ELECTRIC POWER
RESEARCH INSTITUTE

Cyber Security Strategy Guidance for the Electric Sector

1025672

Cyber Security Strategy Guidance for the Electric Sector

1025672

Technical Update, May 2012

EPRI Project Manager

A. Lee

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 □PO Box 10412, Palo Alto, California 94303-0813 □USA
800.313.3774 □650.855.2121 □askepri@epri.com □www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

THE FOLLOWING ORGANIZATION PREPARED THIS REPORT:

Electric Power Research Institute (EPRI)

This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGMENTS

The following organization prepared this report:

Electric Power Research Institute (EPRI)
3420 Hillview Avenue
Palo Alto, California 94304-1338

Principal Investigator
A. Lee

This report describes research sponsored by EPRI.

Some of the material included in this technical update is based on several documents, for example, the National Institute of Standards and Technology Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*, August 2010; the U.S. Department of Energy (DOE), *Electricity Subsector Cybersecurity Risk Management Process*, DRAFT, March 2012; and the *Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector*, September 4, 2009. EPRI acknowledges the dedication and technical expertise of all the individuals who participated in the development of these documents.

This publication is a corporate document that should be cited in the literature in the following manner:

Cyber Security Strategy Guidance for the Electric Sector. EPRI, Palo Alto, CA: 2012. 1025672.

ABSTRACT

Smart grid technologies are introducing millions of new intelligent components to the electric grid that communicate in much more advanced ways (two-way communication, dynamic optimization, and wired and wireless communications) than in the past. Cyber security is important because the bi-directional flow of two-way communication and the control capabilities in the smart grid will enable an array of new functionalities and applications. Two areas of critical importance for the smart grid are cyber security and privacy.

This technical update provides guidance to utilities on developing an overall cyber security strategy, developing a risk management process (including a risk assessment process), and selecting and tailoring cyber security requirements for the electric sector. The National Institute of Standards and Technology Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*, is referenced along with other source documents and approaches. The goal is to provide practical guidance to an organization.

Keywords

Cyber security
Cyber security guidance
Cyber security risk assessment
NISTIR 7628
Security requirements

CONTENTS

LIST OF FIGURES

1
BACKGROUND

Smart grid technologies are introducing millions of new intelligent components to the electric grid that communicate in much more advanced ways (two-way communications, dynamic optimization, and wired and wireless communications) than in the past. Cyber security is important because the bi-directional flow of two-way communication and control capabilities in the smart grid that will enable an array of new functionalities and applications. Two areas of critical importance for the smart grid are *cyber security* and *privacy*. Figure 1-1 below illustrates this new modernized grid.

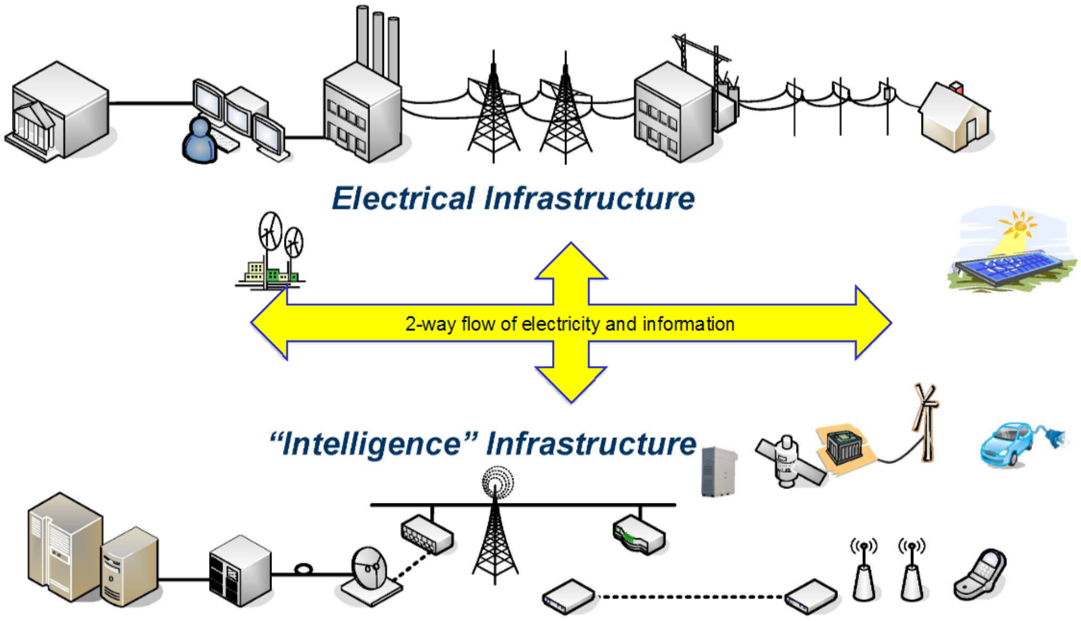

Electrical Infrastructure
2-way flow of electricity and information
"Intelligence" Infrastructure

Figure 1-1
Smart Grid = Electric Infrastructure + Intelligence

A second important change is the interconnectedness of the domains of the smart grid. The conceptual model in Figure 1-2 below provides a high-level, overarching view of some of the major relationships across the smart grid domains: markets, operations, service providers, bulk generation, transmission, distribution, and customer. The conceptual model includes potential communication paths and intra- and inter- domain interactions.

Another change is the interconnections of systems across organizations, for different purposes such as the export/import of electricity, providing situational awareness data, and receiving market data.

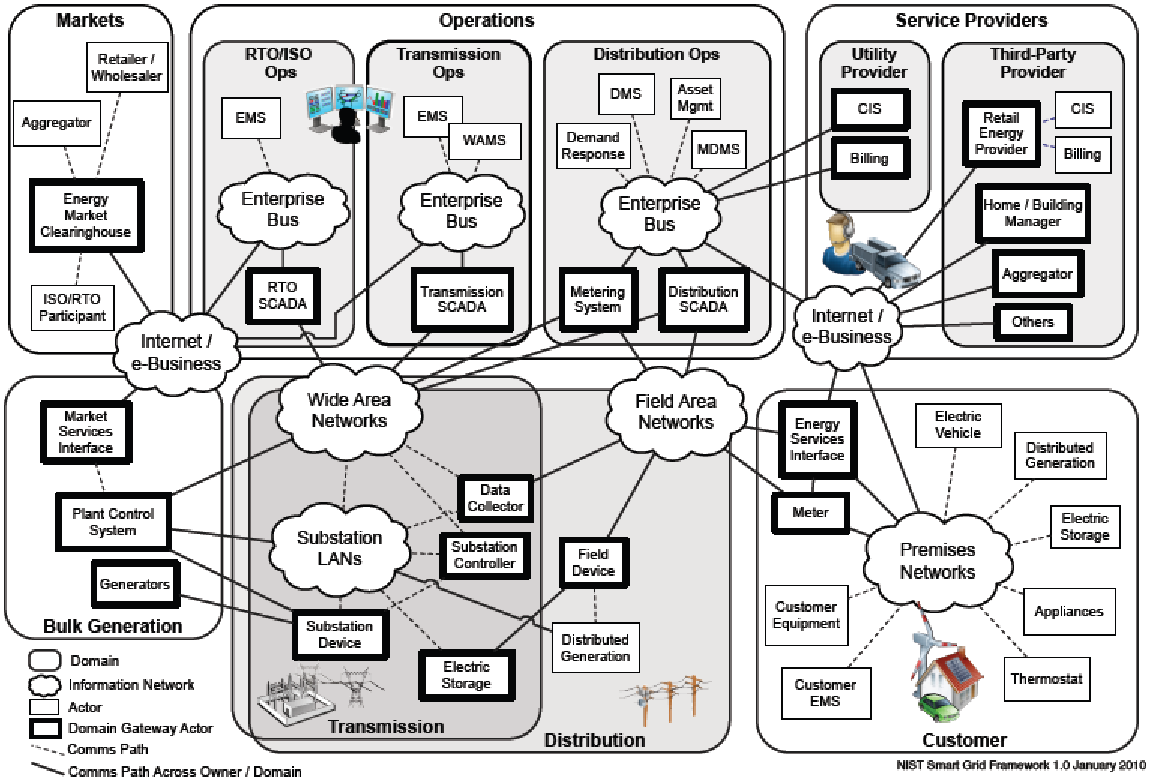


Figure 1-2
Conceptual Reference Diagram for Smart Grid Information Networks

For each utility, the modernization of the electric grid will take many years, possibly decades to complete. Throughout this long transition period, legacy equipment will be operated in conjunction with new equipment. In the current grid environment, the legacy Supervisory Control and Data Acquisition (SCADA) systems may have limited or no cyber security controls in place. The North American Electric Reliability Corporation (NERC) has developed a set of Critical Infrastructure Protection (CIP) standards. However, these standards are only applicable to the bulk power system critical assets and critical cyber assets.

