.

The project unites the following entities:

- The Electric Power Research Institute (EPRI), a lead research institute representing the interests of its member utilities
- The University of Illinois at Urbana-Champaign (U of Ill), lead institution of the Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) Center
- Ameren, a leading utility in the Midwest
- Schweitzer Engineering Laboratories (SEL), a leading vendor in power system hardware

A reference implementation of this framework will be validated to determine its efficacy in supporting the secure configuration of security related configuration parameters across a heterogeneous environment. The core team will also perform technology transfer of results, methodologies, and tools to the utility and industry partners, as well as to the research community.

Energy Sector Impact

Incorrect or inconsistent configuration of the multitude of energy sector devices in the field is a large potential attack vector. By applying a uniform security policy across devices in a way that provides consistency and visibility, this attack vector can be mitigated. Further, both utilities and vendors have indicated the need for configuration through remote access methods for energy sector devices in a uniform way rather than through mutually isolated applications (stovepipes). Some vendors have standardized their device configurations to address this issue, but those solutions are typically only for that vendor's devices. A vendor-neutral framework for secure configuration and remote access is needed to solve these problems for the industry.

The Secure Policy-Based Configuration Framework (PBCONF) addresses these needs through its ontology-driven policy, modular architecture, and distributed secure architecture. The PBCONF system can further serve as an audit tool, allowing an organization to maintain a change-managed repository of the remote access methods implemented on the configured systems. If the remote access configuration of

devices is secured via this mechanism, a utility can also gain efficiency by centrally applying its policies across all devices or sets of devices in a controlled and verifiable way.

The PBCONF approach provides a model for implementation and deployment that is cost-effective and has the potential to dramatically impact the cyber security of the energy infrastructure. This approach will support not only legacy devices but also future devices that have not come to market. The distributed nature of the system provides fault tolerance and increased resiliency and reliability in secure configuration and remote access to the devices and will support monitoring of the configuration.

Commercialization

Open-Source Release

The project will include an open-source implementation of the PBCONF node and a supporting GUI interface, a well-specified and open ontology for describing the security policy, and a well-specified and open API for the translation of ontological policy to vendor-specific configurations. The translation modules would not need to be open-sourced, which would allow vendors to protect any IP that is associated with the configuration of their devices. In order to support the demonstration of the framework, preliminary support will be provided for any necessary devices as part of the open-source implementation, along with a support library that will aid in writing more modules in the future. This approach should facilitate the adoption of the framework by a multitude of vendors and result in more widespread support.

Utility

PBCONF will leverage its utility partner, Ameren, to provide an environment for pilot test and validation of all key aspects of the project, using actual power system hardware and real test environments to the degree possible. PBCONF slave nodes will be deployed both to distribute communications and to configure systems. If successful, the environment will demonstrate the efficacy of the distributed configuration approach for secure remote access, and demonstrate the ability of the developed framework to support the definition and application of global security policy. Refer to the scientific validation section for more information on these planned deployments.

Relevance and Outcomes/Impacts

PBCONF will enable secure configuration and remote access, driven by global policy and applied to heterogeneous devices, for both legacy and emerging energy sector devices. Further, it will provide audit, change management, and verification and validation of any deviation from global policy. Those features are beneficial for bottom-line efficiency and can also serve as tools for compliance with regulations such as NERC CIP.

An iterative experimentation-development process will validate all key concepts and developments of the project. Assessment of results will take place continuously, permitting the team to identify issues early on and make recommendations for program improvement and research re-prioritization. By the time the validation task starts, concepts and tools will already be extensively tested.

Existing synergistic activities among the partner organizations provide evidence of the team's ability to collaborate across power and cyber disciplines, across research organizations, and with active engagement of industry and technology vendors. The support and involvement of both utilities and vendors will promote project impact and adoption of results.

In summary, PBCONF will provide secure configuration and remote access via a deployable framework that enables a flexible environment for future support and vendor adoption while going beyond proof of concept to a demonstration system.

Facilities and Other Resources

Specialized Equipment

The testbed resources of the supporting institutions and the corresponding communication infrastructure will be leveraged for PBCONF both as tools and as validation sources. PBCONF nodes will be installed in various forms in the testbed locations and at other partner locations. The U of Ill testbed facility will serve as the master node location.

Acronyms

AGPL	Affero General Public License
API	Application Programming Interface
BSD	Berkeley Software Distribution License
CIM	Common Information Model
CIP	Critical Infrastructure Protection
COEDS	Cyber security Ontology for Energy Delivery Systems
CPTL	Cyber Physical Topology Language
DB	Database
DOE	Department of Energy
GPL	GNU General Public License
GUI	Graphical User Interface
HSTS	HTTP Strict Transport Security
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IP	Intellectual Property
JSON	JavaScript Object Notation
LGPL	Lesser General Public License
MIT	Massachusetts Institute of Technology
NESCOR	National Electric Sector Cybersecurity Organization Resource
NIST	National Institute of Standards and Technology
OATH	Open Authentication
OWL	W3C Web Ontology Language
PBCONF	Secure Policy-Based Configuration Framework
RDF	Resource Description Framework
RDQL	RDF Data Query Language
REST	Representational State Transfer
RFC	Request for Comments
SAML	Security Assertion Markup Language
SSH	Secure Shell
TLS	Transport Layer Security

Glossary

API

The specification for how components of the application will interact with each other.

CIM

A standard that defines how elements in an infrastructure and their relationship can be represented.

CIP

A plan of requirements for the energy sector that are then utilized for compliance.

Endpoint

Similar to a function call in a traditional application. Denoted by a URI and allows HTTP methods to be performed on an entity.

Entity

An encoded representation of data that is returned by (e.g. the GET method) or sent to (e.g. the PUT method) an endpoint.

Git

A distributed version control system, which is planned to be the core of the PBCONF change management component.

Go (Golang)

A statically typed programming language derived from the C programing language. Golang was initially developed by Google, and was designed with a focus on concurrency.

Hook

A mechanism that enables third parties to extend the capabilities of an application.

Master Node

The PBCONF node that is the highest in the hierarchy.

Metadata

Additional information that supplements existing raw data in some context.

O-Metadata (ontology)

Metadata that augments or is utilized by an ontology.

S-Metadata (system)

Metadata that is directly related to the devices in the PBCONF.

OATH

An open standard for secure delegated authentication.

Ontology

A formal representation of knowledge that captures both objects and their relationships. In PBCONF, ontologies will be used to formally describe devices and device capabilities within the security domain. Rules on the ontology will be leveraged to describe policies.

Plugins (Applicability to PBCONF)

A semi-independent component, which uses hooks, to extend the capabilities of the system. Third party developers may develop plugins to add additional features to PBCONF without changing existing behavior.

REST

A software architectural style that relies on the web standards to implement component intercommunication.

SAML

An XML based standard for exchanging authentication and authorization data between systems.

Semantic Model

A data model that describes the meaning of the data in the model, and enables systems to interpret the meaning of the data.

Slave Node

A PBCONF node that has a parent node (a slave lies below a node in the hierarchy). The parent node could be another slave node or could be the master node for the respective hierarchy.

Syslog

A standard for message logging that is described in IETF RFC 5424.

Taxonomy

A description of objects not including their relationships.

Translation Module

A component which, given a policy, generates device specific commands to apply a PBCONF policy to a device.

Bibliography

[COEDS] Cybersecurity Ontologies for Energy Delivery Systems. https://github.com/timyardley/CoEDS

[CPTL] Gabriel A. Weaver, Carmen Cheh, Edmond J. Rogers, William H. Sanders, and Dennis Gammel. 2013. Toward a cyber-physical topology language: applications to NERC CIP audit. In *Proceedings of the first ACM workshop on Smart energy grid security* (SEGS '13). ACM, New York, NY, USA, 93-104. DOI=10.1145/2516930.2516934 http://doi.acm.org/10.1145/2516930.2516934

[BEAST] Thai Duong, Juliano Rizzo. 2011. Here Come The Ninjas. https://bug665814.bugzilla.mozilla.org/attachment.cgi?id=540839.

[HEARTBLEED] CVE-2014-0160. Common Vulnerability and Exposures. 2014. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160.

[HL7SEC] "Security and Privacy Ontology," HL7 International, Apr. 13, 2012. http://wiki.hl7.org/index.php?title=Security_and_Privacy_Ontology

[HSTS] http://tools.ietf.org/html/rfc6797

[NRL2005] Anya Kim, Jim Luo, and Myong Kang, "Security Ontology for Annotating Resources." Published in R. Meersman & Z. Tari (Eds.), *CoopIS/DOA/ODBASE 2005*, *LNCS* 3761, pp. 1483-1499, Springer-Verlag Berlin Heidelberg, 2005 (online at http://www.nrl.navy.mil/chacs/pubs/05-1226-0470.pdf) and as Naval Research Laboratory technical report NRL/MR/5542--05-8903, Aug. 31, 2005 (online at http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA437938).

[OWL2004] "Web Ontology Language (OWL)," W3C Semantic Web, Oct. 15, 2007. http://www.w3.org/2004/OWL/

[PROTÉGÉ] Protégé home page, Stanford Center for Biomedical Informatics Research, 2013. http://protege.stanford.edu/

[REDLAND] Redland RDF Suite Homepage. http://librdf.org/

[RESTCODES] REST Patterns. HTTP Status Codes. http://restpatterns.org/HTTP_Status_Codes

[RFC2616] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee. 1999. Hypertext Transfer Protocol (online at http://www.ietf.org/rfc/rfc2616.txt)

[SADL] Semantic Application Design Language. http://sadl.sourceforge.net/

[SPARQL] "SPARQL Query Language for RDF," World Wide Web Consortium (W3C), Jan. 15, 2008. http://www.w3.org/TR/rdf-sparql-query/

[TCIPGPASS] "Research Activity: Password Changing Protocol," TCIPG Trustworthy Cyber Infrastructure for the Power Grid. http://tcipg.org/research_Password-Changing-Protocol

PBCONF APPENDIXES

Included in the appendixes are National Electric Sector Cybersecurity Organization Resource (NESCOR) failure scenarios, National Institute of Standards and Technology Interagency Report (NISTIR) 7628 sections, and use cases that are applicable to the PBCONF project. The material included in these appendixes is the initial set and will be revised and tailored as the project progresses.

Appendix A: NESCOR Failure Scenarios

NESCOR Failure Scenarios: Included below are NESCOR failure scenarios that are applicable to the PBCONF project. The failure scenarios have been extracted from the full set of failure scenarios included in the NESCOR document. The scenarios were selected from version 1.0 that was published in September 2013.

1. Distributed Energy Resources (DER)
2. Wide Area Monitoring, Protection, and Control (WAMPAC)
3. Distribution Grid Management (DGM)
4. Generic

Distributed Energy Resources (DER)

This section presents a set of failure scenarios for the Distributed Energy Resources (DER) domain. DER systems are "cyber-physical systems that provide energy and ancillary services to the power grid, typically through the distribution system. DER systems can be generators, storage devices, and even electric vehicles if their chargers are capable of managing the charging and discharging processes. Generally DER systems are small", but they are becoming prevalent in the distribution system (potentially there will be thousands if not millions of DER systems interconnected with the distribution system).[1] The following concepts are used throughout the DER scenarios:

- *Distributed Energy Resource Management System (DERMS):* Utility system that manages the requests and commands to the DER systems. It is also responsible for the database of interconnection permits and registrations of DER systems.
- *Field DER Energy Management System (FDEMS):* System that manages combinations of DER generation, DER storage, and customer loads at a residential, commercial, or industrial customer site.

DER.7 Incorrect Clock Causes Substation DER System Shut Down During Critical Peak

Description: A utility-owned DER system is located in a substation with the primary purpose of providing additional power during a critical peak. A threat agent changes the time clock in the DER system through a false time-synchronization message, so that either the DER system believes that the critical peak event is over or that all time-stamped messages to it are invalid, so it goes into default shut-down mode.

Relevant Vulnerabilities:

[1] NESCOR Guide to Penetration Testing for Electric Utilities, http://www.smartgrid.epri.com/doc/NESCORGuidetoPenetrationTestingforElectricUtilities-v3-Final.pdf

- The time synchronization communication protocol does not adequately authenticate messages or ensure their integrity,
- The DER system does not notify or request confirmation of changes from the utility DER management system before taking actions.

Impacts:

- The DER system performs an immediate shut down and causes damage to a transformer,
- Customer outages occur during the critical peak,
- Utilities need to curtail customer generation and/or loads until a new transformer is installed.

Potential Mitigations:

- *Authenticate messages* in the time synchronization communication protocol,
- *Check message integrity* in the time synchronization communication protocol,
- *Cross check* operationally critical actions with the utility DER management system before acting.

DER.9 Loss of DER Control Occurs due to Invalid or Missing Messages

Description: A malicious or non-malicious individual causes the loss of DER control due to invalid or missing messages. Since the DER system either tries to act on invalid messages or no longer has messages constraining its output, it causes a distribution transformer to overload, thus causing an outage for the site and for neighboring sites. The DER system also sustains damage due to invalid settings.

Relevant Vulnerabilities:

- Lack of message authentication.

Impacts:

- A distribution transformer is damaged,
- A local outage occurs that requires field crews to replace the damaged transformer,
- The DER system may sustain damage due to trying to act on invalid messages or not being constrained by expected messages that did not arrive.

Potential Mitigations:

- *Authenticate messages* in all communication protocols,
- *Validate data* in DER systems messages as reasonable and within the DER intrinsic capabilities,
- *Generate alarms* for messages that fail message authentication,
- *Create audit log* of messages that fail message authentication.

DER.12 Modified Management Settings for Substation FDEMS Impact Power Quality

Description: A malicious individual accesses a utility FDEMS that manages DER generation and storage systems within a substation, and modifies the energy output, the volt-var curves, or other DER management settings. When the utility requests the FDEMS to control the DER systems to provide more vars, the FDEMS causes the DER systems to behave erratically and cause the substation to have power quality problems, including tripping of the transmission line breaker.

Relevant Vulnerabilities:

- Inadequate access control for critical settings in FDEMS,
- Inadequate logical access control for the FDEMS network and operating system,
- Inadequate physical access control to the FDEMS system.

Possible Impacts:

- Power system power quality problems, including erratic supply of vars to the transmission system,
- An outage of all feeders in the substation.

Potential Mitigations:

- *Restrict application access* for all FDEMS user interface interactions,
- *Authenticate users* for all FDEMS user interface interactions,
- *Enforce changing default credentials* as a system enforced step during installation,
- *Use RBAC* in the FDEMS system,
- *Enforce least privilege* for access to the FDEMS operating system and physical host,
- *Enforce restrictive firewall rules* for access to the FDEMS network,
- *Require multi-factor authentication* for users requesting remote access to the FDEMS.

