What Security Topics Should Be Covered in Standards and Specifications

Frances Cleveland (fcleve@xanthus-consulting.com)

Convenor, IEC TC57 WG15 on Data and Communication Security for Power Systems

1. Introduction

1.1 Scope and Purpose

This paper provides suggestions on what security topics should be covered in standards and specifications that are to be used in the power industry. These suggestions cannot be prescriptive for every standard, since individual standards and specifications may legitimately have very different focuses, but it should be expected that the combination of such standards and specifications used in any implementation should cover these security topics. ***These suggestions could therefore be used as a checklist for the combination of standards and specifications used in implementations of systems.***

1.2 Structure of this Document

The security requirements for human users and software applications are different from the purely technical security requirements found in many communication and device standards. For user security standards, more emphasis must be on "policy and procedures" and "roles and authorization" rather than "bits and bytes" cryptographic technologies that should be included in Information and Communications Technology (ICT). In addition, engineering practices and system configurations must be taken into account, since no cryptography can compensate for poor design. Figure 1 illustrates the relationships between security requirements, threats, and attacks.

This document is structured into three sections:

- **Section 2:** Security requirements for standards and specifications which do not address specific cybersecurity technologies but where interactions between human users, software applications, and smart devices must be secured.
- **Section 3:** Security requirements for standards and specifications that address information and communication technologies (ICT).
- **Section 4:** Engineering design and configuration requirements that provide system reliability, defense in depth, and other security threat mitigations.
- **Section 5:** Security requirements related to the OSI Reference Model

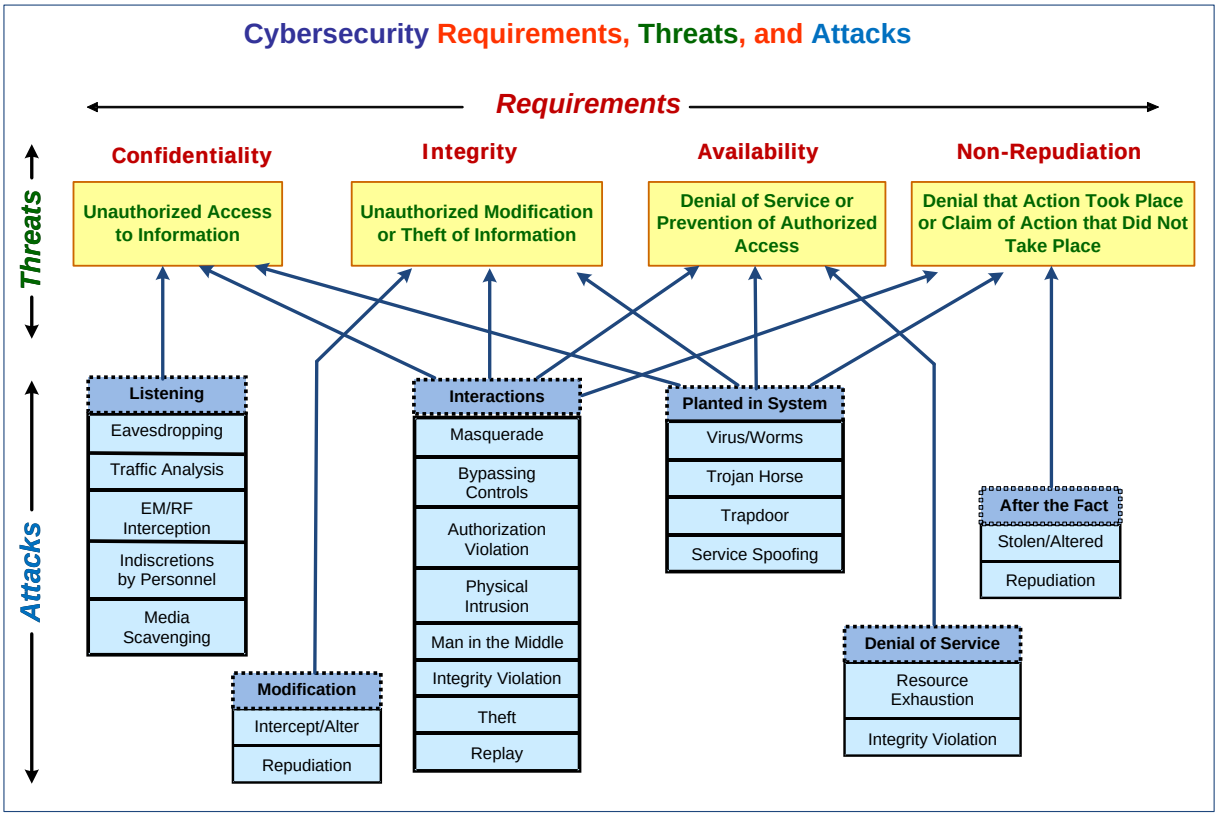

Figure 1: Security Requirements, Threats, and Possible Attacks

2. Security Requirements for Human Users and Software Applications Which Interact with Automation Systems

Users who interact with the automation systems should be required to follow security policies and procedures. These security requirements should cover both the human users and the software applications that interact with each other in response to the automation system designs, user actions, and external monitored events.