1.1 Threats to the Grid

There are many cyber security threats to the existing grid and the developing smart grid, for example, disgruntled employees, unfriendly states, organized crime, and terrorists may launch deliberate attacks. There are also non-malicious cyber security events, such as equipment failure and user/administrator errors. Currently, the majority of cyber security events are non-malicious. Finally, cyber security events may be a result of natural phenomena such as hurricanes, tornados, floods, and solar activity. Regardless of the source of the cyber security event, the impact is often the same.

Figure 1-3 below illustrates the paths that malicious and/or non-malicious individuals may take to affect a cyber security event. The control systems may be accessed directly or through corporate systems. An organized attacker, such as one financed by a nation state, may have significant technical expertise and resources to implement a cyber attack. Alternatively, an individual who acquires knowledge from web sites may launch a cyber security attack. In either scenario, the intended result is the same, a cyber attack against the electric grid.

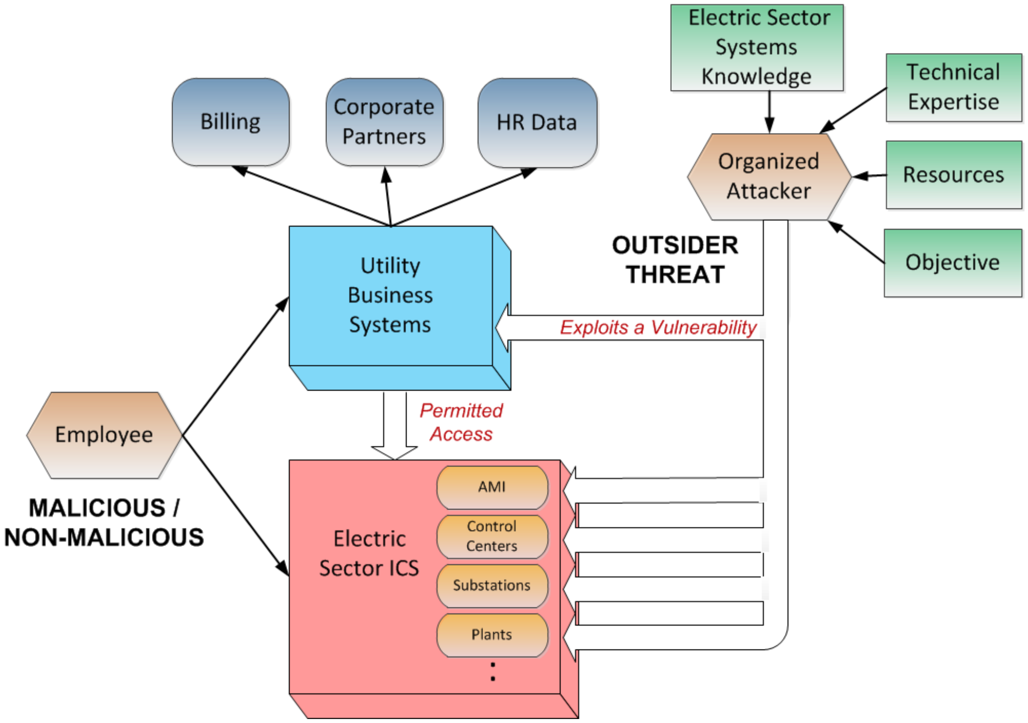


Figure 1-3
Anatomy of Threat Activity

Guidelines for Smart Grid Cyber Security

The three-volume report, National Institute of Standards and Technology Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*, August 2010, is for individuals and utilities that will be addressing cyber security for all smart grid systems in all operational domains – generation, transmission, and distribution. The NISTIR 7628 includes an approach for identifying cyber security threats and risks and selecting and tailoring cyber security requirements. Such an approach recognizes that the electric grid is changing from a relatively closed system to a complex, highly interconnected environment. Each utility's implementation of cyber security requirements should evolve as a result of changes in technology and systems, new threats, as well as changes in techniques used by adversaries. Approaches to securing these cyber technologies must be designed and implemented early in the transition to the smart grid. That is, cyber security should be "built-in" to each system.

The first volume of the NISTIR 7628 describes a cyber security strategy, including a risk assessment process, used to identify high-level security requirements. The volume also presents a high-level architecture followed by a logical reference model used to identify and define categories of logical interfaces within and across the seven domains included in Figure 1-2 above. High-level security requirements for each of the 22 logical interface categories are then described. The first volume concludes with a discussion of technical cryptographic and key management issues across the scope of smart grid systems and devices.

The second volume is focused on privacy issues within personal dwellings. It provides awareness and discussion of such topics as evolving smart grid technologies and associated new types of information related to individuals, groups of individuals, and their behavior within their premises. Additionally, the second volume provides recommendations, based on widely accepted privacy principles, for entities that participate within the smart grid.

The third volume is a compilation of supporting analyses and references used to develop the high-level security requirements. These include classes of vulnerabilities and a discussion of the bottom-up security analysis that was conducted while developing the NISTIR 7628. The vulnerability class list was created from many sources of vulnerability information, such as, the NIST Special Publication 800-82, *Guide to Industrial Control Systems Security,* and NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*, Open Web Application Security Project (OWASP) vulnerabilities, the National Vulnerability Database Common Weakness Enumeration (CWE) vulnerabilities, and the documentation from the Idaho National Laboratory (INL). The goal of the bottom-up analysis was to identify specific protocols, interfaces, applications, best practices, etc. that should be developed to solve specific smart grid cyber security problems. The approach taken was to perform the analysis from the bottom-up; that is, to identify specific problems and issues that needed to be addressed but not to perform a comprehensive gap analysis that covers all issues. Included below are two vulnerability class examples and one bottom-up example from the NISTIR 7628.

7.2 People, Policy, and Procedures

7.2.1 Training

7.2.1.1 Inadequate Security Training and Awareness Program

Description
An adequate security awareness program is a key element of an organization’s policy framework to guard against vulnerabilities introduced by insufficiently trained personnel. Such programs highlight the need for a continuous retraining effort over some identified period of time. The security profile will always be changing and so will the need for new procedures, new technologies, and reinforcement of the importance of the cyber security program.

Examples

- Inappropriate use of network connectivity, such as multi-homing.

7.4 Platform Vulnerabilities

7.4.1 Design

7.4.11 Use of Inadequate Security Architectures and Designs

Description
Development schedule pressures and lack of security training can lead to the use of inadequate security architectures and designs. This includes reliance on in-house security solutions, security through obscurity, and other insecure design practices.

Examples

- Security design by untrained engineers,
- Reliance on non-standard techniques and unproven algorithms, and
- Security through obscurity.

> ## 8.2 Evident and Specific Cyber Security Problems
>
> *This subsection documents specific cyber security problems in the Smart Grid in so far as possible by describing actual field cases that explain exactly the operational, system, and device issues.*
>
> *8.2.20 Event Logs and Forensics*
>
> Timestamps in event logs must be based on accurate time sources so that logs from different systems and locations can be correlated to reconstruct historical sequences of events. This applies both to logs of power data and to logs of cyber security events. Correlating power data from different locations can lead to an understanding of disturbances and anomalies—and difficulties in correlating logs was a major issue in investigating the August 14, 2003 blackout. Correlating cyber security events from different systems is essential to forensic analysis to determine if and how a security breach occurred and to support prosecution.

1.1.1 Purpose of this Technical Update

The purpose of this document is to provide guidance to utilities on developing an overall cyber security strategy, a risk management process (including a risk assessment process), and selecting and tailoring cyber security requirements for the electric sector. The NISTIR 7628 is referenced along with other source documents and approaches. The goal is to provide practical guidance to an organization.

The NISTIR 7628 is a guidance document and is not a mandatory standard. The document may be used as a starting point for selecting and modifying security requirements. Additional criteria must be used in determining the applicable cyber security requirements before selecting and implementing the cyber security controls/solutions. These additional criteria include constraints and issues posed by device and network technologies, the existence of legacy components/devices, varying organizational structures, regulatory and legal policies, and cost criteria.