DER.14 DER Systems Shut Down by Spoofed SCADA Control Commands

Description: A threat agent spoofs DER (supervisory control and data acquisition) SCADA control commands to perform emergency shutdowns of a large number of DER systems simultaneously.

Relevant Vulnerabilities:

- Inadequate authentication mechanisms used by DER SCADA communication protocols,
- Inadequate network and system management to detect intrusions,
- Inadequate access control applied to the DER SCADA system.

Impact:

- Power system instability, including outages and power quality problems,
- Utility legal costs related to DER owner litigation for loss of revenue.

Potential Mitigations:

- *Limit events*, specifically the number of shutdown events of DER systems within a specified time period,
- *Use RBAC* in the DER SCADA,
- *Authenticate data source* for the DER SCADA protocols,
- *Authenticate messages* that convey the DER SCADA control commands,
- *Validate inputs* (as a consistency check) for the DER SCADA control commands,
- *Require intrusion detection and prevention* as part of DER SCADA network management.

DER.15 Threat Agent Spoofs DER Data Monitored by DER SCADA Systems

Description: A threat agent modifies the industrial and the larger commercial DER data being monitored by the utility distribution DER SCADA system in real-time, altering the load value so that it is much higher than the actual value. Although this modification does not affect the monthly revenue metering for these DER systems, it causes the utility to request and pay for additional ancillary services from a neighboring DER storage system.

Relevant Vulnerabilities:

- Inadequate data source authentication employed by the DER SCADA communication protocols,
- Missing consistency checking between load value and meter values.

Impact:

- Increased utility costs for unnecessary ancillary services,
- Utility legal costs for finding and litigating the threat agent.

Potential Mitigations:

- *Use role based access control (RBAC)* for the DER SCADA,
- *Authenticate data source* for the DER SCADA protocols,
- *Authenticate messages* that convey the DER SCADA control commands,
- *Require intrusion detection and prevention* as part of DER SCADA network management.

DER.16 DER SCADA System Issues Invalid Commands

Description: A threat agent breaches a DER SCADA system and causes the DER SCADA system to issue an invalid command to all DER systems. Since DER systems may react differently to invalid commands, the power system experiences immediate and rapid fluctuations as some DER systems shut down, while others go into default mode with no volt-var support, still others revert to full output, and a few become islanded microgrids. The distribution

equipment tries to compensate automatically, but causes more problems as the voltage experiences severe surges and sags.

Relevant Vulnerabilities:

- Inadequate authentication and access control mechanisms.

Impacts:

- Power system rapid fluctuations that cause power quality problems for customers, including outages,
- Equipment damage (that can lead to loss of life) due to power system surges and sags,
- Transmission power quality problem.

Potential Mitigations:

- *Authenticate users* accessing the DER SCADA system,
- *Authenticate messages* communicated in the DER SCADA network,
- *Use RBAC* in the utility's DER SCADA system,
- *Check message integrity* for messages issued by the DER SCADA system.

DER.18 Microgrid Disconnect Process Compromised via DERMS

Description: A threat agent gains access to the utility DERMS system and alters the conditions that determine when a utility has permission to disconnect a pre-established microgrid from the grid. This modification causes the microgrid either to disconnect at some random time in the future, or to prevent it from disconnecting even when it is supposed to disconnect (e.g., in the case of an outage).

Relevant Vulnerabilities:

- Inadequate access control applied to the DERMS system,
- Lack of protection against changes to utility permissions for microgrid disconnect,
- Lack of message authentication and message integrity.

Impact:

- Since the microgrid may not be prepared to disconnect from the grid or may be brought down during the grid outage, it will experience a complete outage,
- Legal costs for litigation with the adversely affected customers.

Potential Mitigations:

- *Use RBAC* to limit those users authorized to change microgrid establishment permissions in the utility's DERMS system,
- *Require intrusion detection*, as part of DERMS network and system management capabilities,

- *Require resiliency* of communications path between the utility and the microgrid management system, to support immediate transmission of such alerts, without additional infrastructure,
- *Require multi-factor authentication* for operationally critical functions, such as modifying configuration files,
- *Authenticate messages* containing alerts to microgrids,
- *Check message integrity* for messages containing alerts to microgrids.

DER.19 Threat Agent Gains Access to Utility DERMS via FDEMS

Description: A threat agent uses a FDEMS to which they have full access, to access the utility's DERMS system. The threat agent is able to modify the DER commands, schedules, and requests sent to other DER systems, making these settings beneficial to their own DER systems, and consequently less beneficial to other DER systems.

Relevant Vulnerabilities:

- Inadequate authentication mechanisms used by the DERMS communication protocols to access the FDEMS,
- Inadequate access control applied to the DERMS system,
- Lack of message authentication and message integrity for the DERMS data accessed from remote locations,
- Lack of detection for unauthorized changes to DERMS functions.

Impact:

- Inefficient or cost-ineffective power system operated by the utility,
- Utility legal costs related to DER owner litigation for unfair practices.

Potential Mitigations:

- *Use RBAC* in the utility's DERMS system,
- *Authenticate data source* to access the DERMS,
- *Validate inputs* in the DERMS control commands,
- *Authenticate messages* containing DER commands,
- *Check message integrity* for messages containing DER commands.

Wide Area Monitoring, Protection, and Control (WAMPAC)

This section presents a set of failure scenarios for the Wide Area Monitoring, Protection, and Control (WAMPAC) domain. "WAMPAC systems constitute a suite of different system solutions aimed at meeting various wide-area application requirements." [2] "WAMPAC systems often center around synchrophasor technology and the devices that generate, receive, and utilize this

[2]NESCOR Wide Area Monitoring, Protection, and Control Systems (WAMPAC) – Standards for Cyber Security Requirements, http://www.smartgrid.epri.com/doc/ESRFSD.pdf

synchrophasor data. WAMPAC systems should be setup to include all components from the Phasor Measurement Unit (PMU) to the WAMPAC applications leveraging that data, including other intermediate devices such as the servers that manage the PMUs, devices that provide alignment services like Phasor Data Concentrators (PDCs), phasor gateways, phasor data stores, and other such components."

The impact of a failure scenario for WAMPAC is fully dependent upon the use of the WAMPAC data. For example, a failure in a WAMPAC application that offers control capabilities has a higher impact than a failure in a monitoring application. Currently, most utilities consider WAMPAC as a supplementary source of data; hence its failure impact is considered less significant. It is anticipated that WAMPAC will become a primary trusted data source in the near future.

NOTE: In Table 1 the possible impact of the WAMPAC failure scenarios are presented, which takes into consideration the state in which the system is in and also the nature of the application that the WAMPAC executes. Impacts that relate to "Loss of data for each application" are distinguished from impacts that relate to "Altered data or timestamps for each application". Each WAMPAC failure scenario refers to the impact presented in Table 1 that is applicable to it.

Table 1 Impact Examples Given the State in Which System is in and the Nature of the Application that the WAMPAC Executes

		Normal	Alert / Emergency
Monitoring	*Data loss*	• No impact	• Delay in taking actions (e.g. load shedding) • Delay in grid reconfiguration • Unnecessary power generation, overload of lines, or creation of fault conditions, if timely or appropriate corrective actions are not taken
	Altered data	• Control actions that create undesirable state	• Incorrect actions to be taken
Local Protection	*Data loss*	• No impact	• Failure in taking action, if no alternative data source is available
	Altered data	• Triggered protection mechanisms when not required • Line trip (which can be recoverable) • Improper synchronous closing, leading to equipment damage	• Line trip, which can lead to cascading failures if lines are overloaded and other protection takes place • Improper synchronous closing, leading to equipment damage
Special	*Data loss*	• No impact	• Delay in triggering protection elements • Overload of lines, or creation of fault conditions, if timely or appropriate corrective actions are not taken

		Normal	Alert / Emergency
	Altered data	• Line trip, which can lead to cascading failures if lines are overloaded and other protection takes place • Improper synchronous closing, leading to equipment damage	• Line trip, which can lead to cascading failures if lines are overloaded and other protection takes place • Improper synchronous closing, leading to equipment damage
Control	*Data loss*	• Control actions that create undesirable state	• Delay in taking actions (e.g. load shedding) • Delay in grid reconfiguration • Unnecessary power generation, overload of lines, or creation of fault conditions, if timely or appropriate corrective actions are not taken
	Altered data	• Taking action when none is necessary, such as opening/closing switches, turning on or shutting down generation • Failure to take action, when needed, leading to voltage or frequency conditions that could have been prevented	• Failure to take action, when needed, leading to voltage or frequency conditions that could have been prevented • Cascading failures

WAMPAC.3 Improper PDC Configuration Interferes with Transmission of Measurement Data

Description: An insider is able to gain access to the network to which a PDC is connected and to the PDC's credentials, assuming credentials are in place. This individual compromises (malicious intent) or misconfigures (accidentally) the PDC. Consequently, the PDC does not recognize certain PDCs/PMUs and sends incomplete measurement data up in the WAMPAC hierarchy.

Relevant Vulnerabilities:

- Firewalls nonexistent or improperly configured allowing access for an unauthorized insider to the PDC,
- Weak network security architecture allowing access to the PDC,
- No security monitoring on the WAMPAC network,
- Inadequate authentication and access control for configuration and programming software on the PDC,
- Insecure remote access to the PDC.

Impact:

- All impacts presented in Table 1, as potentially caused by loss of measurements.

Potential Mitigations:

- *Require redundancy* in PDCs using vendor diversity,

- *Restrict network service access* at multiple layers to prevent unauthorized individuals from gaining access to the PDC,
- *Restrict remote access* to the PDC,
- *Detect unauthorized connections* captured in the communication patterns to and from the PDC,
- *Require approved cryptographic algorithms* for authentication and message integrity on the WAMPAC network.

WAMPAC.4 Measurement Data Compromised due to PDC Authentication Compromise

Description: Although access control and connection authentication from a PMU into a PDC are in place, these are compromised. This may be due to a backdoor not subject to the usual controls, social engineering, network sniffing to gain credentials or an attack on the authentication database to modify or steal credential information. This allows inadvertent or malicious introduction of false measurement data.

Relevant Vulnerabilities:

- Authentication database hosted on a poorly protected network,
- Credentials not protected from disclosure while in transit or at rest,
- Access control enforcement mechanism that can be bypassed,
- Access and modification of the PDC/PMU configuration, which may include connection information.

Impact:

- All impacts presented in Table 1, as potentially caused by altered measurements.

Potential Mitigations:

- *Authenticate users* for access to PDC,
- *Restrict network service access to all interfaces on the PDC*
- *Protect credentials* used to authenticate the PMU to the PDC,
- *Change default credentials*,
- *Encrypt data at rest*, specifically credentials,
- *Encrypt communication paths* used to transmit credentials,
- *Require approved key management,*
- *Restrict remote access* to the network hosting authentication database,
- *Require intrusion detection and prevention* for the network hosting authentication database,
- *Authenticate users* to the network hosting authentication database*,*
- *Detect unauthorized access* to the network hosting authentication database,

- *Protect security configuration* that lists the systems permitted to connect to the PDC.

WAMPAC.5 Improper Phasor Gateway Configuration Obscures Cascading Failures

Description: An authorized or unauthorized insider (e.g., social-engineered by a threat agent or accidentally) is able to gain access and misconfigures a phasor gateway, allowing less synchrophasor measurement data to be shared with other phasor gateways or altering the tagging of PMU ID associated with the shared data. This action results in a delay in other utilities' visibility to a cascading failure across utilities.

Relevant Vulnerabilities:

- Inadequate authentication and access control for configuration and programming software on the phasor gateway,
- Inadequate testing of configuration changes without involving a verification and approval process,
- Insecure remote access to the phasor gateway,
- Lack of redundancy for critical components such as phasor gateways.

Impact:

- All impacts presented in Table 1, as potentially caused by altered data or loss of data, for Special Protection applications.

Potential Mitigations:

- *Require reconfiguration in test mode* for gateways,
- *Require 2-person rule* of test results that must be verified and approved by personnel/entities other than those that carried out the reconfiguration,
- *Require redundancy* of phasor gateways (vendor diversity),
- *Detect unauthorized configuration* at the gateway level.

WAMPAC.8 Malware in PMU/PDC Firmware Compromises Data Collection

Description: A threat agent inserts firmware into PMU/PDC that alters measurements while they are collected. The altering mechanism can be triggered at all times, randomly or by certain events (e.g. time of day, certain date, etc.) that are assumed to inflict significant damage.

Relevant Vulnerabilities:

- Inadequate security for configuration change management process by the manufacturer.
- No integrity checks at the firmware level,
- Inadequate access control for firmware updates.

Impact:

- All impacts presented in Table 1, as potentially caused by altered measurements,

- Significant effort/cost invested in troubleshooting the systems given the lack of measurement consistency, followed by equipment replacement.

Potential Mitigations:

- *Implement configuration management* for controlling modifications to firmware to ensure that a PMU/PDC is protected against inadequate or improper modifications before, during, and after firmware manufacturing,
- *Check software execution integrity* for the firmware , since software may be compromised when loaded for execution,
- *Require redundancy* in PMUs/PDCs using vendor diversity,
- *Restrict system access* for firmware install/updates.

WAMPAC.10 Compromised PMU/PDC/Phasor Gateway Metadata

Description: A threat agent is able to gain unauthorized access to the credentials of the PMU/PDC/Phasor Gateway metadata that describes the data structure, assuming credentials are in place, and corrupts or deletes the associated metadata from the database.

Relevant Vulnerabilities:

- No security monitoring on the WAMPAC backend,
- Inadequate access control on the WAMPAC network,
- PMU configuration database accessible with weak or no credentials.

Impact:

- All impacts presented in Table 1, as potentially caused by altered measurements,
- Significant effort/cost invested in troubleshooting the systems given the inconsistencies in PMU data attribution.

Potential Mitigations:

- *Detect unauthorized configuration* in the configuration databases,
- *Restrict database access* to applications that require access,
- *Require multi-factor authentication* for local administrators that require access,
- *Encrypt data at rest* for database contents related to the PMU configurations.

WAMPAC.11 Compromised Communications between Substations

Description: An insider delays local measurement data exchange between substations by compromising the integrity of the WAMPAC communication link between substations. This might be done by attacking network components such as routers, or gaining access to the network and employing a flooding attack.

NOTE: The impact of the failure scenario presented below is assessed under the assumption that WAMPAC is used as part of a special protection scheme.

