Integrating Electricity Subsector Failure Scenarios into a Risk Assessment Methodology

3002001181 | DEC 2013

U.S. DEPARTMENT OF ENERGY

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Program Leads

Jason D. Christopher

Technical Lead, Cyber Security Capabilities & Risk Management
Department of Energy (DOE), Office of Electricity Delivery and Energy Reliability (OE)

Annabelle Lee

Senior Technical Executive, Cyber Security
Electronic Power Research Institute (EPRI)

For more information on the DOE's cyber security risk management programs, please contact RMPGuideline@doe.gov

Integrating Electricity Subsector Failure Scenarios into a Risk Assessment Methodology

3002001181

Technical Update, December 2013

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.

Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

Copyright © 2013 Electric Power Research Institute, Inc. All rights reserved.

ACKNOWLEDGMENTS

The following organization prepared this report:

Electric Power Research Institute (EPRI)
3420 Hillview Avenue
Palo Alto, CA 94303

Principal Investigator
A. Lee

Jason Christopher, Department of Energy
Fowad Muneer (ICF International)
John Fry (ICF International)

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*, May 2012; the U.S. Department of Energy (DOE), *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), Version 1.0*, 31 May 2012, and the *Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector*, September 4, 2009. The author 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:

Integrating Electricity Subsector Failure Scenarios into a Risk Assessment Methodology. EPRI, Palo Alto, CA: 2013. 3002001181.

IriusRisk
Ex. 1015 - Page 5

ABSTRACT

The nation's power system consists of both legacy and next generation technologies. New grid technologies are introducing millions of novel, intelligent components to the electric grid that communicate in much more advanced ways than in the past: two-way communications, dynamic optimization, and wired and wireless communications. Cyber security is important because the bi-directional flow of two-way communication and control capabilities in the smart grid will enable an array of new functionalities and applications and with them will come new vulnerabilities.

This technical update provides guidance to utilities on developing and implementing a risk assessment process using the failure scenarios developed by the National Electric Sector Cybersecurity Organization Resource (NESCOR) program. NESCOR is a Department of Energy (DOE) funded public-private partnership led by EPRI.

Keywords
Cyber Security
Cyber Security Risk Assessment
Cyber Security Risk Management
Failure Scenarios

IriusRisk
Ex. 1015 - Page 7

EXECUTIVE SUMMARY

The nation's power system consists of both legacy and next generation technologies. New grid technologies are introducing millions of novel, intelligent components to the electric grid that communicate in much more advanced ways than in the past: two-way communications, dynamic optimization, and wired and wireless communications. These new components will operate in conjunction with legacy equipment that may be several decades old and provide no cyber security controls. With the increase in the use of digital devices and more advanced communications and information technology (IT), the overall attack surface has increased.

Cyber security must address deliberate attacks launched by disgruntled employees and nation-states as well as non-malicious cyber security events. Because organizations, including utilities, do not have unlimited resources such as personnel and funds, cyber security must be prioritized with the other components of enterprise risk. *Risk* is the potential for an unwanted impact resulting from an event. *Cyber security risk* is one component of enterprise risk management, which addresses 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 management strategy is a component within an organization's enterprise risk management strategy.

The purpose of this report is to specify a risk assessment process that may be used by utilities. Included are high-level diagrams that illustrate the risk assessment process at the security-requirements and security-control-selection stages, as well as for ongoing assessment and for assessing emerging changes. These are generic high-level diagrams based on commonly available reference documents. A second objective of this report is to illustrate how to use the content of the National Electric Sector Cybersecurity Organization Resource (NESCOR) cyber security failure scenarios and impact analyses document in the risk assessment process. A cyber security failure scenario is a realistic event in which the failure to maintain confidentiality, integrity, and/or availability of sector cyber assets creates a negative impact on the generation, transmission, and/or distribution of power.

IriusRisk
Ex. 1015 - Page 9

CONTENTS

1 BACKGROUND 1-1
1.1 Content of this Technical Update 1-1
1.2 Enterprise Risk Management 1-2
1.2.1 Risk Framing 1-3
1.2.2 Risk Assessment 1-4
1.2.3 Risk Response 1-4
1.2.4 Risk Monitoring 1-5
2 CYBER SECURITY RISK ASSESSMENT 2-1
2.1 Asset/System Characterization 2-2
2.2 Threat Agent Characterization 2-3
2.3 Vulnerability Assessment 2-3
2.4 Impact Analysis 2-3
2.5 Threat Likelihood Assessment 2-3
2.6 Security Requirements/Controls 2-3
2.7 Risk Determination 2-3
3 ONGOING RISK ASSESSMENT 3-1
3.1 Testing and Exercises 3-1
3.2 Mitigation Strategy 3-1
3.3 System Implementation 3-1
4 RISK ASSESSMENT USING THE NESCOR FAILURE SCENARIOS AND THE NISTIR 7628 4-1
4.1 NESCOR Asset Characterization 4-2
4.2 NESCOR Threat Agent Characterization 4-5
4.3 Vulnerability Classes Using the NISTIR 7628 4-7
4.4 NESCOR Impact Analysis 4-8
4.4.1 Impact Criteria Examples 4-11
4.4.2 NESCOR Threat Likelihood Assessment 4-12
4.4.3 Threat Likelihood and Opportunity Examples 4-14
4.4.4 Risk Ranking/Determination 4-14
5 CONCLUSION AND NEXT STEPS 5-1
6 REFERENCES 6-1
A VULNERABILITY CLASSES A-1
A.1 People, Policy and Procedures A-1
A.2 Platform Software/Firmware Vulnerabilities A-1
A.3 Platform Vulnerabilities A-2
A.4 Network A-2

LIST OF FIGURES

Figure 1-1 Risk Management Cycle.....1-3
Figure 2-1 Cyber Security Risk Assessment Process 2-2
Figure 3-1 Cyber Security Risk Assessment – Regularly Scheduled Assessments.....3-2
Figure 3-2 Cyber Security Risk Assessment – Emerging Changes.....3-3
Figure 4-1 Advanced Metering Infrastructure Failure Scenario 4-3
Figure 4-2 Distribution Grid Management (DGM) Failure Scenario.....4-4
Figure 4-3 Risk Ranking Graph 4-15
Figure 4-4 Risk Ranking Graph for the Examples 4-16

LIST OF TABLES

Table 4-1 Electric Sector Cyber Security Domain Threat Model 4-5
Table 4-2 Impact Criteria Table 4-10
Table 4-3 AMI.6 Impact Criteria Score.....4-11
Table 4-4 DGM.6 Impact Criteria Score.....4-12
Table 4-5 Criteria for Threat Likelihood and Opportunity.....4-13
Table 4-6 AMI.6 Threat Likelihood and Opportunity Score.....4-14
Table 4-7 DGM.6 Threat Likelihood and Opportunity Score.....4-14

IriusRisk
Ex. 1015 - Page 15

1
BACKGROUND

The nation's power system consists of both legacy and next generation technologies. New grid technologies are introducing millions of novel, 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. These new components will operate in conjunction with legacy equipment that may be several decades old, and provide no cyber security controls. With the increase in the use of digital devices and more advanced communications and information technology (IT), the overall attack surface has increased. For example, as substations are modernized, the new equipment is digital, rather than analog. These new devices include commercially available operating systems, protocols, and applications rather than proprietary solutions. This increased digital functionality provides a larger attack surface for any potential adversary. Also, many of these commercially available solutions have known vulnerabilities that may be exploited by adversaries. These known vulnerabilities may be exploited in the new control system components that are deployed and implemented.

To adequately address potential threat agents 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 sunset. Cyber security must address deliberate attacks launched by disgruntled employees and nation-states as well as non-malicious cyber security events. Currently, the majority of cyber security events are non-malicious. Because organizations, including utilities, do not have unlimited resources, including personnel and funds, cyber security must be prioritized with the other components of enterprise risk. *Risk* is the potential for an unwanted impact resulting from an event. *Cyber security risk* is one component of enterprise risk, which addresses 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 management strategy is a component within an organization's enterprise risk management strategy.

A primary difference between enterprise risk management for typical IT systems and control systems is the prioritization of the security objectives (confidentiality, integrity, and availability). In general, the primary security objective for control systems is availability, with integrity second, and confidentiality third. This is in contrast with most IT systems, which prioritize confidentiality and integrity as the primary security objectives and availability secondary. These differences in the prioritization of the security objectives may require a separate risk management strategy developed specifically to address control systems.