Some of the key security requirements that could be addressed (as appropriate to their scope) by standards and specifications include the following.

2.1 Risk Assessment, Security Policies, and Security Requirements

These general cyber security considerations should be covered in the standards and specifications as appropriate.

- **Do not re-invent security requirements** if they can be found in well-established standards. Instead, use **normative references to standards** as much as possible, with the selection of alternatives or options normatively stated.

- Some high level security standards that focus on the electric power industry[1] include:
  - ISO/IEC 27019: *Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry*
  - NISTIR 7628: *Guidelines for Smart Grid Cyber Security*
  - NERC CIP 2-9: *Critical Infrastructure Protection*
  - IEC 62351 series: *Power systems management and associated information exchange – Data and communications security*
- Any discussions or explanations that are used to help with understandings of security issues should be clearly identified as informative.
- Use "shall" or "must" for normative statements, and use "should", "could", or "may" for informative statements.
- Preferably normative and informative information should be in separate clauses, although simple introductory informative sentences are reasonable in a normative clause.

- Start by identifying the major **security threats and failure scenarios**, including assessing their **likelihood** and their possible **impacts (risk assessment)**:
  - Reference the SGIS Toolbox, NIST SP-800-30 Rev 1, and other risk assessment documents.
  - Identify **examples of security breaches and failure scenarios**, and develop use cases that illustrate the failures and can be used to identify the most likely threats, impacts, and mitigations.
  - Which **threats** have highest likelihood? Which threats have the most serious impacts? Which threats may not be preventable but could be mitigated? How can successful attacks be coped with? What audit logs are needed to record possible or successful attacks?
  - Taking into account the possible cost of countermeasures, which **threats** are the most important to **prevent, mitigate, cope with, and log**?
  - The results of this step do not need to be included specifically in the standard, but may be very useful during its development to solidify the security requirements and/or may included as informative
- Require or recommend that **security policies and procedures** be developed for all users covered in the standard (e.g. companies, vendors, implementers, employees, guests, contractors, customers, etc.)

[1] See for a more complete list of standards that include cybersecurity aspects, and for security assessments of some of those standards.

  - NISTIR 7628 Volume 1, Chapter 3, Security Requirements provides a very useful list of areas that could be covered (depending upon the scope of the standard).

- State the **major cyber security requirements** – the first four rely on cryptography and require key management methods, while availability may rely more on engineering strategies and other non-cryptographic methods:
  - **Authentication** of the systems, devices, and applications that are sending and receiving data, is generally the most important security requirement.
  - **Data integrity** of all interactions and of information within the systems, is also critical. Data integrity of messages usually implies detecting tampering since it is not possible to prevent messages from being destroyed or modified, but it is possible to detect these actions.
  - **Confidentiality** is usually for financial, corporate, or private data, but not usually for normal power system operational data exchanges.
  - **Non-repudiation** ensures that some entity cannot deny having received or acted upon a message.
  - **Availability** of the interactions can range from milliseconds to hours or days. Unlike the other cyber security requirements, availability generally relies on engineering design, configuration management, redundancy, functional analysis, communication network analysis, and engineering practices.
- **Security must be end-to-end** and therefore the different security solutions and implementations by different vendors should be interoperable.

2.2 User-Focused Cybersecurity Procedures and Techniques

The following items should be covered in standards and specifications that are addressing the high level requirements, but do not need to get into cryptographic details.

- **Validate and register the identity of users and devices**:
  - For authentication, trust must be established that the users are who they say they are.
  - Users need to be identified through the organization or group they belong to (company, vendor, customer, guest, etc.)
  - These organizations and groups must also establish their identities and be trusted by the other stakeholders in transactions.
  - Users provide passwords, biometric data, or other security mechanisms that tie the user to their identity in the organization/group.
  - Devices, usually when manufactured, must be provided with security certificates, pre-established secret keys, or other security tokens for establishing their identity.
  - These identifications can be used assigning users and devices to “roles”.