Relevant Vulnerabilities:

- Weak network security architecture allowing unauthorized access to the network components,
- No security monitoring on the WAMPAC network,
- WAMPAC network accessible with weak or no credentials.

Impact:

- All impacts presented in Table 1, as potentially caused by altered measurements or loss of data, for Special Protection and Control applications.

Potential Mitigations:

- *Restrict network access*,
- *Verify correct operation* by using redundant measurements (redundant PDCs) at each substation end transmitted through an independent communication network to double-check the transmitted measurements,
- *Detect unauthorized access* on the substation communication links,
- *Restrict network access* on the substation communication links,
- *Restrict network access* to throttle network traffic, using solutions such as router access control lists (ACLs) and firewalls,
- *Require intrusion detection and prevention*,
- *Test before install* of an intrusion detection system/intrusion prevention system (IDS/IPS) solution to verify that it does not compromise normal operation of the system.

Distribution Grid Management (DGM)

This section presents a set of failure scenarios for the Distribution Grid Management (DGM) domain. DGM "focuses on maximizing performance of feeders, transformers, and other components of networked distribution systems and integrating with transmission systems and customer operations. As smart grid capabilities, such as advanced metering infrastructure (AMI) and demand response, are developed, and as large numbers of distributed energy resources and plug-in electric vehicles (PEVs) are deployed, the automation of distribution systems becomes increasingly more important to the efficient and reliable operation of the overall power system. The anticipated benefits of distribution grid management include increased reliability, reductions in peak loads, and improved capabilities for managing distributed sources of renewable energy".

DGM.1 Wireless Signals are Jammed to Disrupt Monitoring and Control

Description: A threat agent uses a wireless signal jammer to disrupt wireless communications channels used to monitor and control distribution systems and substations. Examples are wireless local area network (LAN) communications for inter-substation differential protection, wireless communications between a distribution management system (DMS) and static VAR compensators (SVC), and communications to wireless monitoring equipment.

Relevant Vulnerabilities:

- Physical radio frequency (RF) communications are subject to deliberate jamming since few radio systems outside of the military have anti-jamming capability. Sustained jamming is less effective than intermittent jamming with the latter potentially causing the system to execute inappropriate or out of order commands,
- Wireless radio signals propagate through the air and are naturally easier to intercept and influence.

Impact:

- Reduced situational awareness and impaired ability to react to fluctuations in load and apply controlled remedies such as switching capacitor banks and triggering voltage regulators. This could cause voltage adjustment inefficiencies resulting in voltage sags and swells that can trigger unwanted over and under voltage trips on feeders or in substations,
- The uncoordinated capacitor banks due to loss of communications could conflict with substation load tap changer (LTC) actions, causing “hunting” or other inefficient actions that increase utility power losses and premature transformer failures,
- Extreme or long-duration voltage and frequency instability can damage customer or utility equipment,
- Disruption in wireless communications between pilot protection relays can impede differential protection schemes, possibly leading to equipment damage in substations or feeders during fault conditions.

Potential Mitigations:

- *Require spread-spectrum radios*, with channel-hopping or switch to alternate communication paths. Examples include:
    - Switching from licensed band(s) to unlicensed band(s),
    - Switching from unlicensed band(s) to licensed band(s),
    - Transition from RF to fiber or copper land-lines,
    - Transition from RF to dialup (possibly with degraded performance),
- *Require redundancy* in communications channels when the wireless channel is no longer available,
- *Require safe mode* in feeder devices such as capacitor banks and voltage regulators to have default states that rely on local electrical conditions if communications are lost,
- *Require redundancy* via selected AMI meters or alternative devices that provide redundant monitoring information that is out-of-band of compromised communications.

DGM.3 Malicious Code Injected into Substation Equipment via Physical Access

Description: A threat agent injects malicious code into substation equipment through physical access of engineering serial ports or by memory update devices such as USB memory sticks, Secure Digital (SD) cards or Compact Flash (CF) cards. Examples of target equipment

include communications concentrators, remote terminal units (RTUs), and protection relays. Malicious code could change device settings for purposes of rendering equipment inoperable, data gathering, denial of service, or misconfiguration.

Relevant Vulnerabilities:

- Lack of access control and authentication mechanisms to engineering and console ports of substation equipment,
- Lack of software and information integrity mechanisms,
- Physical security controls are inadequate and easily subverted,
- Unused engineering and console ports are not disabled.

Impact:

- Substation components could be modified to fail detection and clearing of bus and feeder faults (although these can be managed by reclosers which are not necessarily in the substation). These faults could lead to destruction of electrical grid equipment,
- Substation components could be reprogrammed to disallow feeder sectionalizing or service restoration via SCADA. However, these are frequently done manually,
- Modification of devices controlling VOLT/VAR equipment, including load tap changers, SVCs, automatic voltage regulators, and synchronous condensers, could prevent direct voltage control leading to potential customer equipment damage, over/under voltage trips, or additional power losses,
- Equipment firmware changes may create the need for equipment servicing that can be costly and time consuming,
- Possible lack of monitoring capabilities reduces situational awareness, inhibits a utility's ability to react proactively, and could increase the number and duration of failures.

Potential Mitigations:

- *Restrict device access* (both physical and logical) to protective relays and other critical devices,
- *Check software execution integrity* of software in substation equipment, since software may be compromised when loaded for execution,
- *Configure for least functionality* by disabling unused console and engineering ports on intelligent electronic devices (IEDs),
- *Create audit log* of substation actions,
- *Generate alarms* for any serious anomalies, such as connection changes and device configuration changes in substations,
- *Restrict physical access* to substation using, for example, card swipes, pin codes, etc.,
- *Require video surveillance* of the human interfaces to the DGM equipment,
- *Restrict access* to engineering functions,

- *Maintain latest firmware* for substation equipment,
- *Maintain patches* for substation equipment,
- *Restrict port access* of device ports on substation equipment.

DGM.4 Malicious Code Injected into Substation Equipment via Remote Access

Description: A threat agent uploads malicious code into substation equipment via remote engineering access, either through an IP network wide area network (WAN) or dialup to a line-sharing switch (LSS). Examples of target equipment include communication concentrators, RTUs, and protection relays. Connections with peers are another avenue of attack. Some distribution substations, particularly in urban environments, use Bluetooth or ZigBee for access to reduce the need for crews to install underground cables. Malicious code could change device settings for purposes of rendering equipment inoperable, data gathering, denial of service, or misconfiguration.

Relevant Vulnerabilities:

- Poor access controls on remote substation WAN communications,
- Cyber security countermeasures or policies for WAN communications are insufficient or outdated,
- Patch management on cyber and communication equipment is inadequate and slow to provide updates,
- Dialup LSS or wireless access negates any physical access controls.

Impact:

- Substation components could be modified to fail detection and clearing of bus and feeder faults (although these can be managed by reclosers which are not necessarily in the substation). These faults could lead to destruction of electrical grid equipment,
- Substation components could be reprogrammed to disallow feeder sectionalizing or service restoration via SCADA. However, these are frequently done manually,
- Equipment firmware changes may create the need for equipment servicing that can be costly and time consuming,
- Possible lack of monitoring capabilities reduces situational awareness, inhibits a utility's ability to react proactively, and could increase the number and duration of failures.

Potential Mitigations:

- *Restrict remote access* to protective relays and other critical devices,
- *Create audit log* of substation actions,
- *Generate alarms* for any serious anomalies, such as connection changes and device configuration changes,
- *Maintain patches* for all substation communication equipment,

- *Maintain anti-virus* on substation equipment,
- *Require application whitelisting* on substation equipment,
- *Authenticate users* in the substation network (possibly two factor authentication),
- *Require VPNs* in the substation network.

DGM.5 Remote Access Used to Compromise DMS

Description: A threat agent compromises distribution management system (DMS) functionality through remote access modification of executable programs and libraries, rendering the DMS inoperable.

Relevant Vulnerabilities:

- Inadequate access controls for modifying software files,
- Outdated security patches,
- Inadequate protections for remote access to DMS systems,
- Weak passwords.

Impact:

- Reduced situational awareness and impaired ability to react to fluctuations in load and apply controlled remedies,
- Possible increase in outage durations,
- Decrease in operational efficiency and increase in utility power losses,
- Decrease in service reliability,
- Decrease in customer satisfaction.

Potential Mitigations:

- *Maintain patches* on DMS systems,
- *Create audit log* of all program changes and updates,
- *Detect abnormal behavior* of voltage on feeders via selected AMI meters or alternative devices that provide redundant information,
- *Check software file integrity* (digital signatures) for driver installation,
- *Require intrusion detection and prevention* on DMS hosts,
- *Implement configuration management* for all software updates including patches and firmware updates,
- *Maintain anti-virus* on DMS hosts,
- *Require application whitelisting on DMS hosts,*
- *Require backup* of DMS when primary DMS is inoperable.

DGM.6 Spoofed Substation Field Devices Influence Automated Responses

Description: Threat agent spoofs data inputs from field devices at substations and below to cause the DMS to report a false system state. This could cause operator or automated responses that are inappropriate.

Relevant Vulnerabilities:

- Communications between field devices and the DMS are not authenticated,
- Communications channels are unencrypted.

Impact:

- Inappropriate fault-clearing actions, feeder sectionalization, and overuse of remedial capabilities leading to loss of power to customers,
- Volt/VAR controls are wrongly applied or adjusted based on erroneous data, possibly triggering over/under voltage trips,
- Collected meter data is incorrect or inaccurate, leading to possible loss in revenue.

Potential Mitigations:

- *Authenticate devices* in communication from field devices to control centers,
- *Detect unusual patterns* of inputs that could indicate they are not trustworthy, by comparing inputs to each other and previous inputs,
- *Restrict communication access*,
- *Encrypt communication paths*.

DGM.9 Weakened Security during Disaster enables DGM Compromise

Description: A threat agent could take advantage of the confusion, lack of security, and hasty reconstitution of the distribution grid after a disaster. For example, a threat agent could delay the recovery effort by leveraging temporary communications with low security to access DMS to switch breakers. Likewise this objective could be achieved by subverting weak physical security at substations (due to damage or communication outages) to access engineering or console ports or relays to change settings and render them inoperable. Further, the interception of temporary communications with low security might support reconnaissance of high priority vulnerabilities to aid in future attacks.

Relevant Vulnerabilities:

- The disregard of security controls due to the objective to restore functionality and service as quickly as possible,
- Oversights in security due to confusion or lack of proper policies and procedures for emergency response.

Impact:

- Delay, damage, disruption, or denial of the recovery effort,
- Damage, disruption, or destruction of a system or components long after the disaster recovery,

- Theft of historian, configuration, or customer information that could support future attacks.

Potential Mitigations:

- *Implement configuration management* of the DGM systems before and after disasters,
- *Define policy* for emergency response that ensure security during a recovery effort,
- *Prioritize recovery activities* for physical security including personnel authentication and access control during the recovery effort,
- *Review recovery response* after the disaster to verify repairs, configurations, and changes are correct,
- *Verify correct operation* on the DGM systems before deployment.

DGM.11 Threat Agent Triggers Blackout via Remote Access to Distribution System

Description: A threat agent performs reconnaissance of utility communications, electrical infrastructure, and ancillary systems to identify critical feeders and electrical equipment. Threat agent gains access to selected elements of the utility DMS system - which includes all distribution automation systems and equipment in control rooms, substations, and on pole tops - via remote connections. After gaining the required access, the threat agent manufactures an artificial cascade through sequential tripping of select critical feeders and components, causing automated tripping of generation sources due to power and voltage fluctuations. A blackout of varying degree and potential equipment damage ensues. The remote connections might be established using a variety of methods or combination of methods. These include, but are not limited to, using a lost, stolen, or acquired utility linemen's laptop to access the DMS directly; compromising an active remote maintenance connection used for vendor DMS application maintenance; taking advantage of an accidental bridged connection to the internet due to DMS misconfiguration; or subverting distribution control communications directly.

Relevant Vulnerabilities:

- Inadequate protection of linemen and maintenance personnel company laptops used for remote connections from loss, theft, or abuse, and from misuse when not under control of authorized individuals,
- Lack of strong authentication on company computers,
- Weak passwords,
- Weak protection of proprietary utility documents and information,
- Inadequate measures to prevent and detect human error in a data center configuration (e.g., Ethernet cable plugged into wrong port),
- Allowing remote access for vendors to do application maintenance and troubleshooting,
- Unencrypted distribution control communications,
- Distribution networks are more radial in nature than meshed, making network reconfiguration to restore power more difficult.

Impact:

- Loss of customer power,
- Disclosure of proprietary utility documents or information,
- Possible customer and utility equipment damage.

Potential Mitigations:

- *Require strong passwords* with complexity requirements for company devices and systems,
- *Train personnel* to protect company information and documents from unauthorized disclosure,
- *Define policy* on handling sensitive information. This includes substation one-line diagrams, equipment information, communication architectures, protection schemes, load profiles, etc.,
- *Train personnel* (operations and maintenance employees) to handle and protect company computing devices securely, incorporating two-factor authentication, requirements on storing devices, and reporting instructions in cases of loss or theft,
- *Create audit log* of all changes in human machine interface (HMI) control actions,
- *Generate alerts* for all changes for all changes in HMI control actions,
- *Restrict remote access* of vendor connections (e.g. physically disconnect remote connections when not in use),
- *Encrypt communication paths* for distribution control communications,
- *Require 2-person rule* for to verify correct DMS configuration,
- *Implement configuration management* for configuration documents,
- *Isolate networks* (distribution control networks) by segmenting the distribution control network itself.

DGM.12 Hijacked Substation Wireless Damages Substation Equipment

Description: A threat agent carries out a man in the middle attack, hijacking the wireless communications channel to a substation transformer. The threat agent uses this capability to disable transformer cooling fans and overheat the device. Depending on the transformer and its controller, this could be done through a direct command or by drastically increasing oil temperature setpoints. Many transformers are also custom built and have long lead times for replacement or repair.

Relevant Vulnerabilities:

- Poor or no authentication between the transformer and the substation controller,
- Wireless communications are unencrypted,

- Long lead times to repair or replace custom built transformers.

Impact:

- Loss of customer power,
- Damage to critical substation equipment,
- Monetary loss.

Potential Mitigations:

- *Authenticate users* of wireless communications,
- *Encrypt communications paths* for wireless communications,
- *Design for trust* by replacing wireless communications with wired ones,
- *Create audit log* of all changes in control functions and set points,
- *Generate alerts* for unusual changes in control functions and set points.