1.1 Content of this Technical Update

The purpose of this report is to specify a risk assessment process that may be used by utilities. High-level diagrams are included to illustrate the risk assessment process. These are generic high-level diagrams based on commonly available reference documents. A second objective of this report is to illustrate how to use the content of the National Electric Sector Cybersecurity Organization Resource (NESCOR) cyber security failure scenarios and impact analyses

IriusRisk
Ex. 1015 - Page 17

document in the risk assessment process. A cyber security failure scenario is a realistic event in which the failure to maintain confidentiality, integrity, and/or availability of sector cyber assets creates a negative impact on the generation, transmission, and/or distribution of power.

Included in this chapter is an overview of enterprise risk management. Chapter 2 provides an overview of risk assessment. Chapter 3 documents how to use the NESCOR failure scenarios in the risk assessment process.

1.2 Enterprise Risk Management

An enterprise *risk management strategy* identifies how an organization frames, assesses, responds to, and monitors risk on an ongoing/continual basis. This overall strategy may be further refined and tailored for specific departments/agencies within an organization and for specific classes or families of systems. Enterprises have developed processes to evaluate risks associated with their business and to address those risks based on organizational priorities and both internal and external constraints. In addition, utilities have developed a variety of risk management methodologies, models, and systems for addressing risks related to safety. This management of all these types of risk is an ongoing process that is part of normal operations.

Although this report focuses on risk management and risk assessment for systems, it is important to consider the overall enterprise risk culture. For example, as specified in the Department of Energy (DOE) *Electricity Subsector Cybersecurity Capability Maturity Model (*ES-C2M2):

> *Institutionalization* describes the extent to which a practice or activity is ingrained into an organization's operations. The more deeply ingrained an activity, the more likely it is that the organization will continue to perform the activity over time.

Risk assessment approaches used by an organization reflect its culture *(the values and norms of its leaders, management, and staff that influence their actions)* in dealing with and communicating risks. Recognizing, and addressing these influences help achieve effective risk management. The ES-C2M2 evaluations measure the institutionalization of various cyber security and risk management practices and thus can serve as a useful tool to understand the organizational culture with regard to risk management.

The following discussion on risk management is drawn from the Department of Energy (DOE) risk management document, *Electricity Subsector Cybersecurity Risk Management Process* (RMP) published in May 2012 and tailors the content to systems, rather than organizations. The RMP provides a scalable risk management process that is specific to the risks inherent in operating information technology (IT) and industrial control systems (ICS). The term *risk management* refers to the program and supporting processes used to manage cyber security risk to an organization's operations, its assets, and individuals.

In implementing the RMP, organizations have the flexibility to determine how best to conduct the activities, including the sequence, degree of rigor, formality, and how the results or outputs of each activity are captured and shared across the organization and between organizations. The RMP is meant to supplement an organization's existing risk management framework and provide flexible guidelines that may be leveraged as needed.

The risk management cycle includes four phases. These phases require utilities to (1) *frame* risk (i.e., establish the context for risk-based decisions), (2) *assess* risk, (3) *respond* to risk once determined, and (4) *monitor* risk on an ongoing basis, using an iterative feedback loop for continuous improvement in the risk-related activities of organizations. The risk management cycle and the four phases are illustrated in Figure 1-1 and further defined below.

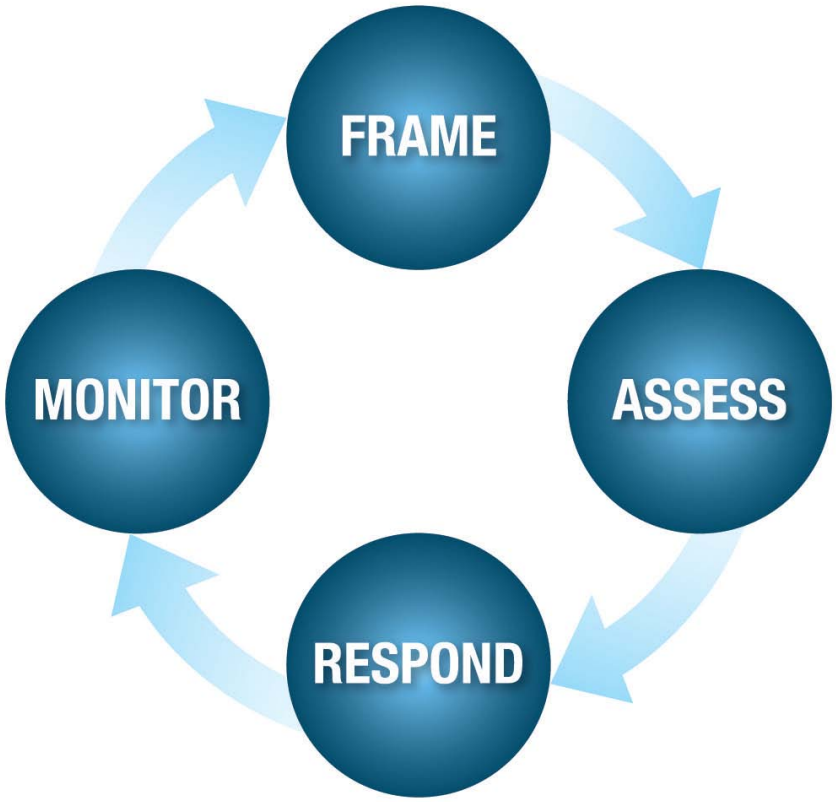

Figure 1-1
Risk Management Cycle

1.2.1 Risk Framing

The risk-framing phase includes the description of the environment in which risk-based decisions are made. The environment for control systems is often distinct from that for IT systems. For example, many control system components are located in physically unprotected areas (e.g., pole tops, sides of buildings) and are expected to operate 24/7 without interruption. Establishing a realistic risk frame requires utilities to specify the following for the control systems:

- Assumptions about threats, vulnerabilities, impacts, and likelihood of occurrence;
- Constraints imposed by legislation, regulation, and resources (time, money, and people);
- Risk tolerance/level of acceptable risk;
- System priorities and criticality within mission/functional areas, and trade-offs between different types of risk; and
- Trust relationships with third parties and vendors and physical interconnections with external organizations.

1.2.2 Risk Assessment

Risk assessment is the identification, estimation, and prioritization of risk to an organization's operations, assets, individuals, and other interconnected electricity subsector organizations. *Risk assessment* involves the integration of threat, vulnerability, and consequence/impact information. Risk assessment outputs are used to prioritize and allocate resources to address identified risks. The first step in the risk assessment process is to identify the assets – control systems or groups of control systems. Once this task has been completed, the utility:

- Identifies, characterizes, and assesses threats;
- Assesses critical assets (control system) vulnerabilities;
- Determines the impact (the expected consequences of cyber security events); and
- Specifies the likelihood of the cyber security event (including the skills, motive, and capabilities of attackers and the availability of attack tools and malware).

To support the risk assessment phase, utilities will need to identify:

- Tools, techniques, and methodologies that are used to assess risk;
- Constraints that may affect risk assessments (assessing risk on test systems rather than operational systems); and
- Roles and responsibilities related to risk assessment (individuals and their various roles).

1.2.3 Risk Response

The risk response phase addresses how a utility responds to each risk associated with control systems. In this phase, a utility:

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

A utility may determine that certain response actions are not feasible to implement, are cost prohibitive, or are not relevant to the utility's control system operations. If the mitigation controls are cost prohibitive, require excessive utility resources to implement, or are not feasible to implement, a utility may implement compensating controls[1] to manage the risk and meet the cyber security requirements. The risk response element is the point where utilities make choices on how best to address risk.

[1] A compensating control is a cyber security control implemented as an alternative to a recommended control that provides equivalent or comparable control.

1.2.4 Risk Monitoring

The risk-monitoring phase addresses how risks are monitored over time in a utility. During the risk monitoring phase, utilities:

- Evaluate the ongoing effectiveness of risk response measures;
- Identify changes that may impact risk to a utility's control systems and the operational environments; and
- Identify changes (e.g., technology, vulnerabilities, threat agents) that may impact the effectiveness of risk responses.

2
CYBER SECURITY RISK ASSESSMENT

As documented above, a cyber security risk assessment process is a component of a cyber security risk management strategy. Risks identified during a risk assessment will then be analyzed using three basic types of measuring risk: 1) *qualitative* where the scoring may be low, moderate, and high, 2) *quantitative* where the scoring may be numeric, such as a score from 1-10, or 3) a combination of both. A utility should select an approach that balances the criticality of the assets in question and the cost of additional analysis. This organization-level risk assessment process should be used and modified, as required, for control systems.

