White Paper: Cyber Security Issues for the Smart Grid

Frances Cleveland, Xanthus Consulting International

1. General Cyber Security Concepts

1.1 What Does “Cyber Security” Cover? The “All Hazards” Approach

In its broadest sense, cyber security for the power industry covers all issues involving automation and communications that affect the operation of electric power systems and the functioning of the utilities that manage them.

In the power industry, the focus has been almost exclusively on implementing equipment that can improve power system reliability. Until recently, communications and information equipment have been considered of peripheral importance – they were often seen as just another isolated piece of equipment to help achieve power system reliability. However, increasingly the reliability of this information infrastructure has become critical to the reliability of the power system. For example, with the exception of the initial power equipment problems in the August 14, 2003 blackout, the on-going and cascading failures were almost exclusively due to problems in providing the right information to the right place within the right time.

But, as also seen in the August 14 blackout, the information infrastructure failures were not due to any terrorist or Internet hacker or virus; these failures were caused by inadvertent events – mistakes, lack of key alarms, and poor design. Therefore, if the goal is really to maintain and improve the reliability of the power system, then inadvertent compromises must be addressed as well – the focus must be an **All-Hazards** approach.

1.2 Cyber Security IAC (Integrity, Availability, Confidentiality) Requirements

FIPS-199 (and many other security documents) classify security requirements of information types by priority into Confidentiality, Integrity, and Availability (CIA). On the other hand, industrial control systems typically classify the priorities of the security requirements in a different order, namely Integrity, Availability, Confidentiality, and (sometimes) Accountability (Non-repudiation).

Integrity is generally considered the most critical security requirement for power system operations, and includes assurance that:

- Data has not been modified without authorization
- Source of data is authenticated
- Timestamp associated with the data is known and authenticated
- Quality of data is known and authenticated

Availability is generally considered the next most critical security requirement, although the time latency associated with availability can vary:

- 4 ms for protective relaying
- Sub-seconds for transmission wide-area situational awareness monitoring
- Seconds for substation and feeder SCADA data
- Minutes for monitoring non-critical equipment and some market pricing information
- Hours for meter reading and longer term market pricing information
- Days/weeks/months for collecting long term data such as power quality information

Confidentiality is generally the least critical for actual power system operations, although this is changing for some parts of the power system, as customer information is more easily available in cyber form:

- Privacy of customer information is the most important
- Electric market information has some confidential portions
- General corporate information, such as human resources, internal decision-making, etc.

Non-repudiation is sometimes considered as well, since there is often a need to prove that a signal, price, response, etc. was sent and received.

1.3 Threats and Threat Agents

Threat agents are the causes of attack threats. These threat agents can be human, the systems themselves, or the environment. The threat agents can be deliberately attacking the information infrastructure or may inadvertently do so.

- **Deliberate**: Threat Agents which undertake deliberate attacks
  - Disgruntled employee
  - Industrial espionage agents
  - Vandals
  - Cyber hackers
  - Viruses and worms
  - Thieves
  - Terrorists
- **Inadvertent**: Threat Agents which may cause inadvertent “attacks” on systems
  - Careless users
  - Employees who bypass security
  - Poorly designed systems
  - Unintended consequences of multiple actions
  - Safety system failures
  - Equipment failures
  - Natural disasters

The most dangerous threat agent is a disgruntled employee who knows exactly where the vulnerabilities are in the system, which security measures are the easiest to breach, and which actions could cause the worst damage. The most destructive threat agents can be natural disasters due to the sheer scope of potential damage. The most common threat agent is the careless user who makes data entry mistakes, incorrectly connects equipment to networks, or leaves his password in full view of others.

1.4 Security Purposes

Security is not just about preventing security attacks or system compromises; it is also about managing the inevitable successful (deliberate or inadvertent) attacks. Particularly for real-time operations, it is crucial to "live through" any attacks or compromises to the information infrastructure, and to recover with minimal disruption to the power system operations – including power system reliability, efficiency, and cost.

The security purposes can be categorized as follows:

- **Deterrence and delay**, to try to avoid attacks or at least delay them long enough for counter actions to be undertaken. This is the primary defense, but should not be viewed as the only defense.
- **Detection of attacks**, primarily those that were not deterred, but could include attempts at attacks. Detection is crucial to any other security measures since if an attack is not recognized, little can be done to prevent it. Intrusion detection capabilities can play a large role in this effort.
- **Assessment of attacks**, to determine the nature and severity of the attack. For instance, is the entry of a number of wrong passwords just someone forgetting or is it a deliberate attempt by an attacker to guess some likely passwords?
- **Communication and notification**, so that the appropriate authorities and/or computer systems can be made aware of the security attack in a timely manner. Network and system management can play a large role in this effort.
- **Response to attacks**, which includes actions by the appropriate authorities and computer systems to mitigate the effect of the attack in a timely manner. This response can then deter or delay a subsequent attack.