DGM.14 Power loss due to lack of serial communication authentication

Description: Serial communications to substations over phone lines often lack authentication of field devices, such as RTUs. This might allow a threat agent to directly dial into modems attached to RTU equipment by war dialing city phone numbers or company phone extensions. Such techniques could allow a threat agent to send breaker trip commands to substation relays and disconnect feeders.

Relevant Vulnerabilities:

- Lack of authentication on serial communications to substations,
- No passwords or default passwords on substation relays and RTU,
- Using public communication channels without authentication or encryption.

Impact:

- Loss of customer power,
- Monetary loss,
- Negative publicity.

Potential Mitigations:

- *Authenticate users* of serial communications using strong passwords,
- *Encrypt communication paths* for serial communications using low latency encryption devices,
- *Design for trust* and migrate serial communications to field devices from public phone lines to private communication channels.

DGM.16 Threat agent compromises serial control link to substation

Description: The Telco/Commercial Service Provider (CSP) provides communications capability between the utility's substation and headend/control center. Both wired and wireless based interfaces may be involved depending on the particular utility standards and site-specific constraints. Wired-based communication links can be analog or digital leased lines, while wireless interfaces are typically radio, cellular or even satellite based. To establish the Telco/CSP end-to-end communications, a point of demarcation (Demarc) is provided where the local utility owned communications infrastructure interfaces the telco owned network infrastructure (Figure 5). A knowledgeable threat agent can compromise the serial communications at the Demarc by intercepting and selectively modifying communicated data to masquerade as a user (man-in-the-middle) or replay attack, in which the threat agent captures control messages and subsequent retransmission with the intent of producing an unauthorized effect. This can potentially compromise both real-time (sometimes referred to as operational) traffic as well as non-real-time (sometimes referred to as non-operational) traffic. In the context of real-time data exchanges, the substation gateway or RTU in the substation or the SCADA Front End Processor (FEP) at the headend can be affected by manipulating command and control messages in the direction of the substation or information messages in the direction of the head end. In the case of non-operational data exchanges, IED settings can be potentially manipulated.

Relevant vulnerabilities:

- Physical security control procedures in the utility or Telco/CSP
- implementation permit access of threat agent to the demarc or within the service providers network CSU/DSU,
- Inadequate authentication and access control to substation gateway/RTU or SCADA FEP,
- Inadequate or nonexistent tamper detection at the Demarc,
- The communication protocol does not detect or alert when information or commands come from an unauthorized source,
- Serial link does not protect against capture and reading of messages by unauthorized individuals.

Impact:

- Loss of customer power, possibly to critical customers (e.g., hospital),
- Potential customer and utility equipment damage,
- Financial loss associated with any equipment damage or restoration to normal operations,
- Increase in public safety concerns (e.g., loss of heating or cooling on extremely cold or hot days),
- Negative impact on customer service due to increase in calls and complaints,
- Damage to goodwill toward utility.

Mitigation:

- *Implement approved cryptographic algorithms* to protect the integrity of communications and the cryptographic keys,
- *Implement approved key management* to protect the cryptographic keys,
- *Detect unusual patterns* of energy usage on Generation Automation (all utilities have some type of revenue protection scheme, but these may not be adequate),
- *Detect unauthorized access* in network traffic between substation and headend,
- *Require authentication* on all data exchanges,
- *Encrypt communication paths* for serial messaging by using bump-in-the-wire solution,
- *Require multi-factor authentication* by Telco/CSP to the device containing CSU/DSU units through SLA.
- *Require tamper detection and response* by Telco/CSP for the Demarc through SLA.
- *Restrict physical access* by implementing personnel security control procedures.

Generic

This section presents a set of failure scenarios which are generic. Particular cases of these generic failure scenarios can be found among the failure scenarios listed for specific domains in the previous sections. They are discussed in their generic form here to enable the reader to recognize additional instances of these types of failure scenarios.

Generic.1 Malicious and Non-malicious Insiders Pose Range of Threats

Description: Authorized personnel - who may be operators, engineering staff or administrators, become active threat agents with legitimate access to IT, field systems, and/or control networks.

Relevant Vulnerabilities:

- Inadequate or no separation of duties,
- Security-relevant and operationally critical functionality is not monitored,
- Lack of situational awareness when privileges are elevated for access to security-relevant or operationally critical functions,
- Either inadequate, or lack of, incident response processes to decrease response time when incidents occur.

Impact:

- Authorized personnel with legitimate access can inflict significant damage on a system either intentionally or by mistake. The impact for this scenario could range from a minor system being offline to a widespread outage of unknown duration.

Potential Mitigations:

- *Require separation of duty*,
- *Use RBAC* to limit access,

- *Detect abnormal behavior* including out-of-policy behavior by authorized users in control networks through protection mechanisms and situational awareness (SIEM, IDS, firewalls, logging, and monitoring),
- *Define procedures* concerning access to security-relevant and operationally critical functionality.

Generic.2 Inadequate Network Segregation Enables Access for Threat Agents

Description: A threat agent compromises an asset that has access to the Internet via the "business" network. The asset on the business network also has access to a control system asset or network. The compromise of the business network asset provides a pivot point for the threat agent to gain control of a control system asset or network.

Relevant Vulnerabilities:

- Lack of or inadequate network segregation such as using virtual local area networks (VLANs) for security or using the same networks for business operations and control systems,
- Lack of situational awareness to show remote command and control of a business asset has been obtained. Situational awareness mechanisms include observing and responding to anti-virus, firewall, IDS, IPS, and system-level alerts,
- Inadequate monitoring of traffic to and from the business operations network to the Internet to notice when an incident is occurring,
- No security controls between the business and control systems network and treating the business network as a "trusted" entity.

Impact:

- The impact for this scenario could range from a minor system being offline to a widespread outage of unknown duration.

Potential Mitigations:

- *Isolate networks* that host business systems from those that host control systems,
- *Generate alerts* using a SIEM and monitor alerts according to the risks associated,
- *Isolate networks* with a defensible, defense in depth, network architecture which includes a demilitarized zone (DMZ),
- *Enforce restrictive firewall rules*,
- *Require intrusion detection and prevention*,
- *Train personnel* to monitor traffic to and from the Internet and to recognize when an incident is occurring,
- *Define incident response plan* to reduce response time when incidents do occur,
- *Define contingency plan* as part of the incident response plan, to maintain adequate resiliency in high-priority control systems.

Generic.3 Portable Media Enables Access Despite Network Controls

Description: A threat agent introduces counterfeit firmware or software, a virus, or malware via removable media to obtain partial or total control of a device or networked system.

Relevant Vulnerabilities:

- Unrestricted access to interfaces such as USB, Firewire, or serial ports that allows the unrestricted ability to load software or firmware to devices.

Impact:

- The impact for this scenario could range from a minor system being offline to a widespread outage of unknown duration.

Potential Mitigations:

- *Configure for least functionality* by permanently physically disabling unnecessary interfaces with epoxy or other methods, or physically removing them,
- *Configure for least functionality* by using software controls or other non-physical methods to disable unnecessary interfaces on equipment,
- *Verify settings* on equipment before the equipment is installed in the field,
- *Test before install* of equipment in the field,
- *Vulnerability scan before install* of equipment in the field,
- *Require periodic walk-downs* of equipment to help ensure there are not any new unauthorized devices connected,
- *Define policy* outlining acceptable and unacceptable use of portable computing devices in a business/corporate local area network (LAN) environment and a control LAN environment,
- *Train personnel* under a user awareness training program that includes portable media guidelines

ACRONYMS

ACL	Access Control List
AMI	Advanced Metering Infrastructure
CF	Compact Flash
CIS	Customer Information System
CSP	Commercial Service Provider
DER	Distributed Energy Resources
DERMS	Distributed Energy Resources Management System
DGM	Distribution Grid Management
DMS	Distribution Management System
DMZ	Demilitarized Zone
DR	Demand Response
FDEMS	Field DER Energy Management System
FEP	Front End Processor
HMI	Human-Machine Interface
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
IPS	Intrusion Prevention System
LAN	Local Area Network
LSS	Line Sharing Switch
LTC	Load Tap Charger
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NESCOR	National Electric Sector Cybersecurity Organization Resource
PDC	Phasor Data Concentrator
PMU	Phasor Measurement Unit
RBAC	Role-Based Access Control
RF	Radio Frequency
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SD	Secure Digital
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SVC	Static VAR Compensators
USB	Universal Serial Bus

VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAMPAC	Wide Area Monitoring, Protection, and Control
WAN	Wide Area Network

DGM.16 Figure

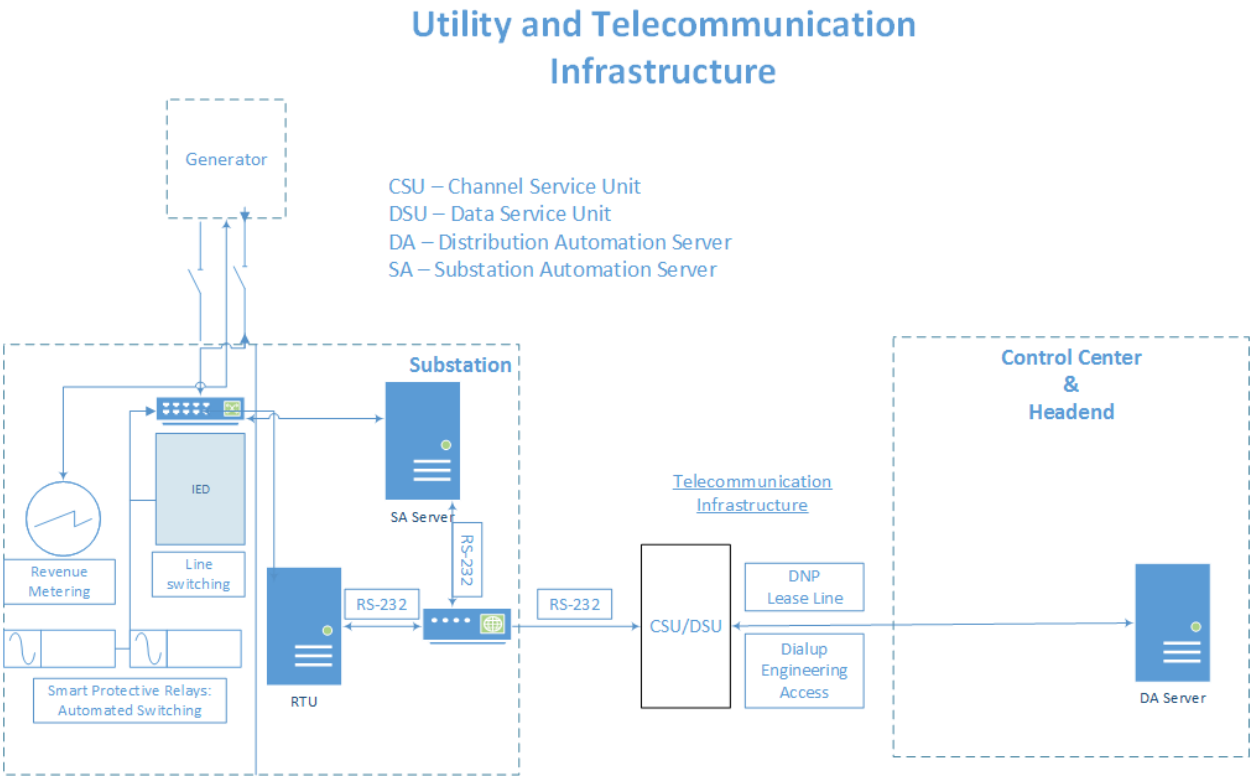


Figure 5 Threat agent compromises serial control link to substation (DGM.16)

Appendix B: National Institute of Standards and Technology Interagency Report (NISTIR) 7628, Guidelines for Smart Grid Cyber Security

Included are the logical interface categories (LICs) and diagrams from the NISTIR 7628, Version 1.0, August 2010 that are applicable to PBCONF. An initial set of revisions have been made to concentrate on substation remote access – the focus of the PBCONF project.

Logical Architecture and Interfaces of the Smart Grid

Included is a logical reference model of the smart grid, including all the major domains—service providers, customer, transmission, distribution, bulk generation, markets, and operations—that are part of the NIST conceptual model. Figure 6 presents the logical reference model and represents a composite high level view of smart grid domains and actors. A smart grid domain is a high-level grouping of organizations, buildings, individuals, systems, devices, or other *actors* with similar objectives and relying on—or participating in—similar types of applications.

Communications among actors in the same domain may have similar characteristics and requirements. Domains may contain subdomains. An *actor* is a device, computer system, software program, or the individual or organization that participates in the smart grid. Actors have the capability to make decisions and to exchange information with other actors. Organizations may have actors in more than one domain. The actors illustrated in this case are representative examples and do not encompass all the actors in the smart grid. Each of the actors may exist in several different varieties and may contain many other actors within them. Table 2 complements the logical reference model diagram () with a description of the actors associated with the logical reference model.

The format for the reference number for each logical interface is U99, where U stands for universal and 99 is the interface number. The reference number is the same on the individual application area diagrams and the logical reference model. This logical reference model focuses on a short-term view (1–3 years) of the proposed smart grid and is only a sample representation.