One of the ten domains in the ES-C2M2 is Risk Management and included in the domain are risk assessment practices. Identified in the practices are two documents that may be used in performing the risk assessment: a network (IT and/or OT) architecture and a current cyber security architecture. Also included in the ES-C2M2 is a *risk register* that identifies risks and associated attributes such as threat and vulnerability information. This register may be used in managing risk.

A risk assessment may be performed in the acquisition/development phase of the system life cycle. The objective would be to develop the security requirements that will be included in procurement specifications or internal design documents. In this phase, the risk assessment may not include granular detail because the utility is not selecting specific products or components. Also, preliminary confidentiality, integrity, and availability impact levels should be specified for each system or group of systems. These impact levels will affect the specification of cyber security requirements.

A utility selects the cyber security controls/countermeasures in the implementation phase of the system life cycle. The *security controls* for each system should be selected and tailored based on an acceptable level of residual risk and should meet the security requirements specified in the acquisition/development phase. Because the risk assessment may then be updated to a more detailed level, the confidentiality, integrity, and availability impact levels should be reevaluated to ensure they remain the same, or are revised, as required. The risk assessment process for the selection of security requirements and the selection and implementation of security controls is illustrated in Figure 2-1. The elements in the figure were identified above and are further defined below. Sequential representation in the figure is there for clarity and organizations have the flexibility to adapt according to their unique needs and processes.

One important aspect of the risk assessment process is the feedback loop between the Risk Acceptance and Security Requirements/Controls Selection. The objective is to ensure that the security requirements and security controls are adequate and that the level of residual risk for each system or groups of systems is acceptable to the utility. The risk approach can include avoiding sharing, mitigating, transferring, or accepting the risk. Because cyber security supports the reliability of the electricity subsector, several of these approaches may not be considered acceptable. The residual risk is determined based on the level of resources required (including both personnel and financial), the adverse impact on the organization, and prioritization with the other organizational risk types described previously.

IriusRisk
Ex. 1015 - Page 23

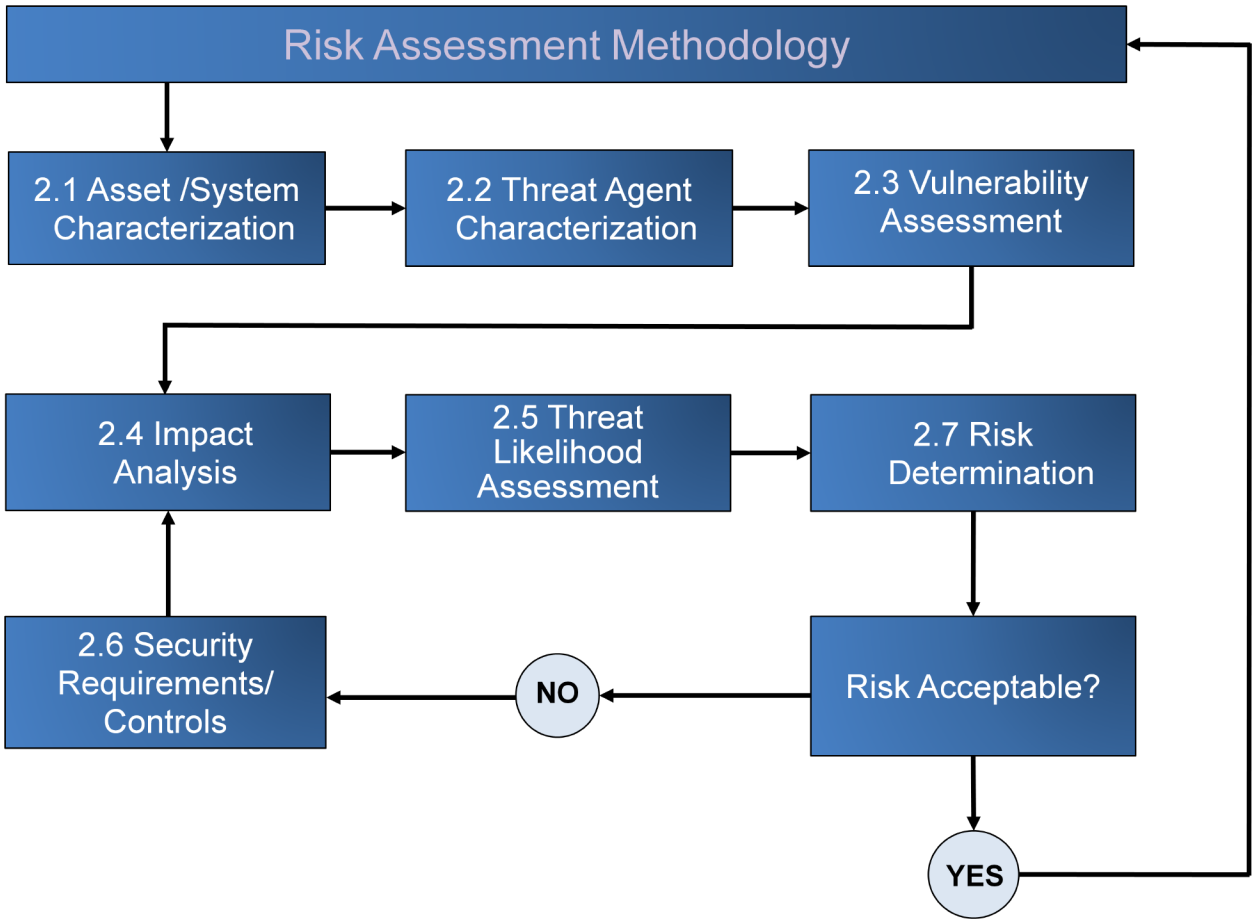

Figure 2-1
Cyber Security Risk Assessment Process

A utility may need to accept the residual risk – based on system performance, cost, and/or a lack of products with the appropriate security functionality. If the residual risk is at an acceptable level, the utility will continue moving forward. If the residual risk is *not* at an acceptable level, the utility will need to redo the risk assessment. If existing security controls significantly impact performance or if products are not available, the utility may need to consider implementing *compensating controls* that provide a comparable level of protection. Typically, the risk assessment will only be performed once during the acquisition/development life cycle phase.

2.1 Asset/System Characterization

The first step in the risk assessment process is to identify all the assets and rank them in terms of priority to the mission, image, reputation, and/or specific functions of the organization. (Note: the term *system,* rather than asset, will be used throughout this report.) Utility owners and operators have many systems that must be assessed. Typically, a system meets a specific business function and consists of many components. The organization will perform the risk assessment on the highest priority systems first and then assess the lower priority systems as resources and time permits. Because the electric grid is changing from a relatively closed system to a complex, highly interconnected environment, the identification of each system and the system boundary has become more complicated. In addition, inter-system dependencies should be considered to ensure that potential cyber security events are adequately addressed.

IriusRisk
Ex. 1015 - Page 24

2.2 Threat Agent Characterization

A *threat agent* is a class of actors that could cause a failure scenario to occur in some specified domain, either as the sole cause or as a contributor to it. Typical examples of threat agents are nation-states, criminals, insiders (whether malicious or non-malicious), and recreational hackers. To be effective, mitigation strategies must take into account the motivation, tactics, and capabilities of those threat agents that may cause cyber security events to occur. As stated above, the majority of cyber security events are non-malicious, for example, the administrator makes an error or the documentation is inaccurate.

2.3 Vulnerability Assessment

A *vulnerability* is a weakness that could be exploited by a threat agent and adversely impact the operation of a system. Potential vulnerabilities can be in policies, procedures, and/or technical controls. Currently, vendors are developing control systems that use commercial rather than proprietary products. Some of the commercial products are operating systems, applications, and communications protocols. Consequently, the vulnerabilities that have been identified for these products may be exploited in the control systems.

2.4 Impact Analysis

The *impact analysis* focuses on the consequences or results of a successful cyber security event. For example, customers may have a negative view of the utility, generation capacity may be reduced, and public safety may be jeopardized.

2.5 Threat Likelihood Assessment

Threat likelihood includes criteria that influence the likelihood and opportunity for a threat agent to exploit a vulnerability, that is, whether the system represents a tempting target for an attacker and whether the attacker has the capability to attack the system. Likelihood may include, for example, the level of skill required by the attacker and how easy it is to obtain the technical means to carry out an attack. A utility can use these criteria to help assess the probability that a cyber security event will occur.