1.5 Security Layers and Levels – Defense in Depth

Security is best applied in layers, with one or more security measures focused on one or more of the security purposes described in the previous section. This is often referred to as "defense in depth".

Defense in depth is a critical concept. If one security barrier is broken (for instance the lock on a door), the next layer may prevent the attack (the attacker does not have the correct password). Or it may just deter the attack until the attack is detected (such as video surveillance or an alarm notifies personnel that an excess of passwords have been attempted). Or it may detect the attack and allow responses to the attack to get into place (such as locking down all access to the attacked facilities).

Because of the large variety of communication methods and performance characteristics, as well as because no single security measure can counter all types of threats, it is expected than multiple levels of security measures will be implemented. For instance, VPNs only secure the transport level protocols, but do not secure the application level protocols.

1.6 End-to-End Security for Information Exchanges

Security of information exchanges implies end-to-end security from the sender of the information all the way across through all intermediate paths to the final receiver of the information. Thus information security must address not only fixed assets but also the virtual paths from end to end. This end-to-end aspect of security makes it far more difficult to assess the risks – threats, vulnerabilities, and impacts – as well as to determine the most appropriate security solutions.

1.7 Security Domains

One method for managing the complexity of security is to define physical and/or virtual security domains. The perimeter of each security domain is maintained at the desired level of security, while within each security domain is the same level of trust. Any information exchanges (including humans) crossing the perimeter are validated to the security level requirements within the security domain before they are allowed to enter. For instance, visitors are checked in at front desks and given passes requiring that they be escorted at all times. Or data entering a virtual security domain must go through a firewall for authentication.

1.8 Cross-Organizational Chain of Trust

One of the real challenges in security is the transition between security domains or across different organizations. How can a chain of trust be achieved as a person or information crosses between domains? How can information be passed from a highly secure domain through a low-level security domain to another high-level domain – without impacting efficiency or becoming security-caused “denial of service” attacks?

A major aspect of chain-of-trust is the implementation of systems – are the hardware components from trusted sources? Is the software to be trusted? Has it been adequately tested not only for functionality but also for hidden security vulnerabilities (e.g. buffer overflow conditions or Trojan horse viruses)? Who is establishing access permissions?

2. General Cyber Security Issues

2.1 How Much Security Is Required?

Cyber security must **balance** the **cost** of implementing security measures against the **likelihood** and **impact** of any security breaches. This balancing of cost vs. impact must take into account that excessive costs could impact customer rates, but that inadequate security measures could allow unnecessary power outages to those same customers. The cost/impact balancing also must recognize that no single security measure is 100% effective in preventing a security breach – and that security breaches will inevitably occur. Therefore, layered security measures must be applied and methods must be developed so that if one security barrier fails, another is there to deter, detect, cope with, or at least create an audit trail for forensic analysis, possible legal actions, and future training.

Therefore, risk assessment is crucial to determining the appropriate levels of security – "*The punishment must fit the crime*", or in this case "*The cost of preventing or coping with security breaches must fit the probable impacts resulting from those security breaches*".

2.2 Where Should Security be Applied?

The first step in determining a good cost/impact balance is to develop security requirements for all "cyber assets", where these assets can be defined as physical systems/equipment, stored cyber software and information, and the flows of information across interfaces between systems.

However, the security requirements for hardware and software are often easier to determine and to protect than those for the information flows across interfaces. For example, a thief can physically steal a laptop (or meter) with a sensitive database, but unless that thief can get the information out of the database, the database is worthless to him. On the other hand, if such a thief can eavesdrop on information being legitimately retrieved from the database by authorized personnel or an AMI application, then he is able to access that sensitive information.

Therefore the focus of cyber security requirements is not only on equipment and systems, but predominantly on the interfaces to and between systems.

3. Special Cyber Security Issues for the Smart Grid

3.1 Key Cyber Security Purposes for the Smart Grid

In the Smart Grid, there are two key purposes for cyber security:

- **Power system reliability**: Keep electricity flowing to customers, businesses, and industry. For decades, the power system industry has been developing extensive and sophisticated systems and equipment to avoid or shorten power system outages. In fact, power system operations have been termed the largest and most complex machine in the world. Although there are definitely new areas of cyber security concerns for power system reliability as technology opens new opportunities and challenges, nonetheless, the existing energy management systems and equipment, possibly enhanced and expanded, should remain as key cyber security solutions.
- **Confidentiality and privacy of customers**: As the Smart Grid reaches into homes and businesses, and as customers increasingly participate in managing their energy, confidentiality and privacy of their information has increasingly become a concern. Unlike power system reliability, customer privacy is a new issue.