- Establish the authorizations and privileges of each role in **Role-Based Access Control (RBAC)** (reference IEC 62351-8):
  - Each (human) user, software application, and device should be assigned to one or more of the roles, thus acquiring the associated authorizations and privileges (read data, issue commands, write data, modify data, delete data, execute applications) that are assigned to those roles.
  - Some roles ought to be mutually exclusive in order to ensure the separation of duties, to eliminate conflicts of interest, and to ensure independence in the responsibilities.
  - Users, applications, and devices may be assigned to multiple roles so long as they are not mutually exclusive.
  - RBAC privileges should be linked to the data wherever it is located, such as in a device or a database.
- **Require the authentication** of all interactions between users and applications, and between different applications, based on the trusted identities of these users and applications.
  - Authentication of interactions can include the use of passwords, application tokens, digital signatures, certificates, message authentication codes (MAC hashes), etc. All authentication relies on cryptography (even passwords if they are transmitted between systems) and thus necessitates **key management** (see clause 2.5). Public key infrastructure (PKI) is the most commonly used for key management, but may not be applicable in all situations.
  - Avoid specifying cryptographic algorithms (such as RSA) if the standard is focused only on user requirements, since there are many valid cryptographic methods. However, there should be a reference to a cryptographic standard that does cover the appropriate cryptographic technologies for these user requirements.
  - Whenever possible and appropriate, reference existing standards, such as the IEC 62351 series and the security-related IETF RFCs.
- Focus on the **integrity of information**:
  - Integrity of information relies on cryptography, specifically message authentication codes (MAC hashes) which use cryptographic keys to ensure that any tampering of information can be detected (not prevented). Often integrity cryptography is combined with authentication, such as with digital signatures with certificates. Integrity cryptography (MAC) is also usually included in confidentiality which combines tamper detection with encryption for prevention of eavesdropping.
  - Key management is required for integrity.
  - Data entry by users and software applications should be checked for validity as much as possible, including reasonability of values, and where possible, cross-checked by algorithms, visual displays, testing, or other mechanisms.

  - Integrity of information should apply also for message exchanges, database access, software patches, software updates, and configuration.

- Identify those interactions that require **confidentiality**:
  - Confidentiality relies on encryption algorithms which use cryptographic keys to prevent eavesdropping. Usually these encryption algorithms are combined with integrity cryptography to ensure both confidentiality and integrity.
  - Key management is required for confidentiality.
  - These interactions usually involve corporate, financial, customer, and market information.
  - Privacy (personal information) can also be considered confidential, but may require additional management if aggregations are used for planning or other functions
  - Avoid specifying cryptographic algorithms (such as RSA) if the standard is focused only on user requirements, but ensure some standard does cover the appropriate cryptographic technologies for all system designs.
- Determine **availability requirements** for all types of interactions:
  - Availability is mostly affected by configuration design and management. Therefore, normally key management is not necessary for availability.
  - What timing latency is allowed for different types of interactions: milliseconds, seconds, minutes, or even days?
  - How closely monitored must that timing be? Issue an alarm? Log it? Ignore?
  - What kind of redundancy (or other methods) should be used to improve this availability?
  - What actions are required if those timing requirements are not met?
- Determine if **non-repudiation and/or accountability** are necessary for different types of transactions:
  - Event logs can capture the fact that a transaction was initiated, while a similar, time-synchronized event log of the recipient of the transaction is necessary for non-repudiation of that transaction.
  - Authenticated responses to transactions can also provide non-repudiation records.
- **Revoke user access** and/or privileges when a user or an application's role changes
  - Revoke access through RBAC and disable the user's passwords.
  - Ensure revocations are made available to all affected systems in a timely manner
  - For temporary assignment of users to roles, ensure that a deadline is associated with that assignment and the user is revoked at the deadline.
- **Deregister applications** and revoke any certificates or tokens if an application is decommissioned or its security is compromised

- Ensure revocations are made available to all affected systems in a timely manner, usually within a day or so.

- Establish **alarm and event logs** content, accuracy of the timestamps, synchronicity of timestamping, and security requirements:
  - Log and timestamp all anomalous events
  - Ensure all alarms are assigned to one or more roles so that they will be viewable.
  - For higher priority alarms, ensure that at least one user has logged on in one of the assigned roles.
  - Track user interactions with applications and systems, as appropriate
  - Synchronize the timestamps across all systems within the necessary accuracy (milliseconds or seconds).
  - Prevent or log all modifications to logs.
  - Archive logs for appropriate lengths of time.
  - Provide relevant logs to security personnel.
  - Provide methods for correlating different types of events – sort/search

3. Information and Communication Technology (ICT) Cryptographic Techniques

In standards and specifications that focus on specific Information and Communication Technology (ICT) requirements such as communication protocols and interactions with "intelligent" equipment, the following security requirements could be directly included or could include normative references to other standards, as appropriate (this is just a checklist, so not all standards or specifications should include all items):

3.1 Best practices for Specifying Cryptography

Some of the best practices for specifying cryptography used for confidentiality, authentication, and/or digital signatures are:

- Use **normative references to cryptographic standards** rather than describing the cryptography (except for informative purposes). If there are alternatives or options within the referenced standards, indicate which are mandatory, which are recommended, which are optional, and which must not be used.
- Cipher suites are always evolving, so specifying only one can be self-defeating over time. However, one cipher suite can be mandated for interoperability, with other cipher suites permitted and negotiated at startup.
- Because cipher suites get broken or "weaken" over time as computer speeds increase and hacker capabilities improve, only cipher suites of "adequate strength" should be permitted. Options for improved cipher suites over time should also be permitted.