2.6 Security Requirements/Controls

The lists of *security requirements* and *security controls* will be input to the risk assessment and to the impact analysis steps. The goal is to ensure that the requirements and controls address the vulnerabilities and mitigate the impacts of a cyber security event.

2.7 Risk Determination

All of the individual components of the risk assessment process described above are performed to determine an overall level of risk. A utility may group systems according to function and criticality and perform the risk assessment on the system group. The purpose is to simplify the overall risk assessment process.

3
ONGOING RISK ASSESSMENT

The risk assessment process is executed on an ongoing basis – to address changes in technology and the threat environment and at regular intervals (Scheduled Assessment). The goal is to ensure that the security controls remain effective, i.e. are implemented correctly, operating as intended, and produce the desired outcome, and that the level of residual risk is acceptable. This ongoing monitoring process may include an assessment of a subset of the systems that were identified and a subset of the security controls that were implemented. The objective is to focus on the highest priority systems and security controls. Each utility will define the time frame for performing regularly scheduled assessments. The time frame may be based on regulations, such as the North American Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards, other regulations, or organization requirements. There are three components in the scheduled assessment risk assessment process: testing and exercising, mitigation strategy, and system implementation.

3.1 Testing and Exercises

The types of *testing and exercises* are defined by the utility and may include testing documented procedures or technical controls. Utilities generally do not conduct tests on operational systems to ensure that the reliability of the electric grid is not compromised. As an alternative, a utility may have a test system that they use to assess security functionality or the potential impact of new security patches or upgrades. To assess the security functionality, a utility may develop a *regression test suite* that consists of a set of test scenarios used to ensure that additions or modifications do not adversely the security or performance of the system. The regression test suite is not intended to be a comprehensive set of tests; rather, it contains tests for the high priority security functionality. This is determined using the results of the risk assessment. The key to an effective regression testing strategy is to design a test suite that provides a high degree of confidence without retesting everything. The security regression test suite should be periodically reviewed and unnecessary or redundant tests removed and new tests added.

3.2 Mitigation Strategy

The *mitigation strategy* developed by the utility provides guidance on how to reduce the risk to an acceptable level. The strategy may include augmenting existing technical controls, developing or revising policies and procedures, implementing new technical controls, or accepting the risk. Utilities do not have unlimited resources to address all potential security vulnerabilities, therefore they must prioritize the vulnerabilities and the mitigation controls.

3.3 System Implementation

The *system implementation* is the operational control system that is being assessed. The utility may select one system from a group of systems to assess, rather than assessing all the systems in the group. This is an alternative approach if the utility has performed the risk assessment on the system group and selected the security controls for the group. In addition, the utility should have developed the mitigation strategy for each group of systems.

IriusRisk
Ex. 1015 - Page 27

Figure 3-1 illustrates a regularly scheduled risk assessment process.

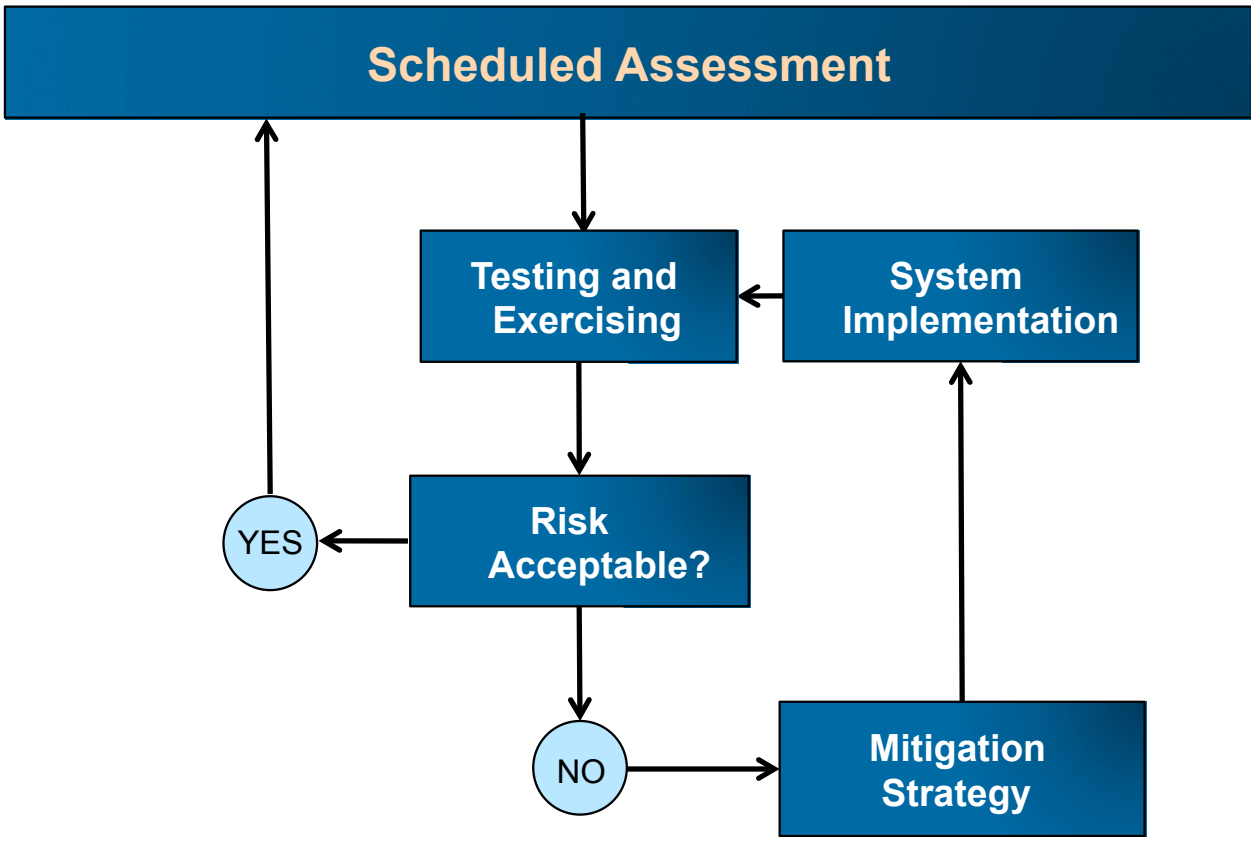

Figure 3-1
Cyber Security Risk Assessment – Regularly Scheduled Assessments

The IT and telecommunications environments are constantly changing-with the development and deployment of new technologies, the emergence of new vulnerabilities, and the development of new attack vectors. A risk assessment may need to be performed if there are significant changes. Because new vulnerabilities are identified almost daily, a utility needs to develop criteria for determining when a risk assessment will be required. The criteria could be based on the severity or scope of the vulnerability. As in the previous risk assessment processes, the highest priority systems should be assessed first. Typically, this risk assessment is only performed when significant changes have been identified that could adversely impact the control systems (for new vulnerabilities and attacks) or that provide significant advancements in cyber security protections. As in the Scheduled Assessment process, the organization's risk mitigation strategy is critical to the decision process. Figure 3-2 illustrates a risk assessment process that may be used during the operations and maintenance life cycle phase to address these emerging changes.