The comprehensive list of security requirements included in the NISTIR 7628 is an amalgam from several sources: NIST SP 800-53, the *DHS Catalog of Control Systems Security: Recommendations for Standards Developers*, the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Standards, and the Nuclear Energy Institute (NEI) Guidance. After the security requirements were selected, they were modified as required. The goal was to develop a set of cyber security requirements that address the needs of the electric sector and the smart grid.

2
CYBER SECURITY STRATEGY

To adequately address potential threats and vulnerabilities, cyber security must be included in all phases of the system development life cycle, from the design phase through implementation, operations and maintenance, and disposition/sunset and address prevention, detection, response, and recovery capabilities. Prevention is the first line of defense. Because cyber security prevention controls can be defeated, utilities have to be able to detect incidents, respond to mitigate damage, and recover systems and data in a timely manner. Figure 2-1 below illustrates these four capabilities and their relationship. The capabilities are not static, but are constantly assessed and revised to address evolving threats, vulnerabilities, and security incidents.

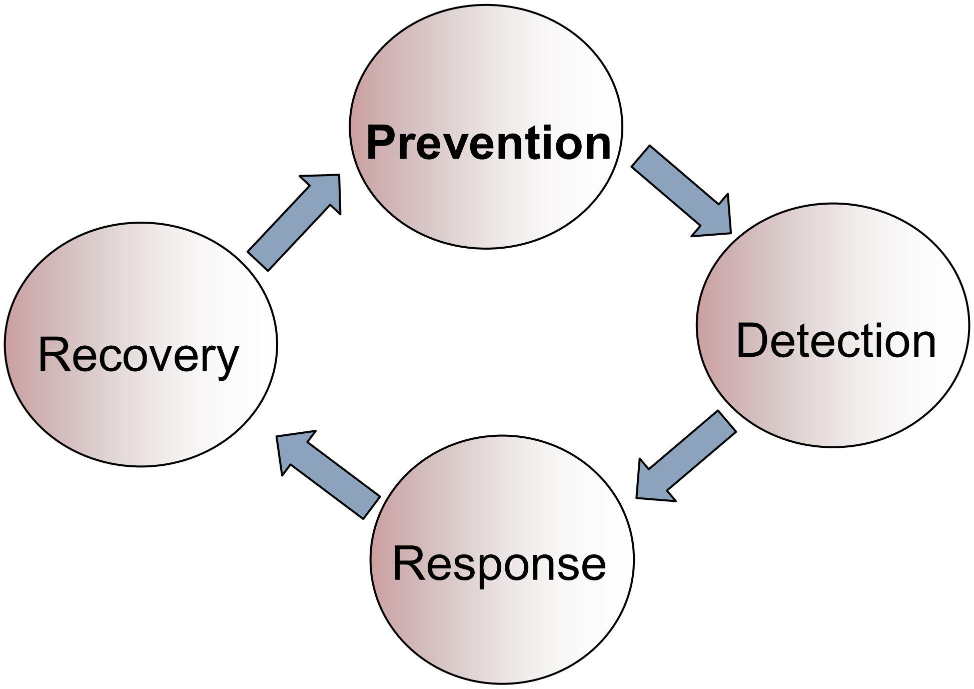


Figure 2-1
Cyber Security Capabilities

Cyber security must address not only deliberate attacks launched by disgruntled employees, agents of industrial espionage, and terrorists, but also inadvertent compromises due to user errors, equipment failures, and natural disasters.

An overall cyber security strategy includes both domain-specific and common requirements that are used when developing a risk mitigation strategy. *Risk* is the potential for an unwanted outcome (or impact) resulting from a cyber security incident, event, or occurrence.

The focus in the first phase of a cyber security strategy is to develop an overall cyber security risk management framework. Included in framework are risk assessment and the selection and tailoring of cyber security requirements and measures/controls. All of these are discussed in this document.

2.1 Cyber Security Risk Management Framework

Typically, a cyber security risk management framework at the organization level is a high level framework that is common across the organization. This framework may be tailored at lower levels in an organization such as for business and operational components. Included below are two high-level risk management/governance approaches – one developed for the European Commission and one developed for the United States. Although the specific phase names are different across the two frameworks, the phases are similar.

2.1.1 European Union (EU) Risk Governance Framework[1]

Figure 2-2 below illustrates the EU Framework and the phases are defined below.

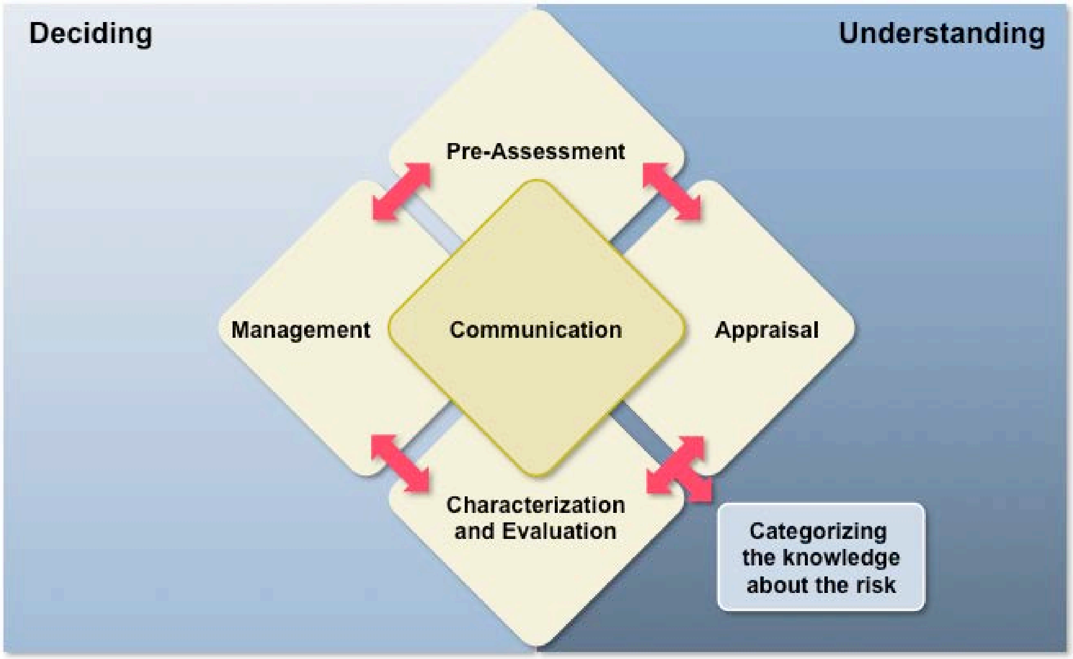

Deciding
Understanding
Pre-Assessment
Management
Communication
Appraisal
Characterization and Evaluation
Categorizing the knowledge about the risk

Figure 2-2
EU Risk Governance Framework

As stated in the introduction to the Framework:

> "The primary purpose of this Risk Governance Framework is therefore to focus on the decision making processes in [European Union] EU member states for dealing with the risk of disruption to cross-border energy supplies that can arise from [Information Communication Technology] ICT related incidents.
>
> The aim is to provide a consistent approach to decisions affecting the Energy-ICT interface, using best practice risk governance theory.

[1] Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector, Final Report to European Commission, AEA/ED05761/Issue 1, Directorate-General Justice, Freedom and Security, September 4, 2009.

> The Risk Governance Framework provides a standardized approach for quantifying and managing risks to cross-border energy supply. The framework defines a minimum standard to be achieved but must also allow flexibility in how it can be applied in each Member State and organization to fit local practice.
>
> It considers the energy supply chain from primary production through storage, transmission and distribution/transportation to metering and financial settlement.
>
> It considers threats arising from anywhere in the world that affect one or more industry participants operating within one or more Member States."

The activities in the process are divided into the following five phases as defined in the Framework:

- **Pre-assessment**: involves getting a broad picture of the risk. Early warning and "framing" the risk in order to provide a structured definition of the problem, of how it is framed by different stakeholders, and of how it may best be handled.

  Good risk governance starts with defining the scope of consideration and gathering information about stakeholders' responsibilities. This ensures that there is a common definition of the topics to be considered, and that all actors involved in the risk management process understand their role. Good preparation and definition makes for a more efficient risk management process.
- **Appraisal**: identifies the knowledge needed for judgment and decisions. Combining a scientific risk assessment (of the hazard and its probability) with a systematic concern assessment (of public concerns and perceptions) to provide the knowledge base for subsequent decisions.
- **Characterization and evaluation**: assesses whether the risk is acceptable or not. The data and a thorough understanding of societal values affected by the risk are used to evaluate the risk as acceptable, tolerable (requiring mitigation), or intolerable (unacceptable).