- The permitted cryptographic algorithms should not be listed as deprecated by leading security organizations, such as NIST. NIST lists the deprecation dates of certain cryptographic algorithms in NIST SP800-131a.
- Legacy equipment may be allowed to use deprecated cryptographic algorithms so long as "mitigating" countermeasures are included. No new implementations should be permitted to implement deprecated cryptographic algorithms.
- Key management and certificate management requirements should be included, either directly or by normative reference.
- Implementation considerations include when "session" keys should be updated, how certificate expirations should be handled (ignored? Warning? Stop interactions?), and how certifications that have been revoked should be provided to affected systems.

3.2 Cryptographic Methods

The following cryptography methods are commonly specified. Normative references should be used where possible. More information on NIST cryptographic toolkit can be found at http://csrc.nist.gov/groups/ST/toolkit/index.html.

- The most common block cipher is the **Advanced Encryption Standard (AES),** usually either AES-128 or AES-256. NIST has identified it as the preferred block cipher. Neither DES nor Triple DES (3DES) should be specified anymore.
- **Confidentiality** (but not authentication) is provided by block cipher modes. Block ciphers only encrypt one block, so block cipher modes are used to string together the encryption of messages that are longer than one block while still using the same cryptographic key. The most common block cipher modes are cipher-block chaining (CBC) mode and counter (CTR) mode.
- **Authentication** and **integrity** are provided by digital signatures and/or by "hashing" messages with cryptographic keys. These methods do not provide confidentiality – the messages can be read by anyone – but they do provide authentication of the sender and the ability to determine if the message has be tampered with. They require less "compute" processing than the block cipher modes.
  - **Digital signatures** algorithms include RSA-based signature schemes, such as RSA-PSS or RSA ANS x9.31, and DSA and its elliptic curve variant ECDSA, e.g. ECDSA ANS X9.62
  - The **cryptographic hashing** methods or "codes" are called Message Authentication Codes (MAC). To avoid some confusion with the term "Media Access Control (MAC)", they are sometimes called Message Integrity Codes (MIC). The most common include the Keyed-Hash Message Authentication Code (HMAC), CBC-MAC (CMAC), and Galois/Counter Mode (GCM) and GMAC. These can be further specified as to which hashing ciphers and size to use, such as HMAC-SHA256 or AES-GMAC-128.

- Combinations of confidentiality and authentication modes are called authenticated encryption (AE). Examples of AE modes are CCM (NIST SP800-38C), GCM (NIST SP800-38D), CWC, EAX, IAPM, and OCB.
- **Certificates** are issued **by Certificate Authorities (CA)** as a method for certifying the validated identity of a device or software application – the equivalent to a birth certificate or passport for a human. Most certificates use the ITU X.509 format for public key certificates, which bind a public key to the certified device or application, which contains (and guards) the corresponding secret key. **Public Key Infrastructure (PKI)** is the most commonly used method.

3.3 Internet Cryptography

Internet cryptography uses cryptographic profiles defined in RFCs by the IETF. The predominant RFCs include:

- **Transport Layer Security (TLS)** was derived from Secure Sockets Layer (SSL) and specifies asymmetric cryptography for authentication of key exchanges via the Public Key Infrastructure (PKI), symmetric encryption for confidentiality, and message authentication codes for message integrity. As indicated by the name, TLS provides security for the transport layer. Although the most commonly implemented version is still TLS 1.0, the newest version TLS v 1.2, defined in RFC 5246, should be specified for new implementations. TLS includes many alternative cipher suites – these could or should be pared down to a few in specifications to ensure that implementations provide adequate security and interoperability. IEC 62351-3 Ed 2 provides such a specification.
- **Hypertext Transfer Protocol Security (HTTPS)** is a combining of HTTP over TLS, and in formalized in RFC 2818.
- **Internet Protocol Security (IPsec)** authenticates and encrypts each IP packet as well as providing mutual authentication at the start of a session, thus providing security at the Network Layer rather than at the Transport Layer.
- **Virtual Private Network (VPN)** creates a “tunnel” through the Internet (or other network) in which the entire IP packet is encrypted and then encapsulated into another IP packet.

3.4 Wireless Cryptography

Wireless cryptography systems use the security provided by **IEEE 802.11i WPA2**, which establishes a Robust Security Network (RSN) that uses the Advanced Encryption Standard (AES) block cipher (as do most cipher suites at this time), requires the Counter Cipher Mode (CCM) with block chaining Message Authentication (Integrity) Code (MAC or MIC) Protocol (CCMP) for a 4-way handshake between two stations, and the includes a Group Key Handshake. Some suggestions for managing WiFi could include:

- Using centrally managed WiFi infrastructures and the authentication
- Adopting the IEEE 801.1x authentication infrastructure

- Adopting a rogue AP detection mechanism

The **Extensible Authentication Protocol (EAP)** is an authentication framework frequently used in wireless networks and point-to-point connections. It is defined in RFC 3748 and was updated by RFC 5247. EAP is one of the possible authentication schema of the more general IEEE 801.1x standard that is the de-facto mandatory standard for WiFi enterprise deployment, and it is also applicable to wired LANs. When applied to wired LANs, 802.1x can allow a logical segregation of VLAN inside the same physical infrastructure. 802.1x is a role based Network Access Control mechanism and brings the RBAC model to LAN access control.