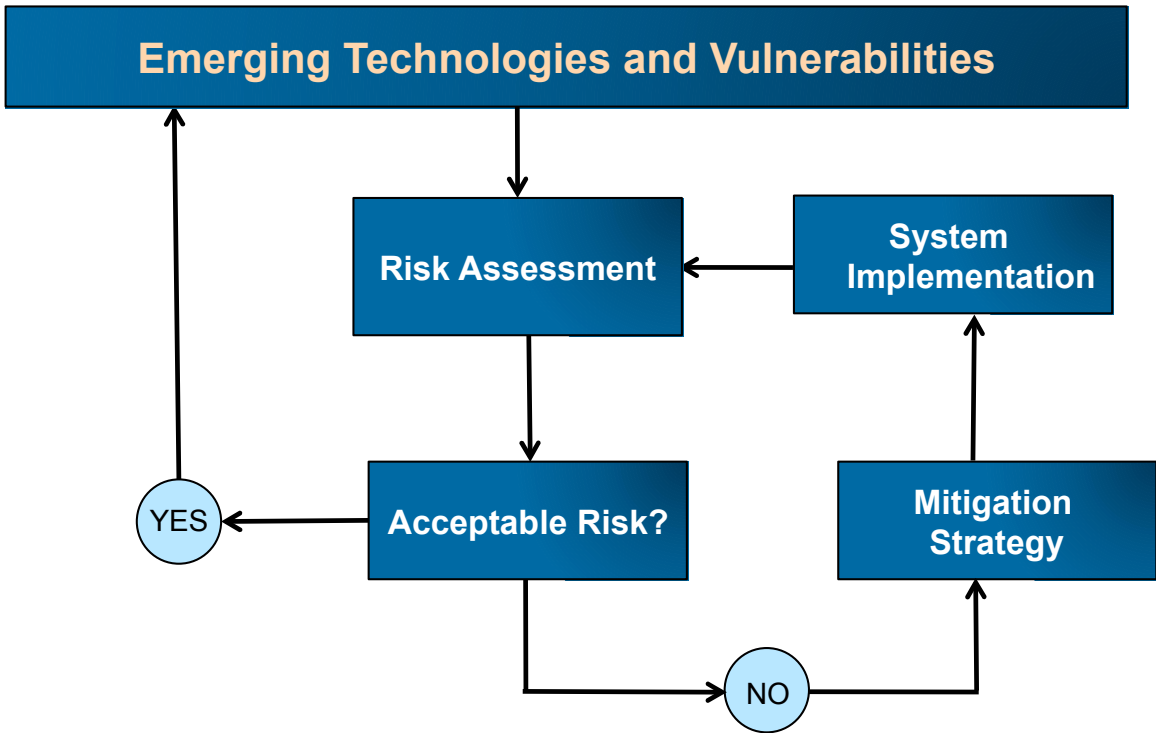

Figure 3-2
Cyber Security Risk Assessment – Emerging Changes

4

RISK ASSESSMENT USING THE NESCOR FAILURE SCENARIOS AND THE NISTIR 7628

The application of the risk assessment process included in this technical update is illustrated below using content from the *Electric Sector Failure Scenarios and Impact Analyses*[2], Version 1.0, September 2013 and the National Institute of Standards and Technology Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security,* August 2010 documents. The list of vulnerabilities included in this technical update was developed from the vulnerabilities classes section of the NISTIR 7628. The major change was to remove some of the vulnerabilities in the Platform Software/Firmware Vulnerabilities section to have a more consistent level of abstraction throughout the list. The threat agent characterization, impact analyses, and mitigation strategies are from the NESCOR Failure Scenarios document. For simplicity, the risk assessment is performed on two of the failure scenarios, rather than on a system.

The following background material is extracted from the NESCOR Failure Scenarios document and provides an overview of the document.

> The National Electric Sector Cybersecurity Organization Resource (NESCOR) developed cyber security failure scenarios and impact analyses for the electric sector. A cyber security failure scenario is a realistic event in which the failure to maintain confidentiality, integrity, and/or availability of sector cyber assets creates a negative impact on the generation, transmission, and/or delivery of power.
>
> Failure scenarios include malicious and non-malicious cyber security events such as:
>
> - Failures due to compromising equipment functionality,
> - Failures due to data integrity attacks,
> - Communications failures,
> - Human error,
> - Interference with the equipment lifecycle, and
> - Natural disasters that impact cyber security posture.
>
> Impacts identified in the failure scenarios include loss of power, equipment damage, human casualties, revenue loss, violations of customer privacy, and loss of public confidence.
>
> Appropriate mitigations are then identified to lower risk where deemed necessary. Mitigations in the document use a common naming schema that improves readability and comprehension, and enables their prioritization.

[2] Hereafter this is referred to as the NESCOR Failure Scenarios document.

Each of the elements of the risk assessment process; asset characterization, threat agent characterization, vulnerability assessment, and threat likelihood are illustrated using the NESCOR Failure Scenarios. In addition, risk mitigation measures are identified. This is part of the risk response phase described above.

4.1 NESCOR Asset Characterization

This is step 2.1 in Figure 2-1. The NESCOR failure scenarios are organized in six categories, corresponding to the priority areas identified in the National Institute of Standards and Technology (NIST) Special Publication 1108, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*[3], Office of the National Coordinator for Smart Grid Interoperability.

1. Advanced Metering Infrastructure (AMI)
2. Distributed Energy Resources (DER)
3. WAMPAC (Wide Area Monitoring, Protection, and Control)
4. Electric Transportation (ET)
5. Demand Response (DR)
6. Distribution Grid Management (DGM)

In addition, there are failure scenarios in a seventh cross cutting category called "Generic," which includes failure scenarios that may impact many of these functional domains. The failure scenarios are not intended to be a complete list of all possible failure scenarios, and their mitigations are a suggested list of recommendations intended to provide a variety of options. The scenario write-ups include: description, relevant vulnerabilities, impacts, and potential mitigations [3]. In addition, a second document provides more detailed descriptions for the highest priority failure scenarios and modified attack tree diagrams [4]. Included below are two failure scenarios from the AMI and DGM priority areas.

[3] Release 2.0 of the NIST Framework has redefined the priority areas. The six listed in this report are included, with additional areas documented.

AMI.6 One Compromised Meter in a Mesh Wireless Network Blocks Others

Description: An unauthorized entity installs rogue firmware or software on a single smart meter. This might be via direct access to the meter or via interception/modification of a legitimate meter update. The compromised meter software could report an understatement of usage, or cause sporadic failure of the self-test process to impede discovery. If meters in the system implement a mesh wireless network, the compromised meter might misroute communications from other meters, blocking the path back to the AMI headend for those meters and making those meters effectively "unresponsive."

Relevant Vulnerabilities:

- Weak or no authentication or authorization controls for privilege to install firmware or software,
- No capability to detect installation of unauthorized firmware or software in a meter.

Impact:

- Continuous loss of revenue for utility if modified software/firmware understates usage (impact scales as more meters are affected),
- Truck rolls needed to investigate compromised meter failure or nonresponsive meters due to misrouting.

Potential Mitigations:

- *Detect unusual patterns* of energy usage on smart meters (all utilities have some type of revenue protection scheme, but these may not be sufficient),
- *Require multi-factor authentication* for firmware or software updates,
- *Check software file integrity* (digital signatures or keyed hashes) to validate software or firmware updates before installation and/or during operation.

Figure 4-1
Advanced Metering Infrastructure Failure Scenario

DGM.6 Spoofed Substation Field Devices Influence Automated Responses

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

Relevant Vulnerabilities:

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

Impact:

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

Potential Mitigations:

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

Figure 4-2
Distribution Grid Management (DGM) Failure Scenario

Each failure scenario documents a specific cyber security event that may adversely impact one or more systems. Each failure scenario should be allocated to a system group and to specific systems within that system group, if applicable. Some of the failure scenarios, particularly the generic scenarios, may be allocated to multiple systems. To ensure that the objective levels for confidentiality, integrity, and availability are adequately addressed for a system or group of systems, *assumptions* about each failure scenario should be documented. For example, is the impact widespread or limited to a single device? These assumptions will ensure that the failure scenario is accurately applied to the system and that the appropriate mitigation strategies are selected to meet the residual risk.

IriusRisk
Ex. 1015 - Page 34

4.2 NESCOR Threat Agent Characterization

This is step 2.2 in Figure 2-1. The NESCOR Failure Scenarios document includes a list of threat agents that are of particular concern to the electricity subsector. The threat agent identification and characterization table was developed based on several models and feedback from the working group participants.

The electric sector cyber security domain threat model incorporates the following elements:

- Adversaries with intent, driven by money, politics, religion, activist causes, recreation, recognition or simply malevolence
- Adversary activity may include spying or have direct impact on operations
- Insiders or outsiders, groups or individuals
- Failure in people, processes, and technology, including human error
- Loss of resources, in particular key employees or communications infrastructure
- Accidents
- Natural hazards as they impact cyber security.

Intentional adversaries are grouped to separate them by motive and modus operandi.