  Using the potential impact of risk events and the vulnerability of systems, the risk events can be placed on a risk tolerability matrix. This can be used to create a consistent and clear understanding of the types of risk events that are acceptable, tolerable and unacceptable.
- **Management**: identifies who needs to do what and when. Effective risk management requires the creation of a strategy, implementing the strategy through a plan of activities, and monitoring the effectiveness of the activities, so that the strategy can be reviewed and adapted if necessary.
- **Communication**: determines who needs to be told, when and how.

These phases can then be repeated to provide a basis for continual improvement.

2.1.2 DOE Cybersecurity Risk Management Process

The DOE risk management process was developed in conjunction with public and private partners[2]. Although the element names are different from those in the EU Risk Governance

[2] DRAFT: For public comment, *Electricity Subsector Cybersecurity Risk Management Process,* U.S. Department of Energy, March 2012.

Framework, the tasks are similar. *Frame* is comparable to Pre-Assessment, *Assess* is comparable to Appraisal, *Respond* is comparable to Characterization and Evaluation, and *Monitor* is comparable to Management. Figure 2-3 below illustrates the four phases of the DOE Cybersecurity Risk Management process.

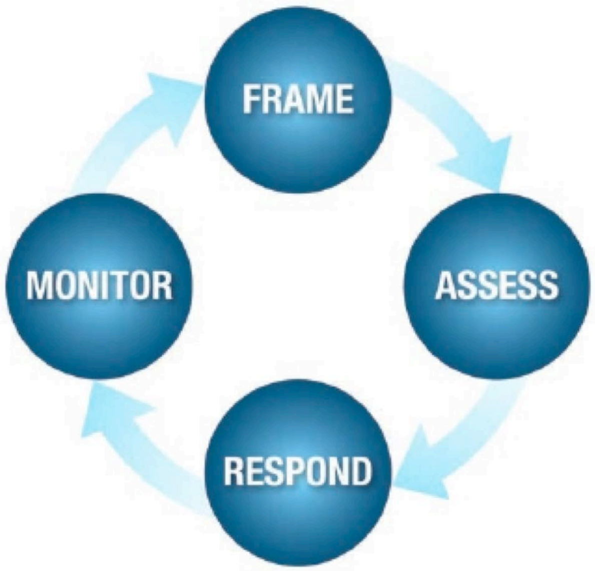


Figure 2-3
DOE Cybersecurity Risk Management Process

The following descriptions of the elements are based on the content of the DOE document.

Frame: describe the environment in which cyber security risk-based decisions are made. Establishing a realistic cyber security risk frame requires a utility to identify:

- Assumptions about threats, vulnerabilities, consequences, impacts, and likelihood of occurrence;
- Constraints imposed by legislation and regulation; resource constraints (time, money, and people); and other factors identified by the utility;
- Cyber security risk tolerance that identifies the level of acceptable risk; and
- Cyber security priority within mission and business processes and other types of risk (e.g., investment, budgetary, program management, legal liability, safety, and inventory risk).

Assess: a utility identifies the following components of cyber security risk and evaluates them for each identified system. The output from the framing element should be used as a starting point for this element.

- Threats (to operations, assets, and/or individuals);
- Vulnerabilities (to operations, assets, and/or individuals);
- Impact (consequence); and
- Likelihood (probability or frequency an event will occur).

To support the risk assessment element, a utility identifies:

- Tools, techniques, and methodologies that they will use to assess risk;
- Roles and responsibilities related to risk assessment; and
- Risk assessment information to be collected, processed, and communicated.

Respond: address how a utility responds to potential cyber security threats and vulnerabilities once they are assessed. The risk response element should be consistent within a utility at a high level, with specific variations for critical systems. In this element, a utility:

- Develops alternative courses of action (accept, avoid, mitigate, share, or transfer) for responding to risk;
- Evaluates the alternative courses of action;
- Determines appropriate courses of action consistent with the utility's risk tolerance level; and
- Implements courses of action.

Certain cyber security measures/controls may not be feasible to implement or are cost prohibitive. This may require implementation of compensating controls.

Monitor: address how risks are monitored and communicated over time in a utility. During the risk monitoring element, a utility:

- Verifies that cyber security measures/controls are implemented and that the cybersecurity requirements derived from the risk management strategy are satisfied;
- Evaluates the ongoing effectiveness of cyber security measures/controls;
- Identifies changes, including new threats and vulnerabilities, that may impact risk; and
- Defines the ongoing monitoring process to assess the effectiveness of the cyber security measures/controls.

2.1.3 NISTIR 7628 Cyber Security Risk Management Strategy

The focus of the NISTIR 7628 is on a high-level risk assessment, logical architecture, and identification of high-level cyber security requirements. The goal is to provide guidance to utilities as they address cyber security for their smart grid systems. Figure 2-4 below illustrates the overall strategy described in the NISTIR 7628. Because the goal was to provide high-level guidance only, the last three steps (in italics) were not performed. The steps that were performed correspond to the first two phases of the EU risk governance framework; pre-assessment and appraisal and the corresponding elements in the DOE risk management process; frame and assess.

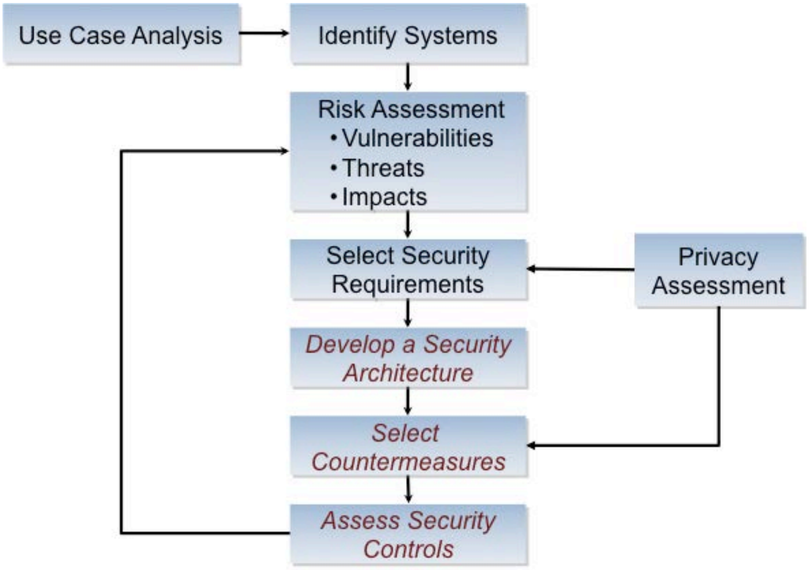


Figure 2-4
NISTIR 7628 Cyber Security Risk Management Strategy

TIPS:

1. There is no single cyber security risk management framework that is applicable to every utility and system. There are several high level frameworks that may be used.
2. The top-level cyber security risk management framework should be at a fairly high level, to limit the requirement for constantly updating the framework.
3. When selecting a cyber security risk management framework, start by reviewing what is currently available in the utility, typically for the IT and communication systems. It is much easier to apply and/or tailor an existing framework, than to develop one from the beginning.
4. Developing or tailoring a cyber security risk management framework and identifying systems requires time and patience.
5. To perform a risk assessment, each utility needs to identify the systems. The definition of a *system* is determined by the utility, but should consist of a common set of functions. In general, one system is too few and 2000 is probably too many. Defining a system is critical to the accuracy of the risk assessment, the definition of the security requirements, and the selection of cyber security controls/measures that address the identified vulnerabilities and threats.
6. Electric sector use cases are a valuable tool that may be used in documenting functionality and identifying systems. Typically these uses do not focus on cyber security. There are several thousand use cases available.
7. There is no single list of systems that is applicable across all utilities – each utility must develop its own list.
8. The phases in the framework may need to be repeated. For example, in identifying systems, a utility may realize that their initial list did not sufficiently differentiate the functionality.

2.1.4 Cyber Security Risk Assessment Process

One component of a cyber security risk management strategy is the cyber security risk assessment. This is referenced in both the EU and DOE risk management strategies discussed above. As stated above, cyber security risk is one component of organizational risk, which can include many types of risk (e.g., investment, budgetary, program management, legal liability, safety, and inventory risk, as well as the risk from information systems).