3.5 Key Management using Public Key Cryptography

Public Key Cryptography is the cryptographic system that requires two keys, a public key and private key that are mathematically linked so that when one key is used to encrypt a message, the other key can decrypt the message. The public key can be made widely available, which the private key must be kept secret. Although mathematically linked, if the keys are long enough the private key cannot be derived from the public key, making it secure. The public keys used in the RSA system are the product of two very large prime numbers with the secret key being one of those prime numbers. A relatively new algorithm for creating keys, the **Elliptic Curve Cryptography (ECC)** system may permit shorter keys to be used. This public-private key concept is used in TLS and most other cryptographic methods.

The Public Key Infrastructure (PKI) key management process entails a number of steps. IEC 62351-9, Key Management, is identifying and standardizing these techniques for the power industry:

- **Register with Registration Authority (RA)**: Entities (systems, devices, and software applications) must be “registered” usually through an RA to confirm their identities. This registration can occur on manufacturing, on installation, on connection to a network, or off-line. Manufacturers often provide the initial registration of their entities using their corporate identity as proof.
- **Generate public/private key pair**: Either the entity generates its own public/private key pair if it has that capability, or a key pair is (securely) installed in the entity.
- **Request certificate from a Certificate Authority (CA)**: Once entities are registered and have generated their key pairs, a CA can provide these entities with security certificates that bind their identity to their public cryptographic key. The CA verifies this binding by using its own digital signature. Certificates usually have an expiration date, so updated certificates should be requested before the previous certificate expires.
- **Chain subsequent certificates by enrollment**: The identity of an entity can be chained from the initial registration by using the initial certificate to validate subsequent requests for additional certificates, as the entity’s ownership or function is changed over time. Thus, the manufacturer’s certificate can be used to create an integrator’s certificate which can be used to create a utility’s certificate, etc. This enrollment process may be through different CAs, so the CAs digital signatures are used to establish trust with each other. A common method for enrollment is the Simple Certificate Enrollment Protocol (SCEP) but this may be replaced in the near future by an updated method.

- **Assign RBAC roles**: The enrolled devices and software applications should be assigned to their RBAC roles, identifying what permissions and privileges they have, and what actions they permit other roles.
- **Create (and update) session keys**: The public/private keys can be used by two (or more) entities to authenticate each to the other and to create session keys that are used to exchange information between the entities for the length of a session, for instance between a user and their on-line banking web site or between two protective relays. In the latter example, the session keys will need to be periodically updated to ensure the keys are not compromised over the many hours and years that the relays interact.
- **Use session keys**: Session keys can be used to hash messages (authentication and integrity only), provide digital signatures (authentication, integrity, and non-repudiation), or encrypt the message payloads to provide confidentiality. Each of these processes has different cryptographic requirements and performance characteristics.
- **Revoke certificates**: Certificates can be revoked if the private key has been compromised or if the entity must no longer be used in its current role.
- **Access Certificate Revocation Lists (CRL):** CRLs are used for general revocation information when systems are able to access CA sites.
- **Provide Online Certificate Status Protocol (OCSP) servers for revoked certificates:** For power system equipment, alternate methods must often be used, such as OCSP servers.
- **White listing** (namely only permitting access by entities on the white list) can also be used to verify the current status of an entity. In particular, **self-signed certificates** should usually be white listed as added authentication.
- Some devices can use **pre-shared keys** installed (securely) to act as the source for managing their keys, so they do not undertake all the steps, but still need to be authenticated, enrolled, assigned RBAC roles, create and update their session keys, and include a method for revocating their participation in information exchanges.

3.6 Multicast and Group Keys

For peer-to-peer or multicast interactions of entities which have stringent performance requirements, group key management is more efficient that pair-wise key management. Group key management uses a combination of asymmetric and symmetric cryptography. The security process steps include:

- One system or device is designated as **group controller**.
- The group controller **authenticates other entities** via their certificates or pre-shared keys.
- The group controller establishes of a **group-based key**.
- The group controller **distributes the group key** to all authenticated entities.