Table 4-1
Electric Sector Cyber Security Domain Threat Model

Threat Agent	Subcategory	Example Members
Economic Criminals		
	Transnational or national criminal Organization	Former Soviet Union Mafia, extortion groups[4]
	Insiders (financial, espionage)	Employees, contractors
	Customers	Residential, commercial, schools
	External individual	
Malicious Criminals		Disgruntled employees or contractors, deranged persons, cyber gangs
Recreational Criminals		Hackers

[4] http://www.safetyissues.com/site/cyber_crime/cia_reveals_hacker_attacks_on_utilities.html?print

IriusRisk
Ex. 1015 - Page 35

Table 4-1 (Continued)
Electric Sector Cyber Security Domain Threat Model

Threat Agent	Subcategory	Example Members
Activist Groups		
	Eco and cause driven	Earth First, Green Peace
	U.S. national separatists	U.S. militias and hate groups (known to steal power)
Terrorists		
	Religious radical extremists	Al Qaeda, Taliban
	Lone extremists	Anti-society individual
	Strategic political	Nation State: China, North Korea, Cuba
	Tactical political	Lashkar-e-Taiba[5], Hamas
Hazards		
	Natural hazards	Tornados, pandemics, floods, earthquakes
	Human errors and other accidents	- Poor human-system design - Configuration or data entry errors - Inadequate or non-existent policies, processes, procedures, and/or training - Non-compliance (not following policies and procedures) - Inadequate auditing, maintenance and testing - Poor plant system design - Legacy and aging systems
	Other hazards to required resources	- Employees that monitor cyber security are absent due to terror threat - Loss of processing/communication facilities due to nearby physical attack

Economic criminals are driven by money and malicious criminals are driven by emotion and the desire to harm. Recreational criminals are driven by the desire for fun or self-promotion.

"Other hazards to required resources" refers to loss or degradation of resources required to maintain cyber security, for reasons not otherwise covered in the threat model.

Each utility will select and prioritize the threat agents based on information received from external sources, such as law enforcement and other utilities, internal knowledge, and the systems that are being assessed. The list of threat agents will be used in determining motivation and likelihood of impact.

[5] http://en.wikipedia.org/wiki/Lashkar-e-Taiba

For each failure scenario, one or more threat agents may be identified. For the AMI failure scenario included above, the applicable threat agent is *Economic Criminals: External Individuals* because of the loss of revenue to the utility. For the DGM failure scenario, the applicable threat agents are *Economic Criminals: External Individuals* because of the loss of revenue and *Malicious Criminals* because of the inaccurate application of Volt/VAR controls.

4.3 Vulnerability Classes Using the NISTIR 7628

This is step 2.3 in Figure 2-1. Each failure scenario includes potential vulnerabilities that may be exploited by a malicious or non-malicious actor. The failure scenario document identified unique vulnerabilities for each scenario and almost 200 vulnerabilities were identified[6]. The vulnerabilities are not vendor-specific; they are defined at a more abstract level. The current list of potential vulnerabilities is constantly changing because of advancements in technology, adversary capabilities, and available tools and techniques.

The NISTIR 7628 identifies vulnerability classes that are applicable to the electricity subsector. There are four high level categories of classes: People, Policy, and Procedures; Platform Software-Firmware Vulnerabilities; Platform Vulnerabilities; and Network. The software development category (under the Platform Software/Firmware Vulnerabilities category) contains several vulnerabilities that are at a low level of granularity. For this risk assessment, these vulnerabilities have been removed to focus on abstract vulnerability classes rather than implementation specific vulnerabilities. For example, buffer overflow and API abuse were deleted.

A preliminary mapping of the vulnerabilities in the failure scenarios to the revised vulnerability classes list shows significant commonality. The revised vulnerability class list from the NISTIR 7628 is included in Appendix A of this document.

For the AMI example, the two vulnerabilities are:

- Weak or no authentication or authorization controls for privilege to install firmware or software,
- No capability to detect installation of unauthorized firmware or software in a meter.

The first vulnerability may be allocated to the *authorization vulnerability* class and the second vulnerability may be allocated to the *inadequate change and configuration management* class.

For the DGM example, the vulnerabilities are:

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

The first vulnerability may be allocated to the *authentication vulnerability* class and the second vulnerability allocated to the *sensitive data protection vulnerability* class.

When systems are evaluated, each implementation specific vulnerability should be allocated to a vulnerability class. The vulnerability classes should be allocated to the system groups.

---

[6] The NESCOR team did not have the time to develop a common set of vulnerabilities across all the scenarios. This was proposed as a future task.

4.4 NESCOR Impact Analysis

This is step 2.4 in Figure 2-1. *Impact* is the effect of the failure scenario on the delivery of power, the business of the utility, and the interests of its customers. Each failure scenario includes one or more impacts. Some examples include:

- Negative publicity
- Financial loss to utility
- Power system instability, including outages and power quality problems
- Decrease in operational efficiency and increase in utility power losses
- Decrease in service reliability

As noted above, a utility should document the assumptions related to a failure scenario. For example, one assumption relates to the *scope* or *scalability* of the impact, that is, whether the cyber security event applies to a few homes, a neighborhood, or a large area. This task should be completed prior to selecting specific impacts and computing the impact ranking score.

In the security requirements selection and security controls selection phases, the impacts should be input to the risk assessment process. The impacts are one component that may be used by the utility in determining the levels for the security objectives of confidentiality, integrity, and availability. The impacts should be used in determining the values for the impact ranking criteria.

Following is material extracted from the NESCOR Failure Scenarios document that describes the impact ranking criteria and scoring methodology.

System Scale: Describes whether the impact of this failure scenario is geographically localized, impacts a subset of all devices but is not localized, or may impact the entire system.

Safety Concern: Two safety criteria consider whether there is a potential for injuries or loss of life. This factor is considered for the public and the utility workforce.

Ecological Concern: This criterion considers whether the failure scenario might cause damage to the environment. For example, burning or leaking of hazardous material would be judged as "Permanent Ecological Damage."

Financial Impact of Compromise on Utility: This criterion considers direct financial loss to the utility as a result of the failure scenario, without consideration of the restoration costs as defined below. A scale for costs is used that is relative to the amount of utility revenue.

Restoration Costs: Restoration costs include the cost to return the system to proper operation, not including any legal or other reparations as a result of the failure. A scale for costs is used that is relative to the total size of the utility operations and maintenance budget.

Negative impact on generation capacity: The scoring for this criterion considers the level of loss of generation capacity, and for how long this loss is sustained.

Negative impact on the energy market: Specific impacts identified are price manipulation, loss transactions, or loss of participation by market members (buyers or sellers). Scores 0, 1 and 3 mean respectively either no such impacts, local impacts or widespread occurrence of these impacts. A breakdown in key market functions that creates a non-operational market earns the highest score.

Negative impact on the bulk transmission system: The scoring for this criterion uses DOE concepts defined for incident reporting[7]. In particular, a *major transmission system interruption* is defined as follows: "An event has occurred that required action(s) to relieve voltage or loading conditions; or transmission separation or islanding has occurred." A *complete operational failure or shut-down of the transmission* system is defined as: "An emergency event where an electrically isolated or interconnected electrical system suffers total system collapse that results in the shutdown of the transmission …electrical system…."

Negative impact on customer service: The scores for this criterion consider the delay a customer experiences in gaining resolution of their problem, and for how long this condition persists.

Negative impact on billing functions: Billing depends upon accurate power usage data. This criterion measures the number of customers for which the utility may lose the capability to generate accurate bills due to the failure scenario. The scores also consider whether or not the data is recoverable.

Destroys goodwill toward utility: This criterion measures the extent to which customers and the community look less favorably on the utility as a result of the occurrence of the failure scenario. It is scaled by the resulting level of decrease in interest by customers in participating in advanced programs such as smart meter deployments and demand response.

Immediate economic damage, Long-term economic damage: Economic damage means a negative impact on the wealth and resources of a country or region. (This is distinct from a financial impact on an organization or individual.) The scoring for these criteria is based upon how widespread the damage is, and for how long it continues to have impact.

Causes a loss of privacy for a significant number of stakeholders: The scale for this criterion considers the number of customers who may have personal information disclosed due to the failure scenario. Personal information is defined in Appendix E of the NISTIR 7628.

Using a wide and unevenly spaced range of numbers requires more thought and better results than a scheme such as 0, 1, 2, 3. In the latter case, "2 is" too often an easy default score. Based on this approach, the scores used in the impact criteria are 0, 1, 3, and 9. The criterion and how to score are defined in the table below.