A cyber security risk assessment includes identifying assets, vulnerabilities, and threats and specifying impacts. The output is the basis for the selection of security requirements and subsequent risk-mitigation strategies (security measures/controls). As with any assessment, a realistic analysis of the impact of inadvertent errors, acts of nature, and malicious threats is critical.

In the NISTIR 7628, the high-level cyber security risk assessment was performed using electric sector use cases and a top-down analysis that analyzed the interfaces between components and between domains. The approach is illustrated in Figure 2-5 below.

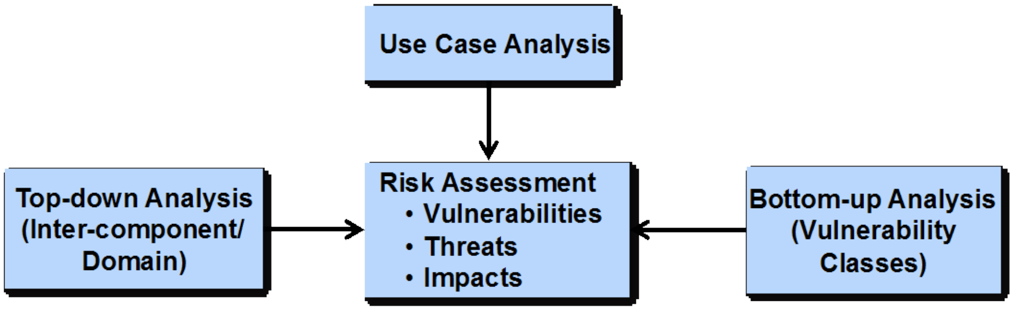

Use Case Analysis
Top-down Analysis (Inter-component/ Domain)
Risk Assessment
• Vulnerabilities
• Threats
• Impacts
Bottom-up Analysis (Vulnerability Classes)

Figure 2-5
NISTIR 7628 Risk Assessment Methodology

<u>TIPS:</u>

1. A cyber security risk assessment should be performed at several stages throughout a system life cycle. For example, an initial assessment is used as input for developing cyber security requirements in the design phase. This assessment will not be at a detailed level. In this initial cyber security risk assessment:
   a. Identify *all* systems and assets, not just the critical cyber assets
   b. Specify preliminary confidentiality, integrity, and availability impact levels for each <u>system</u> based on system criticality and identification of threats and vulnerabilities.
   c. A high in one security objective for a system does NOT mean that the overall impact level for the system must be high. Because the impact levels may not be the same, this will require additional analysis to address these differences.
2. Because the focus in the initial risk assessment is on developing security requirements, vulnerability identification will typically be at a high level corresponding to classes of devices/components.
3. There are two basic types of risk assessment – *qualitative* where the scoring may be low, moderate, and high and *quantitative* where the scoring may be 1-10. A utility should select the approach they believe will provide the most useful results.

Figure 2-6 is the high level “spaghetti diagram” that was developed for the NISTIR 7628. It includes all the domains and interfaces, but does not identify specific systems. That is the responsibility of each utility. This diagram and the security requirements may be used as a starting point for utilities.

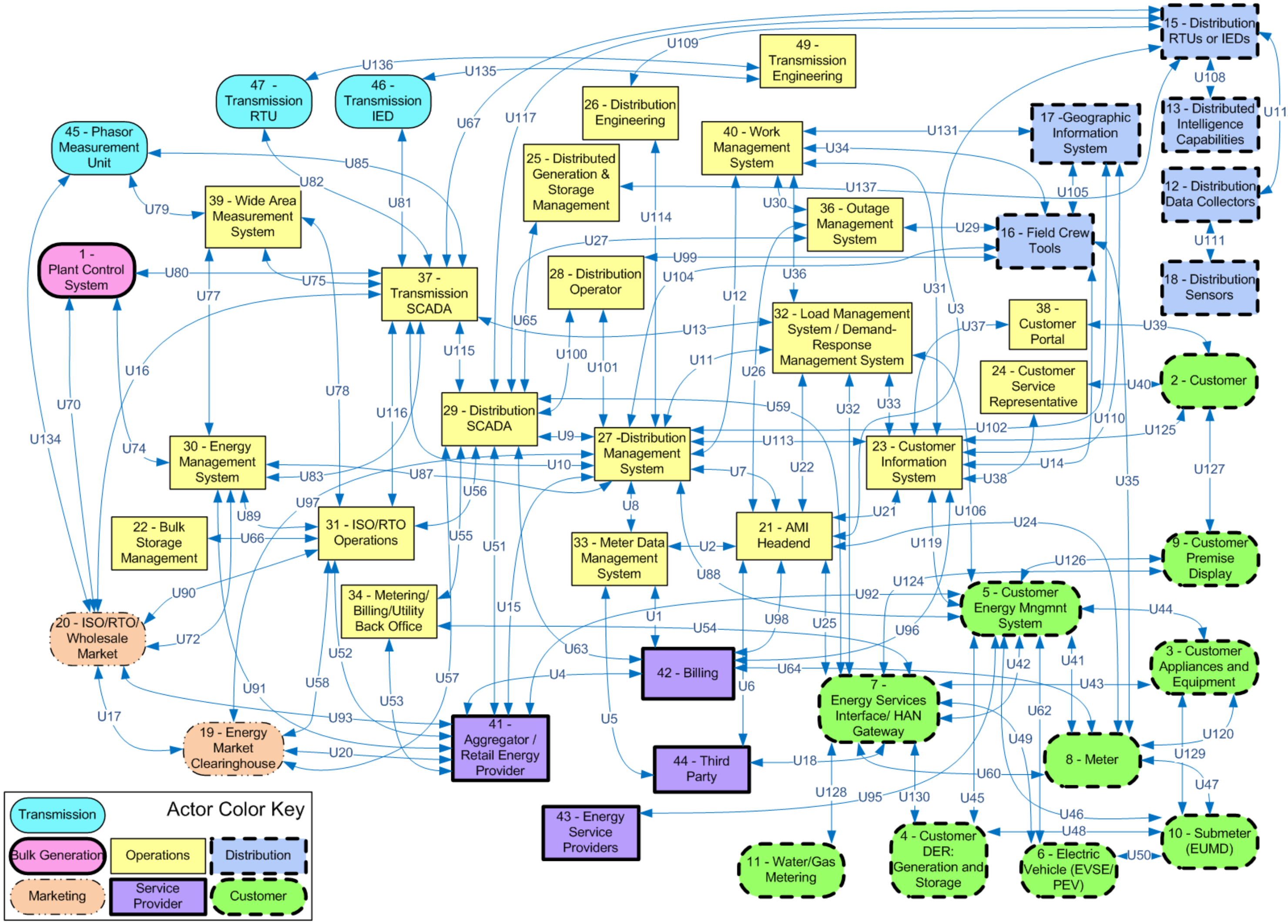

15 - Distribution RTUs or IEDs
49 - Transmission Engineering
47 - Transmission RTU
46 - Transmission IED
45 - Phasor Measurement Unit
26 - Distribution Engineering
40 - Work Management System
17 -Geographic Information System
13 - Distributed Intelligence Capabilities
25 - Distributed Generation & Storage Management
39 - Wide Area Measurement System
36 - Outage Management System
12 - Distribution Data Collectors
16 - Field Crew Tools
1 - Plant Control System
37 - Transmission SCADA
28 - Distribution Operator
18 - Distribution Sensors
32 - Load Management System / Demand-Response Management System
38 - Customer Portal
24 - Customer Service Representative
2 - Customer
29 - Distribution SCADA
27 -Distribution Management System
23 - Customer Information System
30 - Energy Management System
22 - Bulk Storage Management
31 - ISO/RTO Operations
33 - Meter Data Management System
21 - AMI Headend
9 - Customer Premise Display
5 - Customer Energy Mngmnt System
34 - Metering/ Billing/Utility Back Office
20 - ISO/RTO/ Wholesale Market
42 - Billing
3 - Customer Appliances and Equipment
7 - Energy Services Interface/ HAN Gateway
19 - Energy Market Clearinghouse
41 - Aggregator / Retail Energy Provider
8 - Meter
44 - Third Party
43 - Energy Service Providers
10 - Submeter (EUMD)
11 - Water/Gas Metering
4 - Customer DER: Generation and Storage
6 - Electric Vehicle (EVSE/ PEV)
U109
U136
U135
U108
U112
U67
U117
U131
U34
U85
U82
U137
U105
U79
U81
U114
U30
U29
U27
U111
U80
U75
U99
U104
U12
U36
U31
U77
U65
U3
U37
U39
U13
U115
U16
U100
U101
U11
U26
U70
U78
U116
U59
U32
U33
U40
U110
U134
U74
U102
U125
U9
U113
U10
U22
U14
U127
U83
U87
U7
U38
U35
U56
U8
U97
U89
U66
U21
U106
U24
U55
U51
U2
U119
U88
U126
U124
U90
U92
U15
U1
U54
U98
U25
U96
U44
U72
U63
U42
U41
U64
U4
U43
U6
U91
U58
U62
U17
U93
U5
U120
U53
U57
U49
U20
U18
U129
U60
U128
U95
U130
U45
U47
U46
U48
U50
Actor Color Key
Transmission
Bulk Generation
Operations
Distribution
Marketing
Service Provider
Customer