3.7 Device and platform integrity

- Tamper-resistant design

- Digitally signed firmware images
- Secure storage of cryptography credentials
- Secure code development practices
- Device Identity
- Hardening, No backdoors

3.8 Design Secure Network Configurations

Design network configurations for improved security:

- Networks that are dedicated to different scopes should be **physically and/or logically isolated** (e.g. industrial networks and corporate networks).
- Access points to the **Internet** should either be prevented or very carefully managed.
- **Firewalls** should be used at "security boundaries" to permit only authorized traffic to go through
- **Unused ports** in routers should be disabled to prevent denial of service attacks and other malicious attacks.
- **Intrusion detection and/or intrusion prevention systems (IDS/IPS)** should be deployed.
- **Redundant communication paths** should be provided for applications that require high availability.
- **Service level agreements (SLA)** with any third party communication providers should include very stringent security requirements.

3.9 Network and System Management (NSM)

Establish network and system management (NSM) for all communication networks (reference IEC 62351-7).

- **Alarms and events** from power system operations and equipment should be able to be time-synchronized and coordinated with security alarms and events, in order to provide a complete picture of possible threats and attacks.
- **Monitor the traffic flows** and detect/alarm abnormal conditions, such as communication circuit temporary and permanent failures.
- **Provide intrusion detection** and, for more critical circuits, intrusion prevention.
- **Detect both communication and end equipment operational anomalies**, such as failures, internal alarms, security alarms, etc.
- **Determine what automatic and/or manual actions** should be taken for each type of equipment or circuit anomaly

3.10 Security Testing and Validation Procedures

Establish testing and validation procedures for all software applications and all interactions between users and applications, and between different applications

- Testing of all new systems and devices should include testing of security measures.
- The validity of software applications should be tested to ensure they perform their functions correctly and do not have embedded malware or security vulnerabilities.
- Testing requirements could include both static and dynamic code analysis.
- Guidelines from the Open Web Application Security Project (OWASP) could be used to better ensure that web applications are secure.
- The NISTIR report 7920 (2012) discusses software testing and references the software testing standard, ISO/IEC 29119.
- Validation should include checking all data inputs at least as "reasonable", with possible cross-checking against other data or algorithms for higher priority data.
- Testing should cover initial installations, and after any updates or patching.
- Security procedures should also be tested and validated to ensure they perform the security functions they are designed for.

3.11 Security Interoperability

Clearly identify how the interoperability of the security requirements is to be managed. This is particularly important if different organizations are involved.

- What steps must each organization take? For instance is there a pre-established list of Certificate Authorities that are trusted by each as well as all affected stakeholders? What will the different RBAC roles be and what are their privileges? What security testing is required?
- What are the default security technologies? Which additional ones may be used? Which are deprecated?
- Determine how time synchronizations across all organizations are to be handled?
- What happens if suspicious actions are noted? Who must be informed? What actions are taken? How must people and systems cope with the impacts of suspected security attacks?

3.12 Some Additional Cybersecurity Techniques

Some additional cybersecurity techniques include the following:

- **Network Address Translation (NAT)** functions isolate systems from direct access by external systems. They are often included in WiFi network routers, in which a single Internet IP is provided to a site, and is shared by all networked devices at that site. The NAT handles all interactions with the Internet and passes only authorized messages to the systems behind the NAT router, thus providing security against unauthorized traffic.

- **Access Control Lists (ACL)** are used in routers to limit which ports and/or IP addresses are permitted to be accessed by which entities.
- **Intrusion Detection and Prevention systems (IDS and IPS)** monitor networks for malicious or impermissible traffic. The IDS can detect such malicious traffic and notify users, while an IPS can actually block malicious traffic and support prevention of addition traffic from a suspect IP address.
- The **Group Domain Of Interpretation (GDOI)** method defined in RFC 6407 supports the distribution of a symmetric group key to all pre-configured or otherwise enrolled entities, typically devices.

4. Engineering Design and Configuration Management

Utilities have developed many different engineering practices, functions, configurations, checks, and operational methods to help ensure the reliability and safety of the power system. Although not strictly cybersecurity measures, they do provide mitigations against many of the same types of attacks, and indeed provide defense-in-depth and coping methods that cybersecurity measures cannot achieve. From a power system security perspective, it does not matter if cyber tools are used or if power system reliability tools are used – in fact they complement each other and should always be used in conjunction with each other.

Just as with any engineering, the costs for including any particular protection must be weighed against the likelihood and possible impact of a failure that could have been prevented or mitigated by that protection.

The NISTIR 7628 provides examples of these power system engineering practices and functions in Appendix B. The following capture some of these engineering practices and configurations.

4.1 System Engineering Practices and Configurations

Utility systems are engineered and configured with reliability as a major design factor. Single smart systems and devices can include hardened or redundant components, while multiple systems can be deployed such that they can support or back each other up. Some examples of these system engineering practices and configurations include:

- Redundant equipment (e.g., redundant automation systems, redundant components, spares)
- Redundant communication networks (e.g., multiple communication paths, redundant wireless nodes, redundant interconnections to a backhaul network)
- Redundant automation systems (e.g., redundant controllers, redundant master stations, redundant SCADA computers systems, backup systems that can be quickly switched in)
- Validation of information input for format and reasonability, including that the input is in the correct format, that values are within limits, that the values are not beyond the capabilities of the automation system.