[7] DOE form OE-417: ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT. http://www.oe.netl.doe.gov/oe417.aspx

Table 4-2
Impact Criteria Table

Criterion	How to Score	Score
System scale	0: single utility customer, 1: neighborhood, town, 3: all ET, DER or DR customers for a utility, 9: potentially full utility service area and beyond	
Public safety concern	0: none, 1:10-20 injuries possible, 3: 100 injured possible, 9: one death possible	
Workforce safety concern	0: none, 3: any possible injury, 9: any possible death	
Ecological concern	0: none, 1: local ecological damage such as localized fire or spill, repairable, 3: permanent local ecological damage, 9: widespread temporary or permanent damage to one or more ecosystems such as the Exxon Valdez or Chernobyl	
Financial impact of compromise on utility	0: Petty cash or less, 1: up to 2% of utility revenue, 3: up to 5%, 9: Greater than 5%	
Restoration costs-cost to return to normal operations, not including any ancillary costs	0: Petty cash or less, 1: < 1% of utility organization O&M budget, 3: <=10%, 9: > 10%	
Negative impact on generation capacity	0: No effect, 1: Small generation facility off-line or degraded operation of large facility, 3: More than 10% loss of generation capacity for 8 hours or less, 9: More than 10% loss of generation capacity for more than 8 hours	
Negative impact on the energy market	0: No effect, 1: localized price manipulation, lost transactions, loss of market participation 3: price manipulation, lost transactions, loss of market participation impacting a large metro area, 9: market or key aspects of market non operational	
Negative impact on the bulk transmission system	0: No, 1: loss of transmission capability to meet peak demand or isolate problem areas, 3: Major transmission system interruption, 9: complete operational failure or shut-down of the transmission system	
Negative impact on customer service	0: No, 1: up to 4 hour delay in customer ability to contact utility, and gain resolution, lasting one day, 3: up to 4 hour delay in customer ability to contact utility and gain resolution, lasting a week, 9: more than 4 hour delay in customer ability to contact utility and gain resolution, lasting more than a week	
Negative impact on billing functions	0: None, 1: isolated recoverable errors in customer bills, 3: widespread but correctible errors in bills, 9: widespread loss of accurate power usage data, unrecoverable	
Destroys goodwill toward utility	0: No effect, 1: negative publicity but this doesn't cause financial loss to utility, 3: negative publicity causing up to 20% less interest in advanced programs, 9: negative publicity causing more than 20% less interest in advanced programs	
Immediate economic damage-refers to functioning of society as a whole	0: none, 1: local businesses down for a week, 3: regional infrastructure damage, 9: widespread runs on banks	
Long term economic damage	0: none, 1: (not used), 3: several year local recession, 9: several year national recession	
Causes a loss of privacy for a significant number of stakeholders	0: none, 1: 1000 or less individuals, 3: 1000's of individuals, 9: millions of individuals	
Total-impact		**0-135**

4.4.1 Impact Criteria Examples

To illustrate the use of the impact criteria table, values are determined for the two failure scenarios included in this technical update. For the AMI failure scenario, the assumption is that the impact will be limited to a single neighborhood. Based on this assumption, the impact criteria table is completed as follows.

Table 4-3
AMI.6 Impact Criteria Score

Criterion	Score
System scale	1
Public safety concern	0
Workforce safety concern	0
Ecological concern	0
Financial impact of compromise on utility	0
Restoration costs-cost to return to normal operations, not including any ancillary costs	1
Negative impact on generation capacity	0
Negative impact on the energy market	0
Negative impact on the bulk transmission system	0
Negative impact on customer service	0
Negative impact on billing functions	1
Destroys goodwill toward utility	1
Immediate economic damage-refers to functioning of society as a whole	0
Long term economic damage	0
Causes a loss of privacy for a significant number of stakeholders	0
Total – impact criteria	4

For the DGM failure scenario, the assumption is that the impact is limited to a few substations. Based on this assumption, the impact criteria table is completed as follows:

Table 4-4
DGM.6 Impact Criteria Score

Criterion	Score
System scale	1
Public safety concern	0
Workforce safety concern	0
Ecological concern	0
Financial impact of compromise on utility	1
Restoration costs-cost to return to normal operations, not including any ancillary costs	1
Negative impact on generation capacity	0
Negative impact on the energy market	0
Negative impact on the bulk transmission system	0
Negative impact on customer service	1
Negative impact on billing functions	0
Destroys goodwill toward utility	1
Immediate economic damage-refers to functioning of society as a whole	0
Long term economic damage	0
Causes a loss of privacy for a significant number of stakeholders	0
Total – impact criteria	5

4.4.2 NESCOR Threat Likelihood Assessment

This is step 2.5 in Figure 2-1. The next step in the process is to determine the threat likelihood. The table below lists criteria that influence the likelihood and opportunity for a threat agent to exploit a failure scenario. A utility can use these criteria to help assess the probability that a cyber security incident will occur. The criteria do not include specific probabilities, because such a prediction was believed to be speculative as well as dependent upon a number of intangible factors for a specific utility. For example, a terrorist organization would be more interested in attacking a “high profile” organization than one that is relatively unknown outside its customer base. For these criteria, scores get higher as the “cost” to the threat agent gets higher and therefore as the likelihood and opportunity decreases.

Skill Required: This criterion rates the skill and specialized knowledge that it takes for a threat agent to cause the failure scenario to occur.

Accessibility (Physical): This criterion scores the difficulty of obtaining physical access that is required to cause a failure scenario. Accessibility ranges from easy and obvious to obtain for anyone, to not feasible to obtain.

Accessibility (Logical): This criterion in similar to the previous one. Logical access refers to any non-physical form of access required to cause a failure scenario, such as network access or a particular utility employee's phone number. The scoring of this criterion assumes that physical access has already been achieved.

Attack Vector: This criterion evaluates how easy it is to obtain the technical means to carry out a failure scenario, once physical and logical accesses have been achieved. The exploit may be simple to carry out with little further effort given physical and logical access. There may be tools available for download from the Internet, or available instructions for the exploit or for similar exploits, or the exploit may be theoretical at this time.

Common vulnerability among others: This criterion acknowledges that a vulnerability shared among many organizations and in many contexts is more likely to be exploited.

Table 4-5
Criteria for Threat Likelihood and Opportunity

Criterion	How to score	Score
Skill required	0: Basic domain understanding and computer skills, 1: Special insider knowledge needed, 3: Domain knowledge and cyber attack techniques, 9: Deep domain/insider knowledge and ability to build custom	
Accessibility (physical)	0: publicly accessible, 1: fence, standard locks, 3: guarded, monitored, 9: Inaccessible	
Accessibility (logical, assume have physical access)	0: common knowledge or none needed, 1: publicly accessible but not common knowledge, 3: not readily accessible, 9: high expertise to gain access	
Attack vector (assume have physical and logical access)	0: straightforward, for example script or tools available, simple once access is obtained, 1: similar attack has occurred, 3: similar attack has been described, 9: theoretical	
Common vulnerability among others	0: Nearly all utilities, 1: Half or more of power infrastructure, 3: More than one utility, 9: Isolated occurrence	
Total – effects on likelihood and opportunity		

4.4.3 Threat Likelihood and Opportunity Examples

The threat likelihood and opportunity score is computed for the two failure scenarios included in this report. For the AMI failure scenario, the threat likelihood and opportunity score is calculated as follows.

Table 4-6
AMI.6 Threat Likelihood and Opportunity Score

Criterion	Score
Skill required	0
Accessibility (physical)	1
Accessibility (logical, assume have physical access)	1
Attack vector (assume have physical and logical access)	1
Common vulnerability among others	0
Total – effects on likelihood and opportunity	3

For the DGM failure scenario, the threat likelihood score is calculated as follows.

Table 4-7
DGM.6 Threat Likelihood and Opportunity Score

Criterion	Score
Skill required	3
Accessibility (physical)	1
Accessibility (logical, assume have physical access)	3
Attack vector (assume have physical and logical access)	3
Common vulnerability among others	0
Total – effects on likelihood and opportunity	10

4.4.4 Risk Ranking/Determination

This is step 2.7 in Figure 2-1. The final step in the process is to determine a risk ranking score using both the threat likelihood and opportunity score and the impact criteria score. The objective is to determine an "attractiveness" measure from the adversary's perspective. The ranking criteria under impact focus on, for example, the delivery of power, the business of the utility, and the interests of its customers. A higher score means that there is a greater impact from the cyber security event. All of the ranking criteria under *likelihood and opportunity* are considered "costs" to the adversary. For example, these criteria focus on the difficulty of the attack and the (lack of) readily available tools to carry out the attack. Attacks that score higher under these criteria have a higher cost to the adversary.

The impact to cost approach creates two intermediate composite results – one for impact (impact criteria) and one for cost to the adversary (threat likelihood and opportunity). Then the impact result is plotted with the cost result on a graph to get a measure of the effect (impact) relative to cost from the point of view of the adversary. This graph represents a risk rank for the failure scenario.