3.2 Differences between "Corporate" Security and "Smart Grid" Security

Security requirements for the information infrastructure of the Smart Grid are similar but nonetheless significantly different from typical corporate information security requirements. While the security requirements of back office and corporate systems can be identified through assessments similar to those described in FIPS-199, power system operations of the Smart Grid are more closely aligned with Industrial Control Systems as described in NIST SP800-82. On the other hand, customer interactions with utilities and third parties include mixtures of power system operational information with high reliability and availability requirements and highly sensitive personal information with high confidentiality requirements. Compounding these mixtures is the widespread nature of the interactions across completely untrustable environments.

In addition, security requirements for corporate systems typically take the worst case ("high water mark") for determining the level of security (see FIPS-199), but this simple approach is often not feasible for control systems where system performance, time-critical interactions, communication media bandwidth constraints, field equipment resource constraints, and change management introduce considerable challenges to implement some of the security measures (see NIST SP800-82).

3.3 Critical Issues for the Security Requirements of Power Systems

Power system operations pose many security challenges that are different from most other industries. For instance, most security measures were developed to counter hackers on the Internet. The Internet environment is vastly different from the power system operations environment. Therefore, in the security industry there is typically a lack of understanding of the security requirements and the potential impact of security measures on the communication requirements of power system operations.

In particular, the security services and technologies have been developed primarily for industries that do not have many of the strict performance and reliability requirements that are needed by power system operations. For instance:

- Operation of the power system must continue 24x7 with high availability (e.g. 99.99% for SCADA and higher for protective relaying) regardless of any compromise in security or the implementation of security measures which hinder normal or emergency power system operations.
- Power system operations must be able to continue during any security attack or compromise (as much as possible).
- Power system operations must recover quickly after a security attack or compromised information system.
- The complex and many-fold interfaces and interactions across this largest machine of the world – the power system – makes security particularly difficult since it is not easy to separate the automation and control systems into distinct "security domains". And yet end-to-end security is critical.
- There is not a one-size-fits-all set of security practices for any particular system or for any particular power system environment.
- Testing of security measures cannot be allowed to impact power system operations.
- Balance is needed between security measures and power system operational requirements. Absolute security may be achievable, but is undesirable because of the loss of functionality that would be necessary to achieve this near perfect state.

- Balance is also needed between risk and the cost of implementing the security measures.

3.4 How Can Security Requirements for Smart Grid Interfaces be Determined?

There is no single set of cyber security requirements and solutions that fits each of the Smart Grid interfaces. Cyber security solutions must ultimately be implementation-specific, driven by the configurations, the actual applications, and the varying requirements for security of all of the functions in the system. ***That said, "typical" security requirements can be developed for different types of interfaces which can then be used as checklists or guidelines for actual implementations.***

Typically, security requirements address the integrity, confidentiality, and availability of data. However, in the Smart Grid, the complexity of stakeholders, systems, devices, networks, and environments precludes simple or one-size-fits-all security solutions. Therefore, additional criteria must be used in determining the cyber security requirements before selecting the cyber security measures. These additional criteria must take into account the characteristics of the interface, including the constraints and issues posed by device and network technologies, the existence of legacy systems, varying organizational structures, regulatory and legal policies, and cost criteria.

Once these interface characteristics are applied, then cyber security requirements can be applied that are both specific enough to be applicable to the interfaces, while general enough to permit the implementation of different cyber security solutions that meet the cyber security requirements or embrace new security technologies as they are developed. This cyber security information can then be used in subsequent steps to select cyber security controls for the Smart Grid.

3.5 Can Existing and/or Expanded Power System Management Capabilities Be Used for Security Management?

Yes, power system operations have been managing the reliability of the power grid for decades in which "Availability of Power" has been a major requirement, with the "Integrity of Information" as a secondary but increasingly critical, requirement. "Confidentiality of Customer Information" has also been vitally important in the normal revenue billing processes. Although focused on inadvertent security problems, such as equipment failures, careless employees, and natural disasters, many of the methods, technologies, and mindsets can be expanded to cover deliberate security attacks as well.