Figure 2-6
Logical Architecture Diagram for the Smart Grid from NISTIR 7628

The next step in the NISTIR 7628 process was to identify *logical interface categories* and determine the impact levels for the three objectives of confidentiality, integrity, and availability for each category. Each logical interface in the logical architecture diagram (the *spaghetti* diagram) 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 could be categorized together to simplify the identification of the appropriate security requirements. Also, it would have been very time consuming and complicate to allocate security requirements to over 130 logical interfaces. The logical interface categories were defined based on key attributes that include, for example, security objectives and operational constraints. The set of attributes allocated to each logical interface category is not intended to be a comprehensive set nor to exclude interfaces that do not include that attribute. Listed below are some of the attributes[3]:

- **Availability requirements**: Strong requirement that information should be available within appropriate time frames. Often this necessitates redundancy of equipment, communication paths, and or information sources.
- **Low bandwidth of communications channels**: Severely limited bandwidth may constrain the types of security technologies that should be used across an interface while still meeting that interface's performance requirements.
- **Legacy communication**: Older communication technologies may limit the types, thoroughness, or effectiveness of different security technologies that may be employed. This sensitivity to security technologies should be taken into account.
- **Legacy end-devices and systems protocols**: Older end-devices and protocols may constrain the types, thoroughness, or effectiveness of different security technologies that may be employed.
- **Insecure, untrusted locations**: Devices or systems in locations that cannot be made more secure due to their physical environment or ownership, pose additional security challenges.

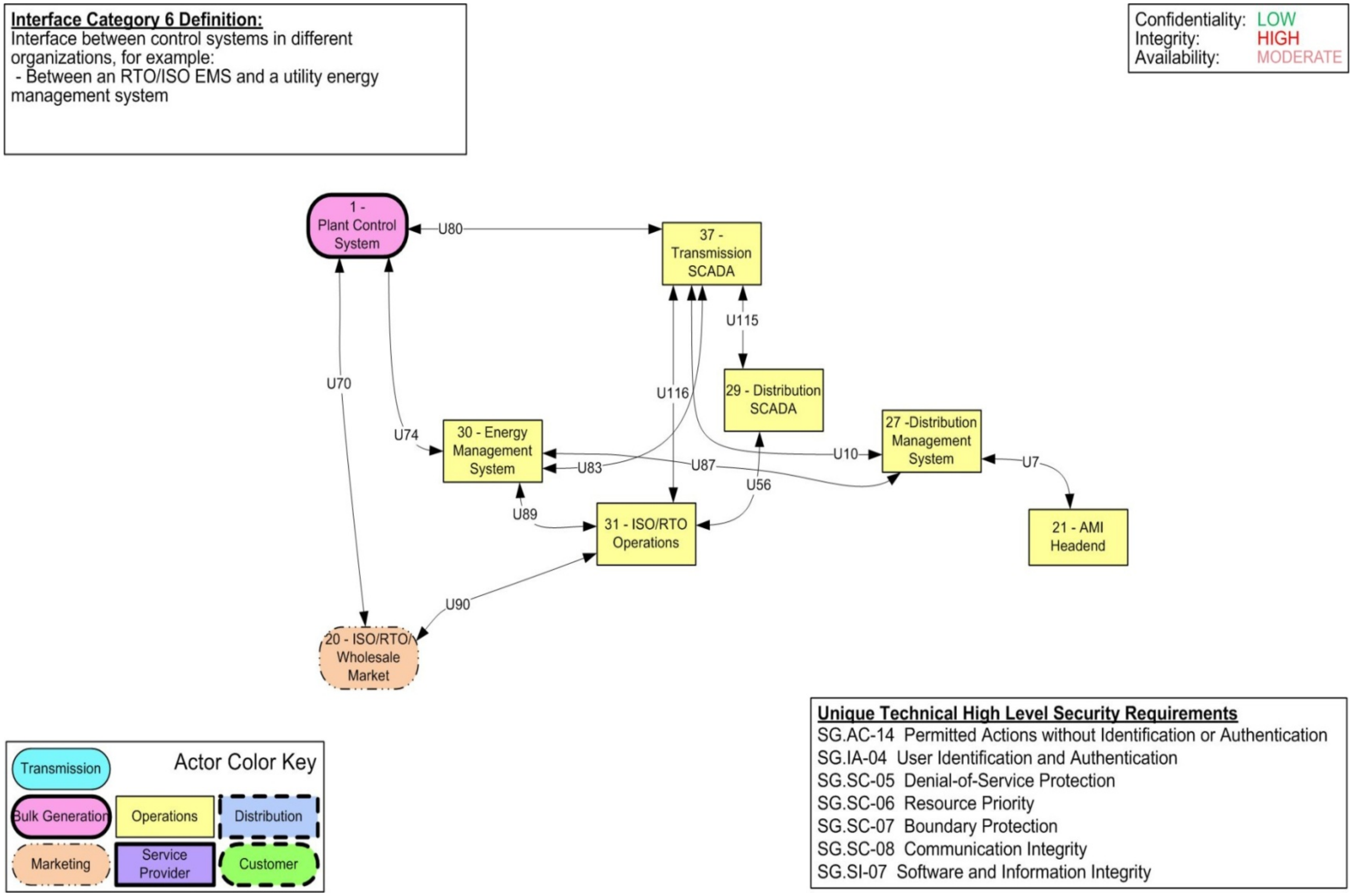
2.1.5 Specification of Cyber Security Requirements

Each security requirement in the NISTIR 7628 was then allocated to one or more logical interface categories. As noted above, the selection of security requirements was based on the attributes and impact levels for each logical interface category. Each security requirement is allocated to one of three categories: governance, risk, and compliance (GRC), common technical, or unique technical. The intent of the GRC requirements is to have them addressed at the organization level and tailored to specific systems, if required. The GRC and common technical requirements are applicable to *all* of the logical interface categories. The unique technical requirements are allocated to one or more of the logical interface categories.

After a utility identifies a system, the applicable logical interface categories and associated security requirements should be selected. This *baseline* needs to be assessed and tailored for the specific system.

Figure 2-7 is one of the logical interface categories from the NISTIR 7628 with the associated impact levels for confidentiality, integrity, and availability, and some of the unique technical requirements highlighted.

[3] The full set of attributes is included in Volume 3 of NISTIR 7628.



Interface Category 6 Definition:
Interface between control systems in different organizations, for example:
- Between an RTO/ISO EMS and a utility energy management system

Confidentiality: LOW
Integrity: HIGH
Availability: MODERATE

Unique Technical High Level Security Requirements
SG.AC-14 Permitted Actions without Identification or Authentication
SG.IA-04 User Identification and Authentication
SG.SC-05 Denial-of-Service Protection
SG.SC-06 Resource Priority
SG.SC-07 Boundary Protection
SG.SC-08 Communication Integrity
SG.SI-07 Software and Information Integrity

Figure 2-7
Logical Interface Category 6 – Interface Between Control Systems in Different Organizations

Each security requirement in the NISTIR 7628 includes the following information:

- A unique identifier and name
- Category: Governance, risk, and compliance (GRC); common technical; and unique technical
- Requirements language
- Supplemental guidance
- Requirement enhancements
- Additional consideration – these are not intended as security requirements
- Impact level – allocates the security and any requirement enhancements to the appropriate impact levels.

As listed above, there is a "base" requirement and requirement enhancements, as applicable, allocated at the different impact levels, e.g., low (L), moderate (M), or high (H). The security requirement may be the same at all impact levels. If there are additional requirements at the moderate and high impact levels, these are listed under requirement enhancements. Also, some security requirements may only be applicable at the moderate and/or high impact levels.