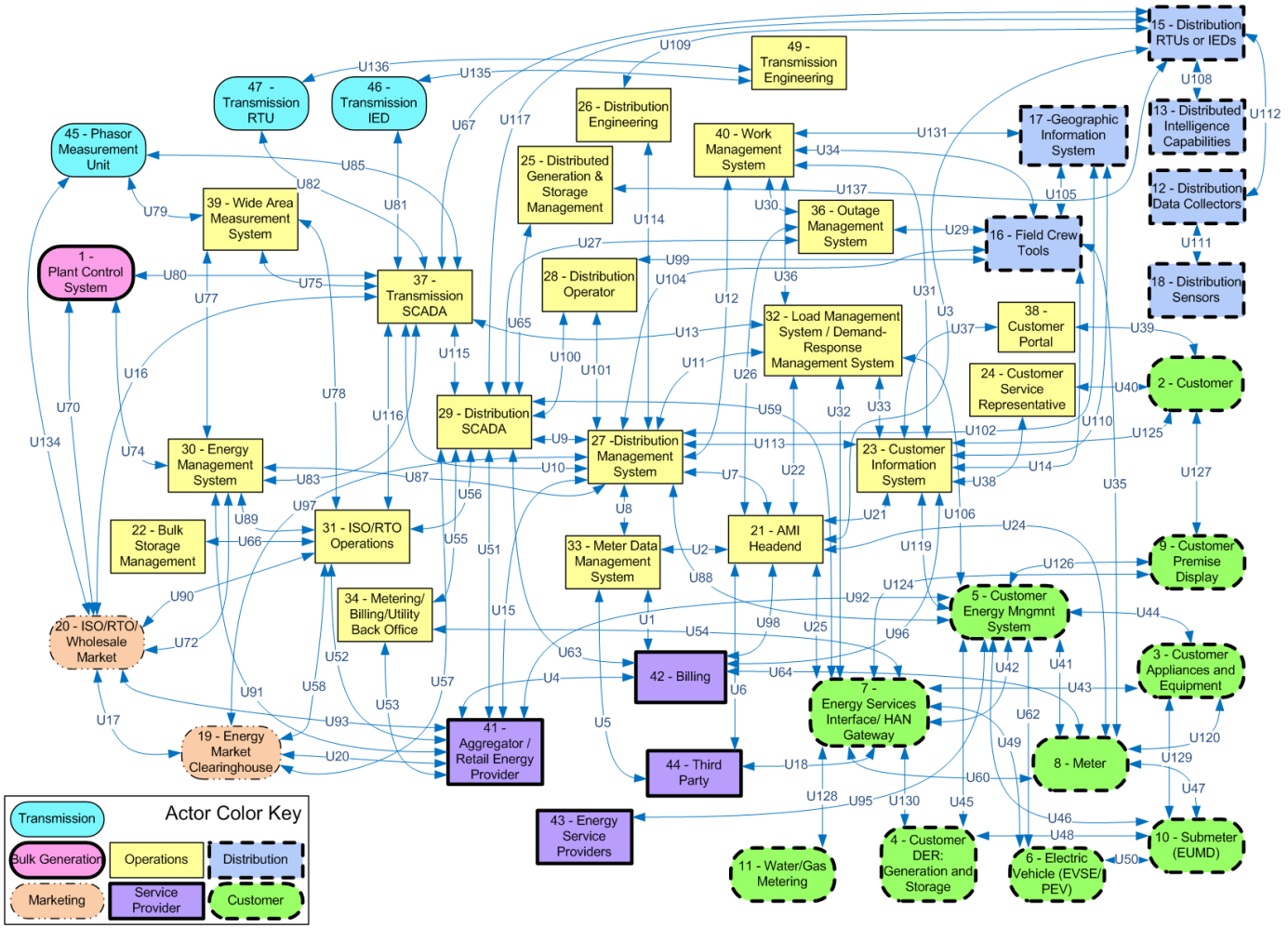


Figure 6 Logical Reference Model

Table 2 Actor Descriptions for the Logical Reference Model

Actor Number	Domain	Actor	Acronym	Description
5	Customer	Customer Energy Management System	EMS	An application service or device that communicates with devices in the home. The application service or device may have interfaces to the meter to read usage data or to the operations domain to get pricing or other information to make automated or manual decisions to control energy consumption more efficiently. The EMS may be a utility subscription service, a 3rd party offered service, a consumer specified policy, a consumer owned device, or a manual control by the utility or consumer.
7	Customer	Home Area Network Gateway	HAN Gateway	An interface between the distribution, operations, service provider, and customer domains and the devices within the customer domain.
12	Distribution	Distribution Data Collector		A data concentrator bringing data from multiple sources and putting it into different form factors.
15	Distribution	Distribution Remote Terminal Unit/Intelligent Electronic Device	RTUs or IEDs	Receive data from sensors and power equipment, and can issue control commands, such as tripping circuit breakers if they sense voltage, current, or frequency anomalies, or raise/lower voltage levels in order to maintain the desired level.
16	Distribution	Field Crew Tools		A field engineering and maintenance tool set that includes any mobile computing and hand-held devices.
17	Distribution	Geographic Information System	GIS	A spatial asset management system that provides utilities with asset information and network connectivity for advanced applications.

Actor Number	Domain	Actor	Acronym	Description
25	Operations	Distributed Generation and Storage Management		Distributed generation is also referred to as on-site generation, dispersed generation, embedded generation, decentralized generation, decentralized energy or distributed energy. This process generates electricity from many small energy sources for use or storage on dispersed, small devices or systems. This approach reduces the amount of energy lost in transmitting electricity because the electricity is generated very near where it is used, perhaps even in the same building. [3]
26	Operations	Distribution Engineering		A technical function of planning or managing the design or upgrade of the distribution system. For example' the addition of new customers, the build out for new load, the configuration and/or capital investments for improving system reliability.
27	Operations	Distribution Management Systems	DMS	A suite of application software that supports electric system operations. Example applications include topology processor, on-line three-phase unbalanced distribution power flow, contingency analysis, study mode analysis, switch order management, short-circuit analysis, volt/VAR management, and loss analysis. These applications provide operations staff and engineering personnel additional information and tools to help accomplish their objectives.
28	Operations	Distribution Operator		Person operating the distribution system.
29	Operations	Distribution Supervisory Control and Data Acquisition	SCADA	Transmits individual device status, manages energy consumption by controlling compliant devices, and allows operators to directly control power system equipment.

[3] Description summarized from http://en.wikipedia.org/wiki/Distributed_generation.

Actor Number	Domain	Actor	Acronym	Description
32	Operations	Load Management Systems/Demand Response Management System	LMS/DRMS	An LMS issues load management commands to appliances or equipment at customer locations in order to decrease load during peak or emergency situations. The DRMS issues pricing or other signals to appliances and equipment at customer locations in order to request customers (or their pre-programmed systems) to decrease or increase their loads in response to the signals.
33	Operations	Meter Data Management System	MDMS	System that stores meter data (e.g. energy usage, energy generation, meter logs, meter test results) and makes data available to authorized systems. This system is a component of the customer communication system. This may also be referred to as a 'billing meter'.
34	Operations	Metering/Billing/Utility Back Office		Back office utility systems for metering and billing.
36	Operations	Outage Management System	OMS	An OMS is a computer system used by operators of electric distribution systems to assist in outage identification and restoration of power. Major functions usually found in an OMS include: • Listing all customers who have outages. • Prediction of location of fuse or breaker that opened upon failure. • Prioritizing restoration efforts and managing resources based upon criteria such as location of emergency facilities, size of outages, and duration of outages. • Providing information on extent of outages and number of customers impacted to management, media and regulators. • Estimation of restoration time. • Management of crews assisting in restoration. • Calculation of crews required for restoration.

Actor Number	Domain	Actor	Acronym	Description
37	Operations	Transmission SCADA		Transmits individual device status, manages energy consumption by controlling compliant devices, and allowing operators to directly control power system equipment.
38	Operations	Customer Portal		A computer or service that makes available Web pages. Typical services may include: customer can viewing of their energy and cost information online, enrollment in prepayment electric services and enablement of third party monitoring and control of customer equipment.
39	Operations	Wide Area Measurement System	WAMS	Communication system that monitors all phase measurements and substation equipment over a large geographical base that can use visual modeling and other techniques to provide system information to power system operators.
40	Operations	Work Management System	WMS	A system that provides project details and schedules for work crews to construct and maintain the power system infrastructure.
42	Service Provider	Billing		Process of generating an invoice to recover sales price from the customer.
43	Service Provider	Energy Service Provider	ESP	Provides retail electricity, natural gas, and clean energy options, along with energy efficiency products and services.
44	Service Provider	Third Party		A third party providing a critical business function outside of the utility.
45	Transmission	Phasor Measurement Unit	PMU	Measures the electrical waves on an electricity grid to determine the health of the system.

Actor Number	Domain	Actor	Acronym	Description
46	Transmission	Transmission IED		IEDs receive data from sensors and power equipment and can issue control commands, such as tripping circuit breakers if they sense voltage, current, or frequency anomalies, or raise/lower voltage levels in order to maintain the desired level. A device that sends data to a data concentrator for potential reformatting.
47	Transmission	Transmission RTU		RTUs pass status and measurement information from a substation or feeder equipment to a SCADA system and transmit control commands from the SCADA system to the field equipment.
48[4]	Operations	Security/Network/System Management		Security/Network/System management devices that monitor and configure the security, network, and system devices.
49	Transmission	Transmission Engineering		Equipment designed for more than 345,000 volts between conductors.

[4] Actor 48 is included in logical interface category 22 for security. It is not included in the logical reference model.

1.1 Logical Interface Categories

Each logical interface in the logical reference model was allocated to a logical interface category. This was done because many of the individual logical interfaces are similar in their security-related characteristics and can, therefore, be categorized together as a means to simplify the identification of the appropriate security requirements. These security-related logical interface categories were defined based on attributes that could affect the security requirements.

Table 3 Logical Interfaces by Category

Logical Interface Category	Logical Interfaces
1. Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints, for example: • Between transmission SCADA and substation equipment • Between distribution SCADA and high priority substation and pole-top equipment • Between SCADA and DCS within a power plant	U67, U79, U81, U82, U85, U102, U117
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: • Between transmission SCADA and substation automation systems	U67, U79, U81, U82, U85, U102, U117
10. Interface between control systems and non-control/corporate systems, for example: • Between a Work Management System and a Geographic Information System	U12, U30, U36, U59, U75, U106, U114, U131, U135, U136
17. Interface between systems and mobile field crew laptops/equipment, for example: • Between field crews and GIS • Between field crews and substation equipment	U29, U34, U99, U104, U105
20. Interface between engineering/maintenance systems and control equipment, for example: • Between engineering and substation relaying equipment for relay settings • Between engineering and pole-top equipment for maintenance • Within power plants	U109, U135, U136, U137

Logical Interface Category	Logical Interfaces
21. Interface between control systems and their vendors for standard maintenance and service, for example: • Between SCADA system and its vendor	U5
22. Interface between security/network/system management consoles and all networks and systems, for example: • Between a security console and network routers, firewalls, computer systems, and network nodes	U133 (includes interfaces to actors 17-Geographic Information System, 38 – Customer Portal, 23 – Customer Information System, 21 – AMI Headend, 42 – Billing, 44 – Third Party, 43 – Energy Service Provider, 34 – Metering/Billing/Utility Back Office)

1.1.1 Logical Interface Categories 1and 3

Logical Interface Category 1: Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints

Logical Interface Category 3: Interface between control systems and equipment with high availability, without compute or bandwidth constraints

Logical interface categories 1 and 3 cover communications between control systems (typically centralized applications such as a SCADA master station) and equipment as well as communications between equipment. The equipment is categorized with or without high availability. The interface communication channel is categorized with or without computational and/or bandwidth constraints. All activities involved with logical interface categories 1 and 3 are typically machine-to-machine actions. Furthermore, communication modes and types are similar between logical interface categories 1 and 3 and are defined as follows:

Interface Data Communication Mode

- Near Real Time Frequency Monitoring Mode (ms, subcycle based on a 60 Hz system) (may or may not include control action communication)
- High Frequency Monitoring Mode (2s – 59s scan rates)
- Low Frequency Monitoring Mode (scan/update rates in excess of 1 min, file transfers)

Interface Data Communication Type

- Monitoring and Control Data for real time control system environment (typical measurement and control points)
- Equipment Maintenance and Analysis (numerous measurements on field equipment that is typically used for preventive maintenance and post analysis)
- Equipment Management Channel (remote maintenance of equipment)

The characteristics that vary between and distinguish each logical interface category are the availability requirements for the interface and the computational/communications constraints for the interface as follows:

Availability Requirements – Availability requirements will vary between these interfaces and are driven primarily by the power system application which the interface supports and not by the interface itself. For example, a SCADA interface to a substation or pole-top RTU may have a HIGH availability requirement in one case because it is supporting critical monitoring and switching functions or a MODERATE to LOW availability if supporting an asset monitoring application.

Communications and Computational Constraints –- Computational constraints are associated with cryptography requirements on the interface. The use of cryptography typically has high CPU needs for mathematical calculations, although it is feasible to implement cryptographic processing in peripheral hardware. Existing devices like RTUs, substation IEDs, meters, and others are typically not equipped with sufficient digital hardware to perform cryptography or other security functions.

Bandwidth constraints are associated with data volume on the interface. In this case, media is usually narrowband, limiting the volume of traffic and impacting the types of security measures that are feasible.

With these requirements and constraints, logical interface categories 1 and 3 can be defined as follows:

1. Interface between control systems and equipment with high availability and with computational and/or bandwidth constraints:

   Between transmission SCADA in support of state estimation and substation equipment for monitoring and control data using a high frequency mode;

   Between distribution SCADA in support of three phase, real time power flow and substation equipment for monitoring data using a high and low frequency mode;

   Between transmission SCADA in support of automatic generation control (AGC) and DCS within a power plant for monitoring and control data using a high frequency mode;

   Between SCADA in support of Volt/VAR control and substation equipment for monitoring and control data using a high and low frequency mode; and

   Between transmission SCADA in support of contingency analysis and substation equipment for monitoring data using high frequency mode.

3. Interface between control systems and equipment with high availability without computational and/or bandwidth constraints:

   Between transmission SCADA and substation automation systems for monitoring and control data using a high frequency mode;

   Between EMS and generation control (DCS) and RTUs for monitoring and control data using a high frequency mode;

   Between distribution SCADA and substation automation systems, substation RTUs, and pole-top devices for monitoring and control data using a high frequency mode;

   Between a PMU device and a phasor data concentrator (PDC) for monitoring data using a high frequency mode; and

   Between IEDs (peer-to-peer) for power system protection, including transfer trip signals between equipment in different substations.