- Redundant information sources (e.g., redundant sensors, voltage measurements from multiple sources such as at the ECP, the PCC, or even the feeder substation)
- Redundant or backup control systems (e.g., multiple master stations that can be assigned to manage different intelligent electronic devices, SCADA systems in physically different locations),
- Redundant power system configurations (e.g., networked grids, multiple feeds to customer site from different substations, microgrid formation)
- Redundant logs and databases with mirrored or frequent updates
- DER generation and storage systems connected at different locations on the grid
- Reserve generation capacity (DER or bulk power) available to handle the rapid emergency changes in generation or load situations
- Configuration setting development procedures, including remedial relay settings
- Post-event engineering forensic analysis capabilities

4.2 Power System Equipment Monitoring, Analysis, and Control

Smart grid systems are part of the larger power system grid, and therefore the reliability of the grid is critical to the reliability of these systems.

- Sensors on substation and feeder equipment monitor volts, VARs, current, temperature, vibrations, etc. – eyes and ears for monitoring the power system
- Control capabilities for local control, either automatically (e.g., breaker trip) or manually (e.g., substation technician raises the voltage setting on a tap changer)
- Volt/var regulation by local equipment to ensure voltages and vars remain within prescribed limits and are coordinated with DER systems volt/var settings
- Protective relaying to respond to system events (e.g., power system fault) by tripping breakers
- Reclosers which reconnect after a “temporary” fault by trying to close the breaker 2-3 times before accepting it as a “permanent” fault. Their actions need to be coordinated with DER “ride-through” settings
- Manual or automatic switching to reconfigure the power system in a timely manner by isolating the faulted section, then reconnecting the unfaulted sections. These actions need to be coordinated with DER microgrid formation and DER volt/var settings, since connection to different sections can necessitate different settings
- Device event logs capture all significant power system events, including DER status changes
- Digital fault recorders capture wave forms of anomalous behavior of the grid
- Power quality (PQ) harmonics recorders

- Time synchronization to the appropriate accuracy and precision is used by all power system equipment to ensure that the events captured in logs can be synchronized across all locations.

4.3 Centralized Monitoring and Control

Utility SCADA systems monitor the equipment that manages the power system and can issue control commands. These SCADA systems report alarms and anomalous events related to the power system. However, these alarms and anomalous events can also indicate automation equipment failures, communication problems, the status of facility equipment, and other automation problems, whether inadvertent or maliciously deliberate.

- SCADA systems have approximately 99.98% availability with 24x7 monitoring,
- SCADA systems continuously monitor generators, substations, and feeder equipment (e.g., every second and/or report status and measurements "by exception"),
- SCADA systems perform remote control actions on generators, substations, and feeder equipment in response to operator commands or software application commands,
- Automatic Generation Control (AGC) issues control commands to generators to maintain frequency and other parameters within limits,
- Load Shedding commands can drop feeders, substations, or other large loads rapidly in case of emergencies,
- Load Control commands can "request" or command many smaller loads to turn off or cycle off,
- Disturbance analysis (rapid snapshots of power system during a disturbance for future analysis),
- Alarm processing, with categorization of high priority alarms, "intelligent" alarm processing to determine the true cause of the alarm, and events, and
- Comparisons of device settings against baseline settings.

4.4 Centralized Power System Analysis and Control

Energy Management Systems (EMS) and Distribution Management Systems (DMS) (along with the DERMS and other control center systems) use many software functions to analyze the real-time state and probable future state of the power system. These software functions include:

- "Power Flow" models of the transmission system, bulk generators, and loads simulate the real-time or future (or past) power system scenarios
- "Power Flow" models of the distribution system simulate real-time or future power system scenarios, and include the characteristics and status of DER systems either individually or in aggregate
- State estimation uses redundant measurements from the field to "clean up" or estimate the real measurements from sometimes noisy, missing, or inaccurate sensor data. Since

many smaller DER systems will not be directly monitored, state estimation can provide estimated values.

- Power flow applications use the state estimated data to better simulate real-time conditions
- Load and renewable generation forecasts based on weather, history, day-type, and other parameters will forecast the generation requirements
- Contingency Analysis (Security Analysis) assesses the power flow model for single points of failure (n-1) as well as any linked types of failures, and flags possible problems
- Generation reserve capacity is available for instantaneous, short term, and longer term supply of generation in the event of the loss of generation
- Ancillary services from bulk generation are available to handle both efficiency and emergency situations (e.g. generator is set to “follow load” for improved efficiency, generator is capable of a “black start” namely to start up during an outage without needing external power)
- Fault Location, Isolation, and Service Restoration (FLISR) analyze fault information in real-time to determine what feeder section to isolate and how to best restore power to unfaulted sections
- Volt/VAR/Watt Optimization determine the optimal voltage, VAR, and generation levels usually for efficiency, but also to handle contingencies and emergency situations
- Direct control of DER and loads (load management) for both efficiency and reliability
- Indirect control of DER and loads (pre-established settings, broadcasts, demand response) for both efficiency and reliability
- Ancillary services from DER for both efficiency and reliability (e.g., var support from inverters, managed charging rates for PEVs).