Following is an example of one of the security requirements from the NISTIR 7628:

SG.IA-5 Device Identification and Authentication

Category: Unique Technical Requirements

Requirement

The Smart Grid information system uniquely identifies and authenticates an organization-defined list of devices before establishing a connection.

Supplemental Guidance

The devices requiring unique identification and authentication may be defined by type, by specific device, or by a combination of type and device as deemed appropriate by the organization.

Requirement Enhancements

1. The Smart Grid information system authenticates devices before establishing remote network connections using bi-directional authentication between devices that is cryptographically based; and
2. The Smart Grid information system authenticates devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.

Additional Considerations

None.

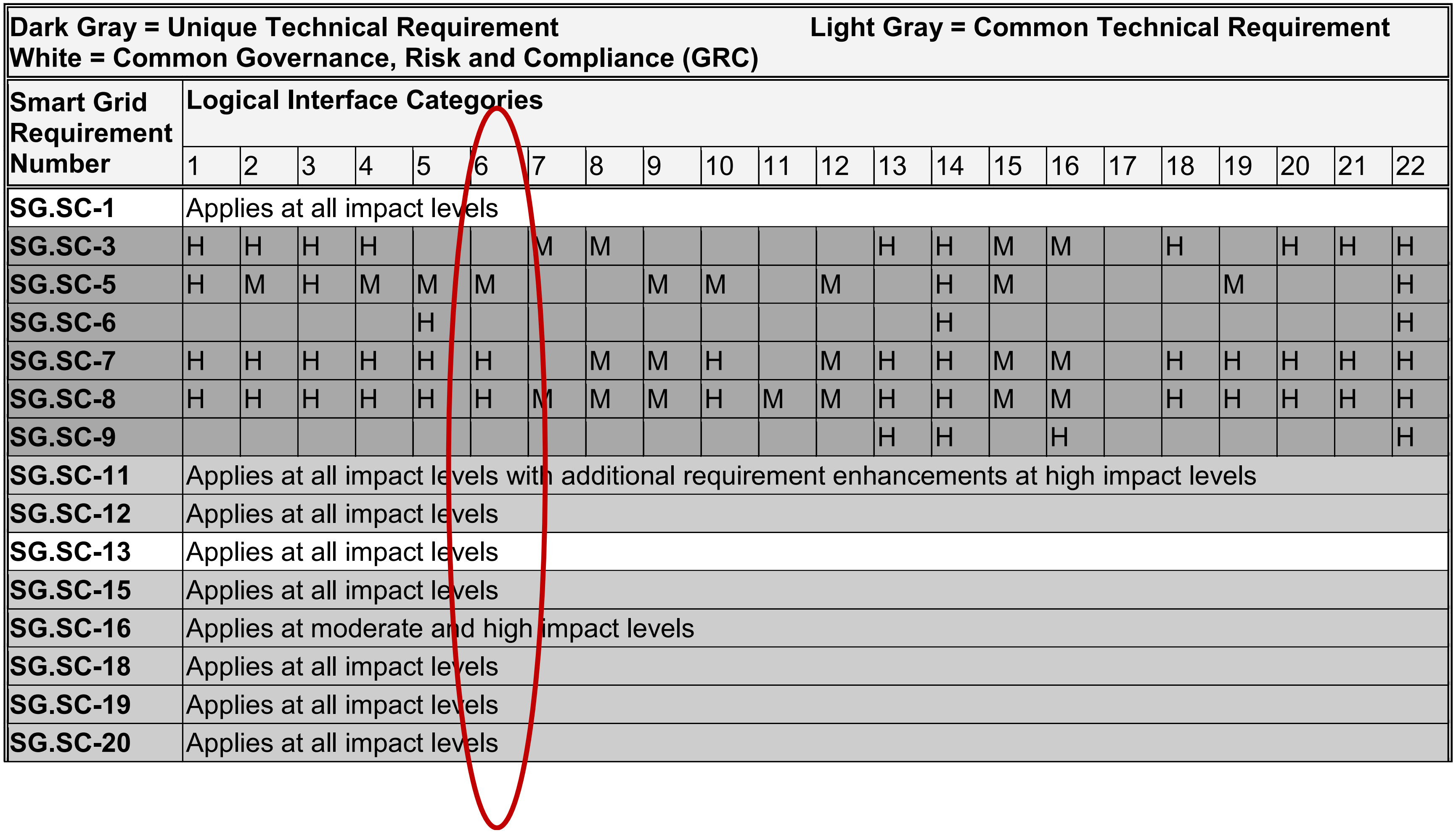
Impact Level Allocation

Low: Not Selected	Moderate: SG.IA-5 (1), (2)	High: SG.IA-5 (1), (2)

The following example illustrates the sequence of tasks from identifying the logical interface category to selecting and tailoring the security requirements.

Example: Control system XYZ: this system includes logical interface 6: *interface between control systems in different organizations* and requires high data accuracy and high availability.

- Figure 2-8 below identifies some of the security requirements from NISTIR 7628 for this logical interface category. Some of the applicable requirements are listed below and any changes that need to be made to address the specific requirements of the XYZ control system:
  - <u>GRC Requirements</u>
    - SG.SC-1, *Smart Grid Information System and Communication Protection Policy and Procedures* is applicable at the organization level for all systems and does not need to be revised.
  - <u>Common Technical Requirements</u>
    - SG.SC-11, Cryptographic Key Establishment and Management is applicable and does not need to be tailored.
    - SG.SC-19, Security Roles is applicable and needs to be tailored for the specific roles that are necessary for the XYZ control system.
  - <u>Unique Technical Requirements</u>
    - *SG.SC-5, Denial-of-Service Protection* is important to mitigate or limit the effects of denial-of-service attacks. The requirement needs to be tailored for the specific attacks that are applicable to the XYZ system. The requirement is the same at all three impact levels.
    - *SG.SC-7, Boundary Protection* is used to, for example, define the boundary of the system and monitor and control communications at the boundary. This requirement is uniquely applied to each system. At the moderate and high impact levels, there are requirement enhancements



Dark Gray = Unique Technical Requirement **Light Gray = Common Technical Requirement**
White = Common Governance, Risk and Compliance (GRC)

Smart Grid Requirement Number	**Logical Interface Categories**																					
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
SG.SC-1	Applies at all impact levels																					
SG.SC-3	H	H	H	H			M	M					H	H	M	M		H		H	H	H
SG.SC-5	H	M	H	M	M	M			M	M		M		H	M				M			H
SG.SC-6					H									H								H
SG.SC-7	H	H	H	H	H	H		M	M	H		M	H	H	M	M		H	H	H	H	H
SG.SC-8	H	H	H	H	H	H	M	M	M	H	M	M	H	H	M	M		H	H	H	H	H
SG.SC-9													H	H		H						H
SG.SC-11	Applies at all impact levels with additional requirement enhancements at high impact levels																					
SG.SC-12	Applies at all impact levels																					
SG.SC-13	Applies at all impact levels																					
SG.SC-15	Applies at all impact levels																					
SG.SC-16	Applies at moderate and high impact levels																					
SG.SC-18	Applies at all impact levels																					
SG.SC-19	Applies at all impact levels																					
SG.SC-20	Applies at all impact levels																					

Figure 2-8
Security Requirements for the Logical Interface Category 6 from the NISTIR 7628

TIPS:

1. Prioritize the security requirements and focus on the highest impact systems – no utility has unlimited resources to address all the security requirements.
2. There may be additional considerations when specifying security requirements at the system level. For example:
    a. There may be security requirements that supplement the device/component security requirements.
    b. Security requirements in one subsystem/component may impact the security requirements in another subsystem.
    c. Security requirements in one subsystem/component may require security requirements in another subsystem/component.
3. Consider inter-system dependencies to ensure that potential cyber security events are adequately addressed.
4. When developing the security requirements, consider related requirements. For example, to meet the audit requirements, access control and authentication requirements are needed.
5. A utility may need to accept the residual risk – based on the implementation timeline, the cost, and/or a lack of products with the appropriate security functionality.
6. The security requirements in the NISTIR 7628 are high-level guidance only and should be evaluated for applicability and tailored to meet a utility's specific needs. The set of security requirements is <u>not</u> prescriptive.
7. The NISTIR 7628 common and unique technical requirements should be allocated to each system and not necessarily to every component within a system, as the focus should be on security at the system level.
8. Organizations may find it necessary to identify compensating security requirements in lieu of a recommended security requirement to provide equivalent or comparable level of protection. More than one compensating requirement may be required.
9. NO system can be 100% secure – there will be security breaches. Also, most cyber security events are non-malicious.