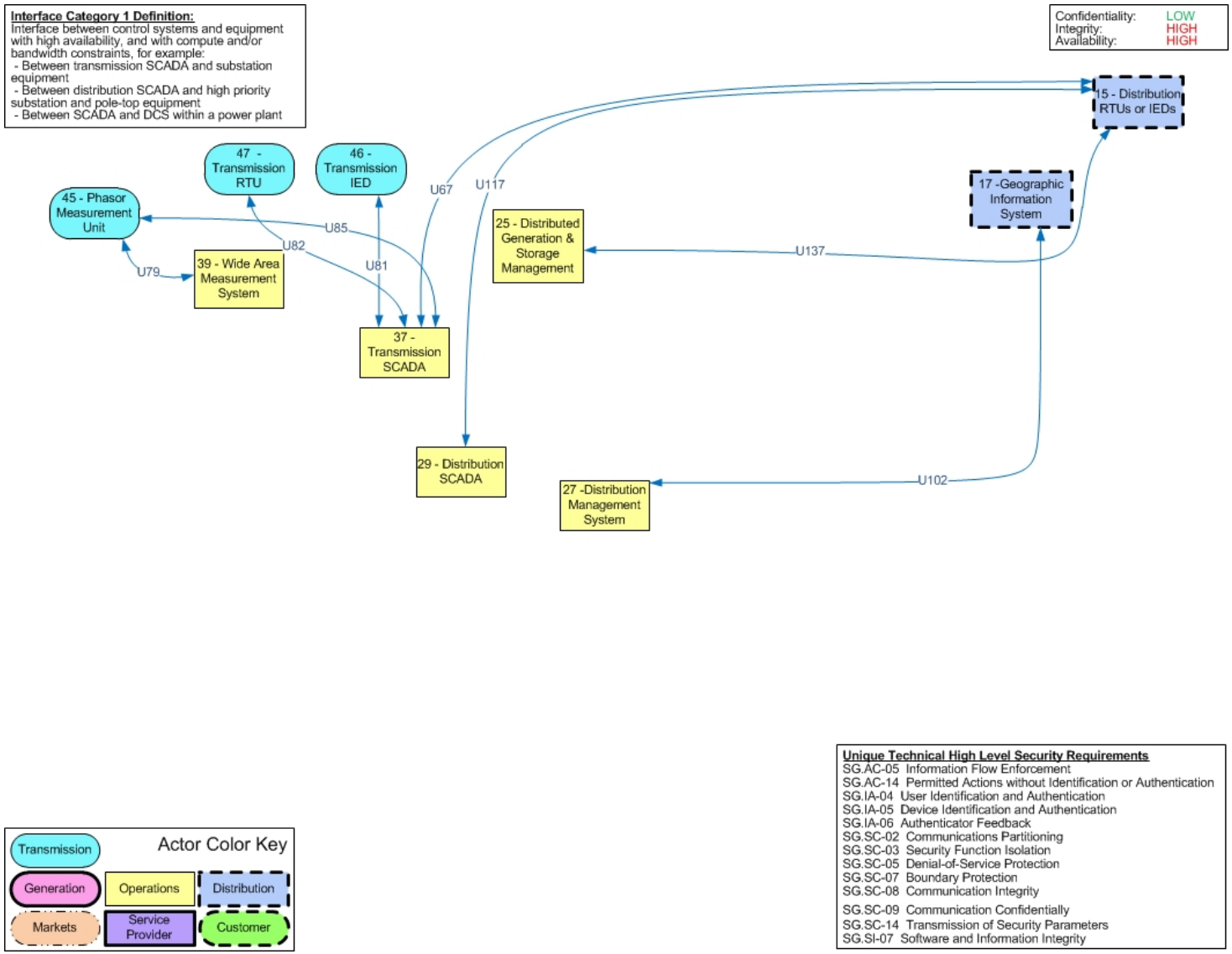


Figure 7 Logical Interface Category 1

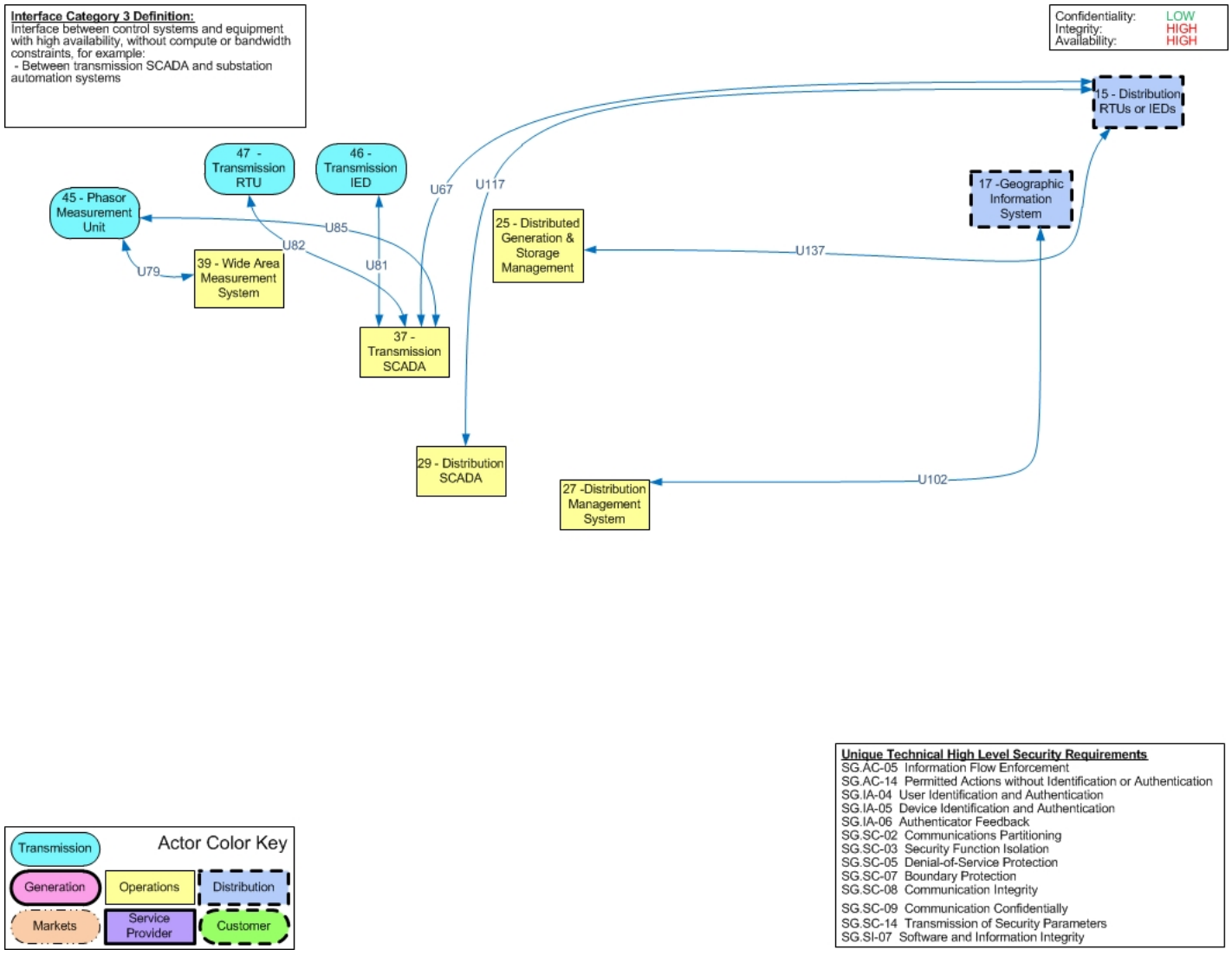


Figure 8 Logical Interface Category 3

1.1.2 Logical Interface Category 10: Interface between control systems and non-control/ corporate systems

Logical interface category 10 covers the interfaces between control systems and noncontrol/corporate systems, for example:

Between a WMS and a GIS;

Between a DMS and a CIS; and

Between an OMS and a WMS.

These interactions between control systems and noncontrol systems have the following characteristics and issues:

The primary security issue is preventing unauthorized access to sensitive control systems through noncontrol systems. As a result, integrity is the most critical security requirement.

Since control systems generally require high availability, any interfaces with noncontrol systems should ensure that interactions with these other systems do not compromise the high reliability requirement.

The interactions between these systems usually involve loosely coupled interactions with very different types of exchanges from one system to the next and from one vendor to the next.

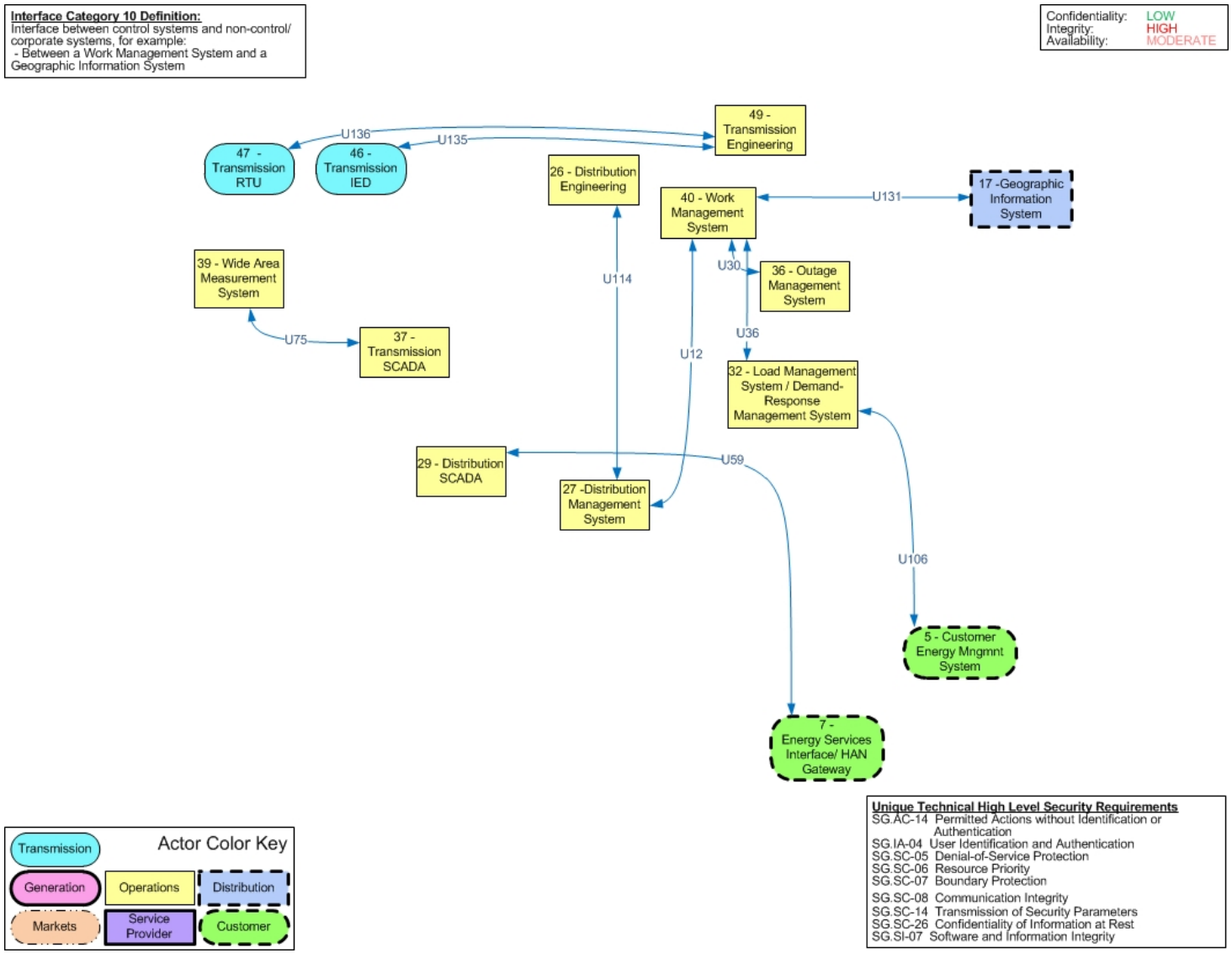


Figure 9 Logical Interface Category 10

1.1.3 Logical Interface Category 17: Interface between systems and mobile field crew laptops/equipment

Logical interface category 17 covers the interfaces between systems and mobile field crew laptops/equipment, for example:

Between field crews and a GIS;

Between field crews and CIS;

Between field crews and substation equipment;

Between field crews and OMS;

Between field crews and WMS; and

Between field crews and corporate marketing systems.

As with all other logical interface categories, only the interface security requirements are addressed, not the inherent vulnerabilities of the end equipment such as the laptop or personal digital assistant (PDA) used by the field crew.

The main activities performed on this interface include:

Retrieving maps and/or equipment location information from GIS;

Obtaining and providing substation equipment information, such as location, fault, testing, and maintenance updates;

Obtaining outage information and providing restoration information, including equipment, materials, and resource information from/to OMS; and

Obtaining project and equipment information and providing project, equipment, materials, resource, and location updates from/to WMS;

The key characteristics of this interface category are as follows:

This interface is primarily for customer service operations. The most critical needs for this interface are

- To post restoration information back to the OMS for reprediction of further outage situations.

Information exchanged between these systems is typically corporate-owned, and security is managed within the utility between the interfacing applications. Increased use of wireless technologies and external service providers adds a layer of complexity in security requirements that is addressed in all areas where multivendor services are interfaced with utility systems.

Integrity of data is clearly important in general, but since so many different types of interactions are taking place, the integrity requirements will need to be specific to the particular application. However, the integrity of revenue-grade metering data that may be collected in this manner is vital since it has a direct financial impact on all stakeholders of the loads and generation being metered.

Availability is generally not critical, as interactions are not necessary for real time. Exceptions include payment information for disconnects, restoration operations, and efficiency of resource management.

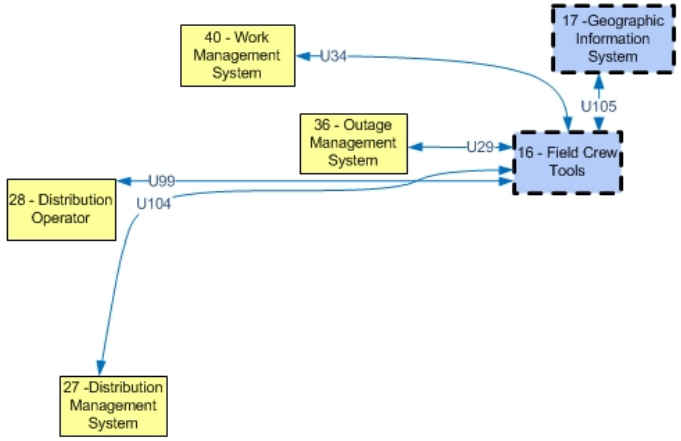
Bandwidth is not generally a concern, as most utilities have sized their communications infrastructure to meet the needs of the field applications, and most field applications have been designed for minimal transmission of data in wireless mode. However, more and more applications are being given to field crews to enhance customer service opportunities and for tracking and reporting of construction, maintenance, and outage restoration efforts. This will increase the amount of data and interaction between the corporate systems, third-party providers, and the field crews.

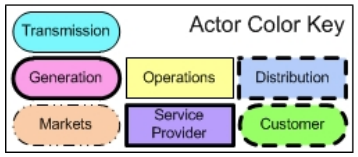
In addition, most mobile field applications are designed to transmit data as it is input, and therefore data is not transmitted when the volume of data is too large to transmit over a wireless connection or when the area does not have wireless coverage. In such cases, data is maintained on the laptop/PDA until it is reconnected to a physical network.

Note: data that is captured (e.g., metering data, local device passwords, security parameters) must be protected at the appropriate level.