So, one of the most powerful security solutions is to utilize and expand existing power system management technologies to provide additional security measures. After all, these power system management technologies (e.g. SCADA systems, Energy Management Systems, Distributed Control Systems, Contingency Analysis applications, Fault Location, Isolation, and Restoration functions, as well as Revenue Protection capabilities) have been refined for years to cope with the ever-increasing reliability requirements and complexity of power system operations, and are designed to detect anomalous events, notify the appropriate personnel or systems, cope during a problem, take remedial actions, and log all events with very accurate timestamps.

In the past, there has been little need for distribution management except possibly some load shedding to avoid serious problems. In the future, with generation, storage, and load on the distribution grid, utilities will need to implement more sophisticated power-flow-based applications to "manage" the distribution grid. AMI systems can also be used to provide energy-related information and act as secondary sources of information These same capabilities could be designed to help manage security as well.

Metering has also addressed concerns about revenue protection and customer confidentiality for many years, although the advent of smart meters has expanded those concerns to a significant degree. However, many of the same concepts of revenue protection could also be used for the smart grid.

In fact, expanding existing power system management capabilities to cover specific security requirements, such as power system reliability, should be a major security requirement.

3.6 Cyber Security: Implementation Driven

Cyber security solutions must ultimately be implementation-specific, driven by the requirements for security of all of the functions in the system. However, "typical" security requirements can be developed and used as checklists for actual implementations.

In corporate settings, security requirements address the confidentiality, integrity, and availability of data using "Information Technology (IT)" security solutions such as cryptography, certificates, and physical access control. However, in the Smart Grid, the complexity of stakeholders, systems, devices, networks, and environments precludes just IT security techniques or one-size-fits-all security solutions. Therefore, additional criteria must be used in selecting the cyber security measures. These additional criteria must take into account the constraints posed by device and network technologies, legacy systems, organizational structures, regulatory and legal policies, and cost criteria. They should also take advantage of the existence of sophisticated equipment and systems that are already being used in the power system industry.

3.7 Examples of Using Power System Management for Security Management

Examples of using power system management systems and methods for Smart Grid cyber security include:

- **Utilize normal SCADA capabilities**, such as alarm handling, integrity scans, communications monitoring, data entry validation, etc., to detect and log equipment failures, communication failures, invalid data, and other (typically inadvertent) security compromises.
- **Utilize and expand existing SCADA systems** to monitor additional security-related points, such as opening doors and gates, status of IEC equipment (such as loss of power, processor restarts, application crashes, etc.), status of networks (unexpected requests, traffic anomalies, availability performance) in additional to the normal communications notifications of permanent failures.
- **Extend typical Area of Responsibility (AoR) SCADA capabilities to Role-Based Access Control**, to tighten permissions, log all invalid access events, and identify not only roles but individuals.

- **Expand transmission and sub-transmission power-flow analysis** to identify anomalous power system behavior such as unexpected shifts of load and generation patterns, unexpected state estimation mismatches between monitored data and estimated data, and abnormal power flow contingency analysis results to identify unexpected situations.
- **Design and/or expand the Distribution Management System** to include judiciously selected power system information from the AMI system, such as local loads, DER generation, voltage levels, etc. The DMS should also receive any demand response signals and load control signals and/or "expected customer-side response schedules" resulting from these signals. Using all of this information DMS power flow applications such as distribution contingency analysis can then assess both normal and abnormal situations (due to inadvertent as well as deliberate security events).
- **Expand distribution management of customer-based DER generation and storage** to ensure not only protection against security threats, but also just to maintain current power system reliability, given the rapidly expanding implementation of DER equipment at customer sites and the fact that the distribution system has not been designed to handle either the variability of renewables as well as possible back-flow of generation.
- **Expand normal revenue protection assessment** of individual metering information to include possible tampering of multiple meters, such as failed logins to multiple meters, similar events across multiple meters (e.g. multiple unsolicited remote disconnects), unexpected restarts of multiple meters, and other patterns not normally expected.
- **Expand and tighten the normal Role-Based Access Control (RBAC)** capabilities (used in SCADA systems to split operational responsibilities and capabilities) to cover more users (human and software application), and to include the security principle of "least privilege", which provides a user with only the minimum privileges on each resource that they need to accomplish their authorized required activities.
- **Validate as reasonable all data entries and modifications** from a power system perspective, as well as authenticated as made by an authorized user.
- **Expand information alarm and event logs** not only of power system events but also of information infrastructure events and specific security events, with timestamps of the appropriate accuracy and resolution.
- **Notify a "security" operator** in addition to the power system operator of anomalous events resulting from power system management tools.

Therefore, normal and expanded power system management technologies and procedures should be seen as very valid components of security solutions. ***In fact, requiring the expanded use of these power management technologies to address security requirements may become one of the most powerful solutions to security management for power system reliability.***