2.1.6 Selection of Cyber Security Controls/Countermeasures and Operations and Maintenance

Once security requirements have been specified, a utility selects the cyber security controls/countermeasures in the implementation life cycle phase. The *security controls* should be selected and implemented based on an acceptable level of residual risk. The next life cycle phase is operations and maintenance, and the security controls should be continuously assessed to ensure they remain effective.

The following two diagrams illustrate the risk assessment processes that may be used in the implementation and operations and maintenance life cycle phases. The first diagram (Figure 2-9) illustrates the risk assessment process that may be used when selecting security controls during the implementation life cycle phase.

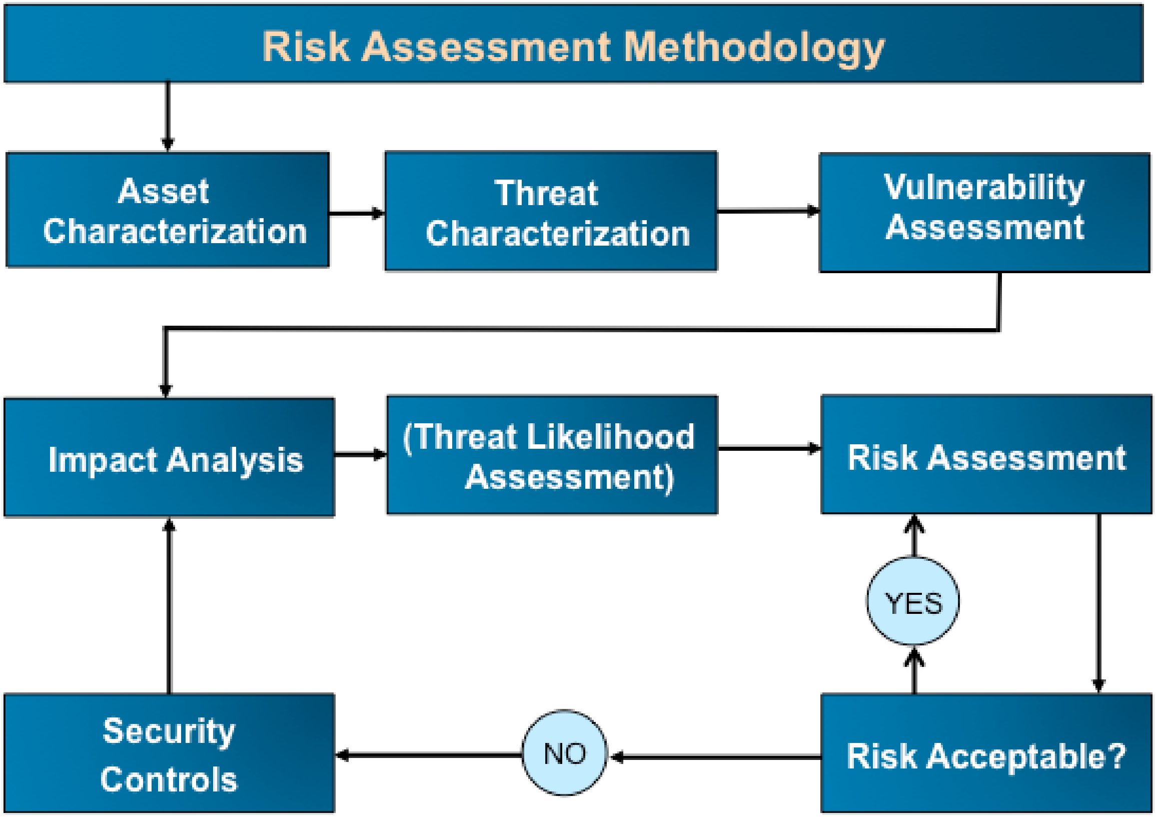


Figure 2-9
Cyber Security Risk Assessment Process

For the risk assessment during the operations and maintenance life cycle phase, the major difference is to make decisions about residual risk and whether the risk should be accepted, avoided, mitigated, shared, or transferred. In addition, the definition of the security controls is at a more granular level. Figure 2-10 below illustrates a risk assessment process that may be used during the operations and maintenance life cycle phase to address new threats and vulnerabilities and system changes.

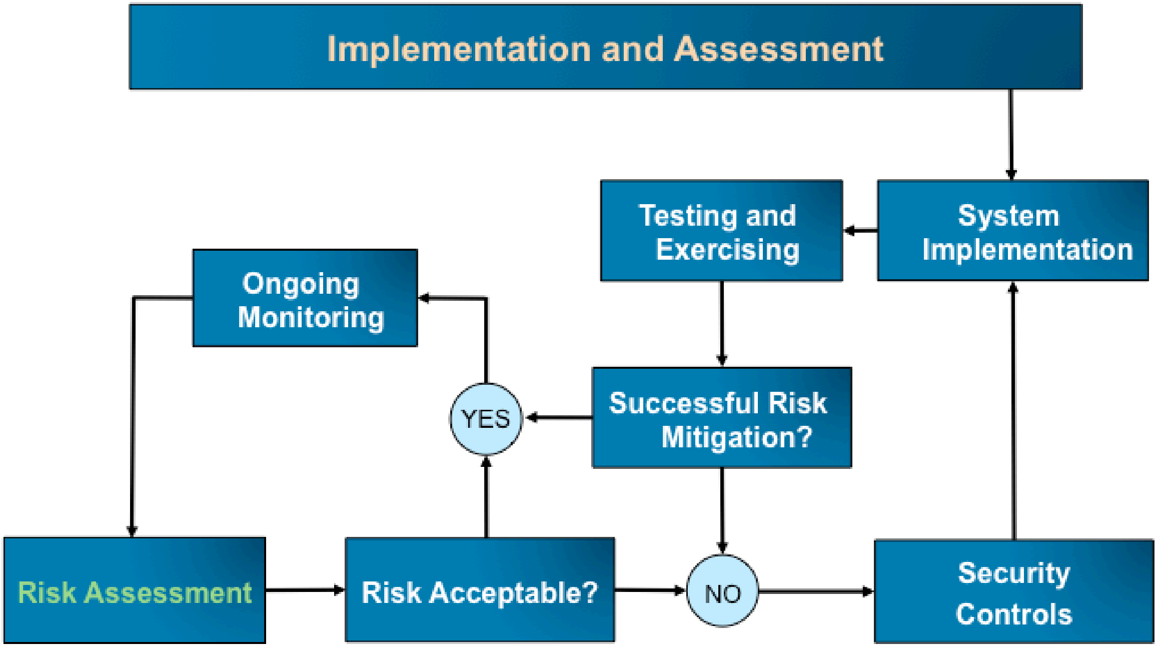


Figure 2-10
Cyber Security Risk Assessment – Implementation and Ongoing Monitoring

The implementation and operations and maintenance life cycle phases are outside the scope of the NISTIR 7628. However, some of the tips listed above for the design life cycle phase are applicable, if revised, to these life cycle phases.

TIPS:

1. Prioritize the security controls and focus on the highest impact systems – no utility has unlimited resources to address all the security controls.
2. Once the cyber security requirements are specified, the initial cyber security risk assessment should be updated and specified at a more granular level to be used in selecting cyber security measures/controls. This is typically done during the acquisition/development phase.
3. Consider inter-system dependencies to ensure that potential cyber security events are adequately addressed.
4. The cyber security controls may need to be revised based on available products. Current products and protocols may not provide all the required security functionality.
5. If applicable, use existing power system features/functionality as the security controls.
6. With the constantly changing environment of threats and vulnerabilities, the risk assessment process is not a one-time activity; it must be repeated at regular intervals or after a cyber security incident.
7. Organizations may find it necessary to identify compensating security controls in lieu of a recommended security control to provide equivalent or comparable level of protection. More than one compensating control may be required.
8. NO system can be 100% secure – there will be security breaches. The security controls should address resiliency of the electric sector.

3 SUMMARY

Cyber security supports the reliability of the electric sector and must address interconnected systems in grid modernization. Cyber security needs to be addressed in all systems, not just critical assets. To ensure that cyber security is adequately addressed throughout all the life cycle phases, the security posture of each system needs to be continuously monitored and assessed.

With the modernization of the electric sector, the cyber security issues that a utility implementing cyber security functionality must address are diverse and complicated.

1025672

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com