Interface Category 17 Definition:
Interface between systems and mobile field crew laptops/equipment, for example:
- Between field crews and GIS
- Between field crews and substation equipment

Confidentiality: LOW
Integrity: HIGH
Availability: MODERATE





Unique Technical High Level Security Requirements
SG.AC-11 Concurrent Session Control
SG.AC-12 Session Lock
SG.AC-13 Remote Session Termination
SG.AC-14 Permitted Actions without Identification or Authentication
SG.IA-04 User Identification and Authentication
SG.IA-05 Device Identification and Authentication
SG.SC-02 Communications Partitioning
SG.SI-07 Software and Information Integrity

Figure 10 Logical Interface Category 17

1.1.4 Logical Interface Category 20: Interface between engineering/ maintenance systems and control equipment

Logical interface category 20 covers the interfaces between engineering/maintenance systems and control equipment, for example:

Between engineering and substation relaying equipment for relay settings;

Between engineering and pole-top equipment for maintenance; and

Within power plants.

The main activities performed on this interface include:

Installing and changing device settings, which may include operational settings (such as relay settings, thresholds for unsolicited reporting, thresholds for device mode change, and editing of setting groups), event criteria for log record generation, and criteria for oscillography recording;

Retrieving maintenance information;

Retrieving device event logs;

Retrieving device oscillography files;

Software updates; and

The key characteristics of this interface category are as follows:

The functions performed on this interface are not considered real-time activities.

Some communications carried on this interface may be performed interactively.

The principal driver for urgency on this interface is the need for information to analyze a disturbance.

Device settings should be treated as critical infrastructure information requiring confidentiality.

Logs and files containing forensic evidence following events should likely remain confidential for both critical infrastructure and organizational reasons, at least until analysis has been completed.

These functions are presently performed by a combination of

- Separate remote access to devices, such as by dial-up connection;
- Local access at the device (addressed in Logical Interface Category 17); and
- Access via the same interface used for real-time communications.

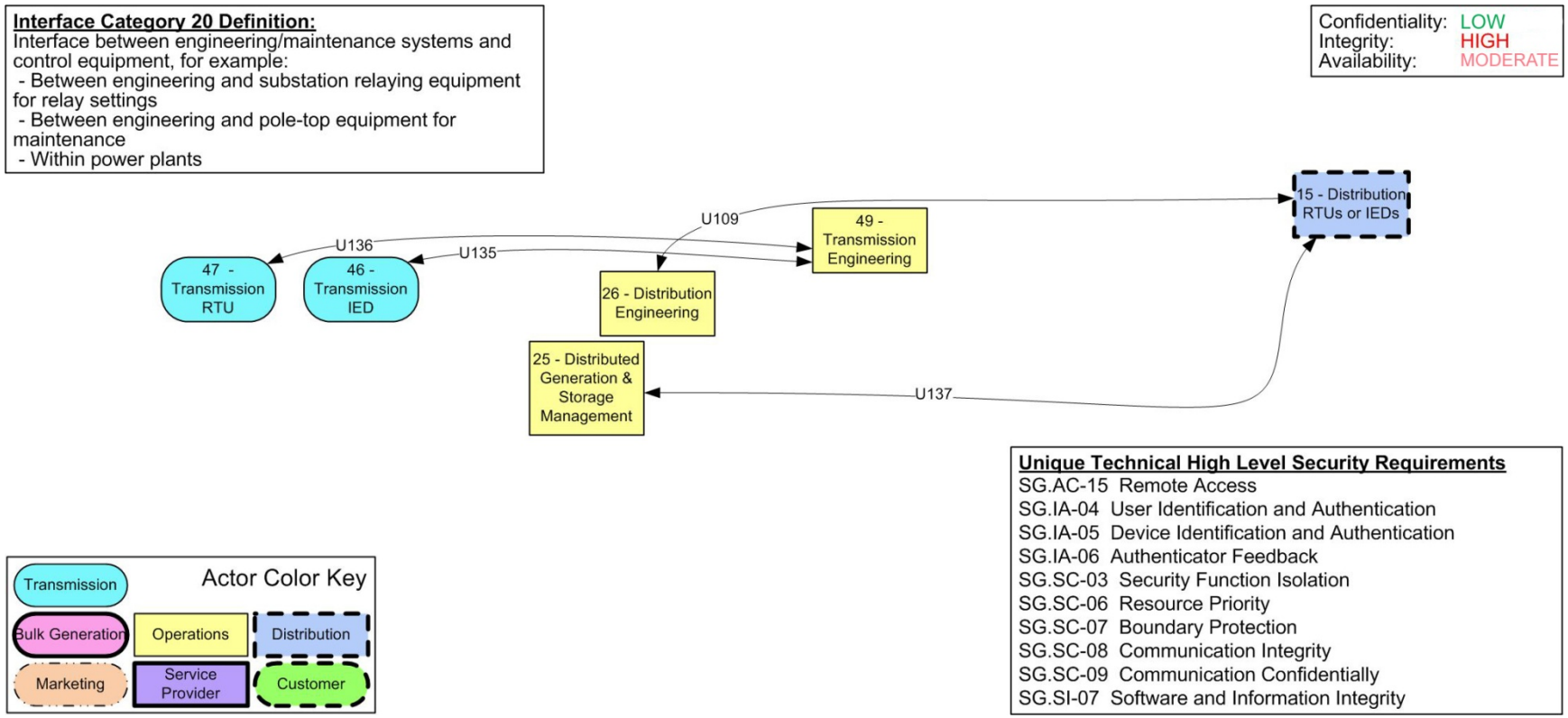


Figure 11 Logical Interface Category 20

1.1.5 Logical Interface Category 21: Interface between control systems and their vendors for standard maintenance and service

Logical interface category 21 covers the interfaces between control systems and their vendors for standard maintenance and service:

Between SCADA system and its vendor.

The main activities performed on this interface include:

Firmware and/or software updates;

Retrieving maintenance information; and

Retrieving event logs.

Key characteristics of this logical interface category are as follows:

The functions performed on this interface are not considered real-time activities.

Some communications carried on this interface may be performed interactively.

The principal driver for urgency on this interface is the need for critical operational/security updates.

These functions are presently performed by a combination of

- Separate remote access to devices, such as by dial-up connection;
- Local access at the device/control system console; and
- Access via the same interface used for real-time communications.

Activities outside of the scope of Logical Interface Category 21 include:

Vendors acting in an (outsourced) operational role (see logical interface categories 1, 4 or 20, depending upon the role).

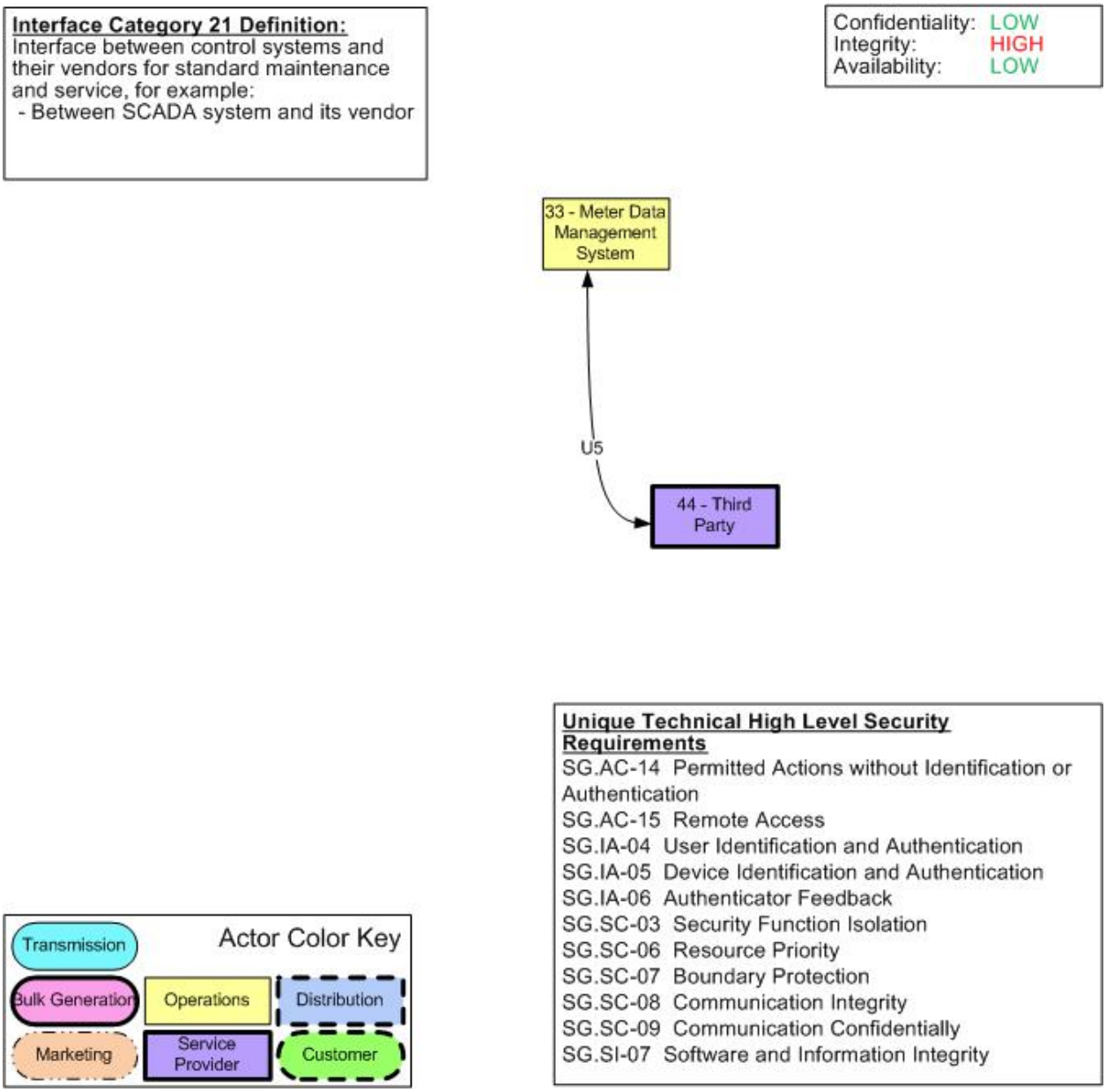


Figure 12 Logical Interface Category 21

1.1.6 Logical Interface Category 22: Interface between security/network/ system management consoles and all networks and systems

Logical interface category 22 covers the interfaces between security/network/system management consoles and all networks and systems:

Between a security console and network routers, firewalls, computer systems, and network nodes.

The main activities performed on this interface include:

Communication infrastructure operations and maintenance;

Security settings and audit log retrieval (if the security audit log is separate from the event logs);

Future real-time monitoring of the security infrastructure; and

Security infrastructure operations and maintenance.

Key characteristics of this logical interface category as follows:

The functions performed on this interface are not considered real-time activities.

Some communications carried on this interface may be performed interactively.

The principal driver for urgency on this interface is the need for critical operational/security updates.

These functions are presently performed by a combination of

- Separate remote access to devices, such as by dial-up connection;
- Local access at the device/control system console; and
- Access via the same interface used for real-time communications.

Activities outside of the scope of Logical interface category 22 include:

Smart grid transmission and distribution (see logical interface categories 1 and 3-);

Control systems engineering and systems maintenance (see logical interface category 20).

(Note: This diagram is not included in the logical reference model.)

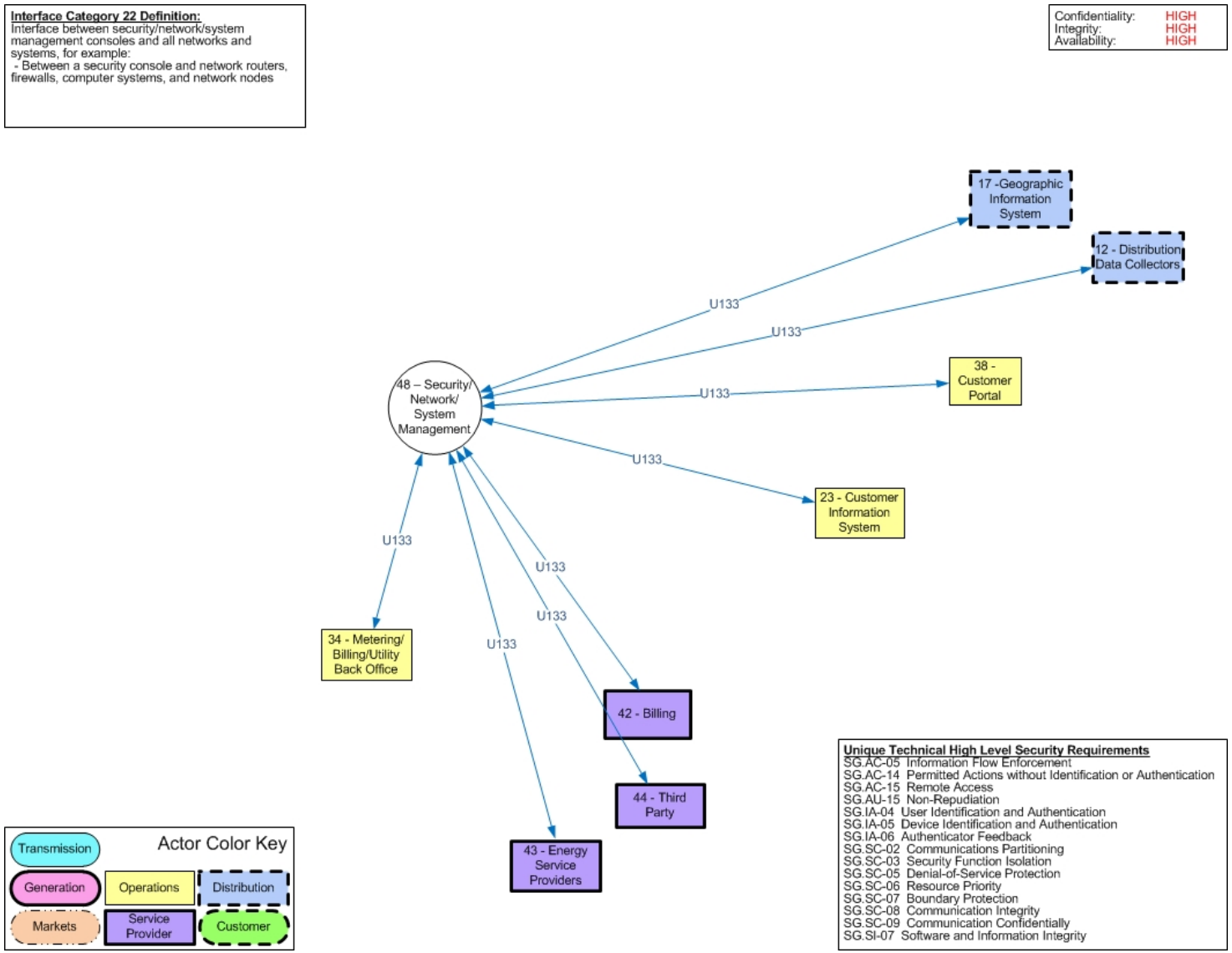


Figure 13 Logical Interface Category 22

Appendix C: Use Cases

Included in this appendix is a use case template and use cases.