4.5 Testing

Testing of DER systems for their functionality, and their role in the power system once installed, is critical to reliable operations. Some types of testing include:

- Lab and field testing of all power system and automation equipment minimizes failure rates
- Software system factory, field, and availability testing
- Rollback capability for database updates
- Configuration testing
- Relay coordination testing
- Communication network testing, including near power system faults.

4.6 Training

Training of operators and other stakeholders who are involved with DER systems is vital to ensuring that they are operated reliably and safely:

- Dispatcher training simulator, using snapshots of real events as well as scenarios set up by trainers
- Operational training using case studies, etc.
- Training in using new technologies
- Security training.

5. OSI Reference Model Considerations

In some standards, the OSI reference model layers are pertinent to their specifications. Some considerations on the security at each of these layers is discussed below.

- **Physical layer (PHY)** refers to the actual media such as wireless, cable, and power line carrier (PLC). Some security techniques are included in PHY layer, but are usually focused on checksums and parity bits for detecting and potentially correcting bit-errors during transmissions. Confidentiality, integrity, and authentication security generally relies on the data link layer (and higher layers). However, more secure PHY layer techniques can be incorporated for very sensitive transmissions, such as those used in the military.
  - Most types of PHY layer encoding of 0-1 bits to the media include cyclic redundancy check (CRC) to detect errors in this encoding, usually due to interference or other electrical noise.
  - Wireless LAN security uses techniques such as frequency hopping spread spectrum techniques both to minimize interference and to protect against eavesdropping. For instance, IEEE 802.11 (WiFi) uses direct-sequence spread spectrum (DSSS) and orthogonal frequency-division multiplexing (OFDM).
- **Data link (DLL) layer** covers the node-to-node data link protocols and includes the media access control (MAC) sublayer that links to the PHY layer by defining the format of the data blocks. In some protocols, security is embedded in the DLL layers, but often the primary security is provided by the layers above the DLL layer while affecting the contents of the MAC data blocks and mandating some of the interactions between nodes, particularly those that establish a link. Thus the boundary between the Data Link Layer and the Network Layer can be fuzzy when discussing security. Common data link layer protocols include:
  - Ethernet (IEEE 802.3) defines the media access control (MAC) of the PHY and DLL layers, using “carrier-sense, multiple-access with collision detection (CSMA/CD)” technology. It is used in most wired LANs and some WANs. Ethernet relies on security at the Network Layer and above.
  - Wireless protocols are defined in the IEEE 802.xx series, including 802.11 for wireless, 802.15.4 for Bluetooth, etc. The security requirements for these wireless

protocols are defined in 802.11i. Although ostensibly for wireless communications, these security requirements can also be used over other media such as narrowband PLC.

  - Power line carrier data link layer security is covered in IEEE 1901, the wideband ITU G.9960 - 9961, and the narrowband ITU G.990x series (9902, 9903, and 9904).
  - Digital Subscriber Line (DSL) is used over telephone lines, usually to provide Internet access to individual homes. DSL relies on security at the Network Layer and above.
  - General packet radio service (GPRS) is a packet oriented mobile data service on the 2G and 3G cellular communications. GPRS relies on security at the Network Layer and above as defined by the Global System for Mobile Communications (GSM).

- **Network layer** covers the interactions through networks from node to node. Virtually all networks now us Internet Protocol (IP), although there are three flavors of IP:
  - IPv4 is the current protocol used across the Internet
  - IPv6 is the new protocol that uses longer IP addresses in order to provide unique address to the billions of new devices
  - IPsec provides security as part of the Network layer
- **Transport layer** covers the end-to-end management of messages.
  - TLS is the predominant transport security for establishing authenticated interactions across networks that use TCP/IP.
  - VPNs also provide network security through insecure networks by encrypting entire messages and tunneling them through the network by encapsulating them.
- **Application layer** covers the structure, format, and interaction sequences of messages. At this layer, the most important security issues are authentication of the actual software applications that are interacting. For power system communication protocols, particularly those that do not use the TCP transport layer and therefore cannot use TLS or other transport security techniques, protocol-specific security is necessary. Examples include:
  - IEC 62351-4 for the Manufacturing Message Specification (MMS) used in IEC 61850 and IEC 60-870-6 (aka. TASE.2 or ICCP)
  - IEC 62351-5 for IEC 60870-5
  - IEC 62351-6 for IEC 61850 GOOSE and SV
  - IEEE 1815 for DNP3
  - IEC 62351-11 for XML-based protocols (in development)
  - ANSI C12.22 for (North American) AMI systems