Use Case Template: Included below is the use case template that will be used in PBCONF. This template is based on the IntelliGrid template, but has been revised to reduce the content that is not directly applicable to PBCONF. When the use cases have been selected and tailored to PBCONF, they will be documented using this template.

2. Descriptions of Function

All prior work (intellectual property of the company or individual) or proprietary (non-publicly available) work should be so noted.

2.1 Function Name

Name of Function

2.2 Function ID

Identification number of the function

2.3 Brief Description

Describe briefly the scope, objectives, and rationale of the Function.

2.4 Narrative

A complete narrative of the Function from a Domain Expert's point of view, describing what occurs when, why, how, and under what conditions. This will act as the basis for identifying the Steps in Section 2. All actors should be introduced in this narrative. All sequences to be described in section 2 should be introduced in prose here. Embedded graphics is supported in the narrative.

2.5 Actor (Stakeholder) Roles

Describe all the people (their job), systems, databases, organizations, and devices involved in or affected by the Function (e.g. operators, system administrators, technicians, end users, service personnel, executives, SCADA system, real-time database, RTO, RTU, IED, power system). Typically, these actors are logically grouped by organization or functional boundaries or just for collaboration purpose of this use case. We need to identify these groupings and their relevant roles and understand the constituency. The same actor could play different roles in different Functions, but only one role in one Function. If the same actor (e.g. the same person) does play multiple roles in one Function, list these different actor-roles as separate rows.

Actor Name	***Actor Type (person, organization, device, system, or subsystem)***	***Actor Description***

Replicate this table for each logic group.

2.6 Information exchanged

Describe any information exchanged in this template.

Information Object Name	*Information Object Description*

2.7 Diagram

For clarification, draw (by hand, by Power Point, by UML diagram) the interactions, identifying the Steps where possible.

3. Auxiliary Issues

3.1 References and contacts

Documents and individuals or organizations used as background to the function described; other functions referenced by this function, or acting as “sub” functions; or other documentation that clarifies the requirements or activities described. All prior work (intellectual property of the company or individual) or proprietary (non-publicly available) work must be so noted.

ID	Title or contact	Reference or contact information
[1]		
[2]		

3.2 Revision History

For reference and tracking purposes, indicate who worked on describing this function, and what aspect they undertook.

No	Date	Author	Description

Use Cases

Listed below are use case repositories and the selected use cases that are being reviewed for applicability to PBCONF. As with the material in the previous appendixes, the selected use cases will be further tailored for PBCONF. Items 1 through 4 in the list below focus on cyber security for the electric sector. Items 5 through 9 are general repositories that focus on the functionality of the electric sector, and typically do not address cyber security. The use cases that are selected from these repositories will focus on substation functionality.

The use cases that are selected will focus on securing remote access to a variety of transmission and distribution substation devices. This includes security change management, monitoring for change, security auditing and reporting, secure remote access, global security policy application, and authentication and non-repudiation.

1. NISTIR 7628 Use Cases in Volume 3. Included in this PBCONF appendix are nine use cases from the NISTIR 7628.

2. ASAP-SG security profiles that are applicable to PBCONF:
   a. Security Profile for Distribution Management
   b. Security Profile for Wide-Area Monitoring, Protection, and Control
   c. Security Profile for Third Party Data Access
   d. Security Profile for Substation Automation

   The profiles are available at: *osgug.ucaiug.org/*

3. The NIST National Cybersecurity Center of Excellence Identity and Access Management Use Case. It is available at: http://csrc.nist.gov/nccoe/energy/NCCoE%20ES%20Use%20Case%20-%20Identity%20and%20Access%20Management%2020131105.pdf

4. NIST Cyber Security Working Group (CSWG) 2009 working sessions use cases applicable to PBCONF. There are 46 use cases. All the use cases are available at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/ConsolidateUseCasesandRawMaterial

5. Intelligrid Use Cases: There are approximately 200 and they are available at: http://www.smartgrid.epri.com/Repository/Repository.aspx

6. SCE Use Cases: The focus is on AMI and they are available at: https://www.sce.com/SC3/CustomerService/smartconnect/industry-resource-center/use-cases.htm .

   The most applicable use case is: Draft AMI Use Case: D2 - Distribution Engineering or Operations optimize network based on data collected by the AMI system 04/13/06

7. I3P, Requirements for Cross Domain Information Sharing Within SCADA Environments (Including Use Cases), January 2006 (none selected). The url is: http://www.thei3p.org//docs/publications/ResearchReport4.pdf

8. The Integrated Energy and Communication Systems Architecture Volume II: Functional Requirements, *Appendix E: Use Cases (as authored)*, 2004. The url is:

http://www.intelligrid.info/intelligrid_architecture/iecsa_volumes/iecsa_volumeii_appendixe.pdf

NISTIR 7628 Use Cases:

Included in this section are use cases from the NISTIR 7628. As with the previous material, this will be used to in the PBCONF and will be revised as the project continues.

Use Case Scenarios

Distribution Automation Security Use Cases

Category: **Distribution Automation (DA)**		
Scenario: **DA within Substations**		
Category Description A broad definition of "distribution automation" includes any automation that is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources, and automated interfaces with end-users. No one approach is optimal for a utility or its customers. Certain DA functions, such as optimal volt/VAR control, can be more beneficial to one utility or even a few feeders in one utility, while other DA functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities. Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.		
Scenario Description Distribution automation within substations involves monitoring and controlling equipment in distribution substations to enhance power system reliability and efficiency. Different types of equipment are monitored and controlled: • Distribution supervisory control and data acquisition (SCADA) systems monitor distribution equipment in substations • Supervisory control on substation distribution equipment • Substation protection equipment perform system protection actions • Reclosers in substations		
Smart Grid Characteristics Provides power quality for the range of needs in a digital economy Optimizes asset utilization and operating efficiency Anticipates and responds to system disturbances in a self-correcting manner	**Cyber Security Objectives/Requirements** Integrity of distribution control commands is critical for distribution operations, avoiding outages, and providing power to customers reliably and efficiently Availability for control is critical, while monitoring individual equipment is less critical Confidentiality is not very important	**Potential Stakeholder Issues** Customer safety Device standards Cyber Security

Category: Distribution Automation

Scenario: DA Using Local Automation

Category Description

A broad definition of “distribution automation” includes any automation that is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources, and automated interfaces with end-users.

No one approach is optimal for a utility or its customers. Certain distribution automation functions, such as optimal volt/VAR control, can be more beneficial to one utility or even a few feeders in one utility, while other distribution automation functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.

Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.

Scenario Description

Local automation of feeder equipment consists of power equipment that is managed locally by computer-based controllers that are preset with various parameters to issue control actions. These controllers may just monitor power system measurements locally, or may include some short range communications to other controllers and/or local field crews. However, in these scenarios, no communications exist between the feeder equipment and the control center.

Local automated switch management

Local volt/VAR control

Local Field crew communications to underground network equipment

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Provides power quality Optimizes asset utilization Anticipates and responds to system disturbances	Integrity of distribution control commands is critical for distribution operations, avoiding outages, and providing power to customers reliably and efficiently Availability for control is critical, while monitoring individual equipment is less critical Confidentiality is not very important	Customer safety Customer device standards Demand response acceptance by customers

Transmission Resources Security Use Cases

Category: Transmission Operations

Scenario: Real Time Normal Transmission Operations Using Energy Management System (EMS) Applications and SCADA Data

Category Description

Transmission operations involve monitoring and controlling the transmission system using the SCADA system to monitor and control equipment in transmission substations. The EMS assesses the state of the transmission system using applications typically based on transmission power flow models. The SCADA/EMS is located in the utility's control center, while the key equipment is located in the transmission substations. Protective relaying equipment monitors the health of the transmission system and takes corrective action within a few milliseconds, such as tripping circuit breakers if power system anomalies are detected.

Scenario Description

Transmission normal real-time operations involve monitoring and controlling the transmission system using the SCADA and EMS. The types of information exchanged include:

- Monitored equipment states (open/close), alarms (overheat, overload, battery level, capacity), and measurements (current, voltage, frequency, energy)
- Operator command and control actions, such as supervisory control of switching operations, setup/options of EMS functions, and preparation for storm conditions
- Closed-loop actions, such as protective relaying tripping circuit breakers upon power system anomalies
- Automation system controls voltage, VAR, and power flow based on algorithms, real-time data, and network linked capacitive and reactive components

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Provides power quality Optimizes asset utilization Anticipates and responds to system disturbances	Integrity is vital to the safety and reliability of the transmission system Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g., 1 s) Confidentiality is not important	Customer safety Customer device standards Demand response acceptance by customers

Category: Transmission Operations

Scenario: EMS Network Analysis Based on Transmission Power Flow Models

Category Description

Transmission operations involve monitoring and controlling the transmission system using the SCADA system to monitor and control equipment in transmission substations. The EMS assesses the state of the transmission system using applications typically based on transmission power flow models. The SCADA/EMS is located in the utility's control center, while the key equipment is located in the transmission substations. Protective relaying equipment monitors the health of the transmission system and takes corrective action within a few milliseconds, such as tripping circuit breakers if power system anomalies are detected.

Scenario Description

EMS assesses the state of the transmission power system using the transmission power system analysis models and the SCADA data from the transmission substations

EMS performs model update, state estimation, bus load forecast

EMS performs contingency analysis, recommends preventive and corrective actions

EMS performs optimal power flow analysis, recommends optimization actions

EMS or planners perform stability study of network

Exchange power system model information with RTOs/ISOs and/or other utilities

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Provides power quality Optimizes asset utilization Anticipates and responds to system disturbances	Integrity is vital to the reliability of the transmission system Availability is critical to react to contingency situations via operator commands (e.g. one second) Confidentiality is not important	Cyber Security

Category: Transmission Operations

Scenario: Real Time Emergency Transmission Operations

Category Description

Transmission operations involve monitoring and controlling the transmission system using the SCADA system to monitor and control equipment in transmission substations. The EMS assesses the state of the transmission system using applications typically based on transmission power flow models. The SCADA/EMS is located in the utility's control center, while the key equipment is located in the transmission substations. Protective relaying equipment monitors the health of the transmission system and takes corrective action within a few milliseconds, such as tripping circuit breakers if power system anomalies are detected.

Scenario Description

During emergencies, the power system takes some automated actions and the operators can also take actions:

Power System Protection: Emergency operations handles under-frequency load/generation shedding, under-voltage load shedding, load tap changer (LTC) control/blocking, shunt control, series compensation control, system separation detection, and wide area real time instability recovery

Operators manage emergency alarms

SCADA system responds to emergencies by running key applications such as disturbance monitoring analysis (including fault location), dynamic limit calculations for transformers and breakers based on real-time data from equipment monitors, and prearming of fast acting emergency automation

SCADA/EMS generates signals for emergency support by distribution utilities (according to the T&D contracts):

Operators performs system restorations based on system restoration plans prepared (authorized) by operation management

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Provides power quality	Integrity is vital to the safety and reliability of the transmission system	Customer safety
Optimizes asset utilization	Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g., 1 s)	Customer device standards
Anticipates and responds to system disturbances	Confidentiality is not important	Demand response acceptance by customers

Asset Management Security Use Cases

Category: Asset Management

Scenario: Utility Performs Localized Load Reduction to Relieve Circuit and/or Transformer Overloads

Category Description

At a high level, asset management seeks a balance between asset performance, cost, and risk to achieve the utilities business objectives. A wide range of conventional functions, models, applications, devices, methodologies, and tools may be deployed to effectively plan, select, track, utilize, control, monitor, maintain, and protect utility assets.

For our purposes we will establish the scope for the asset management category to be the use of specific applications and devices by utility staff, such as condition monitoring equipment, protection equipment, event recorders, CMMS, display applications, ratings databases, analysis applications, and data marts (historians).

Advanced functions that are associated with asset management include dynamic rating and end of life estimation.

Scenario Description

Transmission capacity can become constrained due to a number of system-level scenarios and result in an overload situation on lines and substation equipment. Circuit and/or transformer overloads at the distribution level can occur when higher than anticipated customer loads are placed on a circuit or when operator or automatic switching actions are implemented to change the network configuration.

Traditional load reduction systems are used to address generation shortfalls and other systemwide issues. Localized load reduction can be a key tool enabling the operator to temporarily curtail the load in a specific area to reduce the impact on specific equipment. This scenario describes the integrated use of the demand response system, other load reduction systems, and the SCADA/EMS to achieve this goal.

Smart Grid Characteristics	Objectives/Requirements	Potential Stakeholder Issues
Provides power quality for the range of needs in a digital economy Optimizes asset utilization and operating efficiency Anticipates and responds to system disturbances in a self-correcting manner	Load reduction messages are accurate and trustworthy DR messages are received and processed timely	Demand response acceptance by customers

Category: Asset Management

Scenario: Utility System Operator Determines Level of Severity for an Impending Asset Failure and Takes Corrective Action

Category Description

At a high level, asset management seeks a balance between asset performance, cost, and risk to achieve the utilities business objectives. A wide range of conventional functions, models, applications, devices, methodologies, and tools may be deployed to effectively plan, select, track, utilize, control, monitor, maintain, and protect utility assets.

For our purposes we will establish the scope for the asset management category to be the use of specific applications and devices by utility staff, such as condition monitoring equipment, protection equipment, event recorders, CMMS, display applications, ratings databases, analysis applications, and data marts (historians).

Scenario Description

When pending asset failure can be anticipated, the system operator, asset management, apparatus engineering, and maintenance engineering staff work closely together with the objective of avoiding an unplanned outage while avoiding further damage to the equipment.

This scenario involves the use of online condition monitoring devices for the range of assets monitored, offline test results, mobile workforce technologies, the communications equipment used to collect the online data, data marts (historian databases) to store, and trend data, as well as condition analysis applications, CMMS applications, display applications, and SCADA/EMS.

Smart Grid Characteristics	Objectives/Requirements	Potential Stakeholder Issues
Provides power quality for the range of needs in a digital economy Optimizes asset utilization and operating efficiency Anticipates and responds to system disturbances in a self-correcting manner	Asset information provided is accurate and trustworthy Asset information is provided in a timely manner	Cyber Security