Figure 4-3 below illustrates how the two scores (impact and cost) can be used to determine an overall risk. The X-axis is threat likelihood and opportunity and the Y-axis is impact.

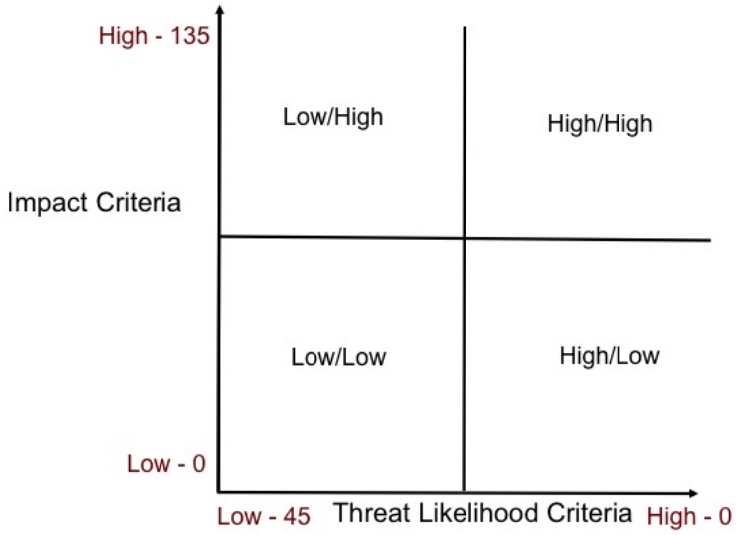

Figure 4-3
Risk Ranking Graph

Systems that fall in the lower right quadrant (high/low) have the lowest impact scores and the highest threat likelihood (the cost to the adversary is low). In the upper right quadrant, the systems have the highest impact scores and the highest threat likelihood (the cost to the adversary is low). These systems are the most likely targets to an adversary because the attacks are the easiest to execute and the potential impact is high. A utility should focus on the systems (or groups of systems) that fall in the upper right quadrant, as they are the highest priority. These are the systems at highest risk. In general, systems that fall in the upper left quadrant should be ranked second because the impact is high even though the threat likelihood is low (the cost to the adversary is high) and those in the lower right quadrant ranked third. However, there may be some mitigation measures that are identified the systems in the upper right quadrant that will be effective for systems in three or four quadrants. These measures should be considered for early deployment.

Within each quadrant, a utility may develop additional prioritization levels. For example, each quadrant may be divided into two or more sub-quadrants. This gives a utility more flexibility in addressing potential vulnerabilities, threat agents, and impacts.

To change the risk exposure of the highest-ranking systems or group of systems, security controls should be implemented to mitigate the potential vulnerabilities. The proposed security controls should be prioritized based on such factors as cost, performance, and usefulness (i.e. can the security control be implemented in multiple systems).

Figure 4-4 below illustrates the placement of the AMI.6 and DGM.6 examples in the Risk Ranking graph. For both of these failure scenarios, the impact level is low and the threat likelihood is high (the cost is low), so they fall within the lower right quadrant. This means that the potential impact level is low and that the attractiveness to an attacker is high (because the cost to the attacker is low).

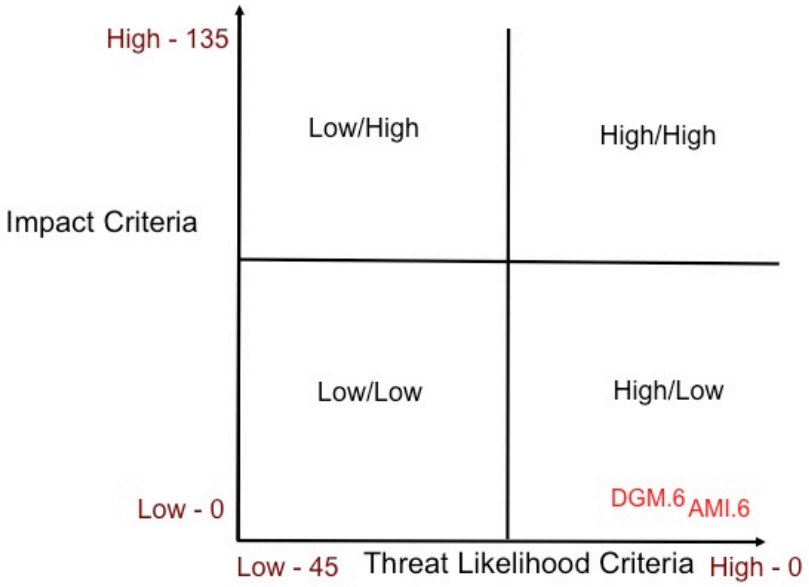

Figure 4-4
Risk Ranking Graph for the Examples

5
CONCLUSION AND NEXT STEPS

This report provides an overview of cyber security risk assessment and includes a basic methodology and risk assessment methodologies for ongoing assessments and emerging changes. The methodology is further refined using the criteria included in the NESCOR Failure Scenarios document and example rankings are provided for two of the failure scenarios.

In the next phase of this project, the ranking methodology will be expanded to consider the common vulnerabilities and the common mitigations. This methodology will be combined with the preliminary metrics approach that was developed using the Department of Energy *Electricity Subsector Cybersecurity Capability Maturity Model* (ES-C2M2) and the NISTIR 7628 security requirements. The goal is to develop a metrics scheme that is applicable to systems, rather than organizations.

IriusRisk
Ex. 1015 - Page 47

6
REFERENCES

1. National Institute of Standards and Technology, Cyber Security Working Group, National Institute of Standards and Technology Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*, August 2010 [government publication].
2. U.S. Department of Energy (DOE), *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2),* Version 1.0, 31 May 2012 [government publication].
3. National Electric Sector Cybersecurity Organization Resource (NESCOR), *Electric Sector Failure Scenarios and Impact Analyses,* Version 1.0, September 2013 [report].
4. National Electric Sector Cybersecurity Organization Resource (NESCOR), *Analysis of Selected Electric Sector High Risk Failure Scenarios,* Version 1.0, September 2013 [report].
5. *Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector*, September 4, 2009 [report].
6. U.S. Department of Energy (DOE), *Electricity Subsector Cybersecurity Risk Management Process*, May 2012 [government publication].

A
VULNERABILITY CLASSES

A.1 People, Policy and Procedures

- ***Training***
  - Insufficiently Trained Personnel
  - Inadequate Security Training and Awareness Program
- ***Policy and Procedures***
  - Insufficient Identity Validation, Background Checks
  - Inadequate Security Policy
  - Inadequate Privacy Policy
  - Inadequate Patch Management Process
  - Inadequate Change and Configuration Management
  - Unnecessary System Access
- ***Risk Management***
  - Inadequate Periodic Security Audits
  - Inadequate Security Oversight by Management
  - Inadequate Continuity of Operations or Disaster Recovery Plan
  - Inadequate Risk Assessment Process
  - Inadequate Risk Management Process
  - Inadequate Incident Response Process

A.2 Platform Software/Firmware Vulnerabilities

- ***Software Development***
  - Code Quality Vulnerability
  - Authentication Vulnerability
  - Authorization Vulnerability
  - Cryptographic Vulnerability
  - Environmental Vulnerability
  - Error Handling Vulnerability
  - Logging and Auditing Vulnerability
  - Password Management Vulnerability
  - Protocol Errors
  - Sensitive Data Protection Vulnerability
  - Insufficient Safeguards for Mobile Code
  - Use of Insecure Protocols

A.3 Platform Vulnerabilities

- ***Design***
  - Use of Inadequate Security Architectures and Designs
  - Lack of External or Peer Review for Security Design
- ***Implementation***
  - Inadequate Malware Protection
  - Installed Security Capabilities Not Enabled by Default
  - Absent or Deficient Equipment Implementation Guidelines
- ***Operational***
  - Lack of Prompt Security Patches from Software Vendors
  - Unneeded Services Running
  - Insufficient Log Management
- ***Poorly Configured Security Equipment***
  - Inadequate Anomaly Tracking

A.4 Network

- ***Network***
  - Inadequate Integrity Checking
  - Inadequate Network Segregation
  - Inappropriate Protocol Selection
  - Weaknesses in Authentication Process or Authentication Keys
  - Insufficient Redundancy
  - Physical Access to the Device

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI's members represent approximately 90 percent of the electricity generated and delivered in the United States, and international participation extends to more than 30 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together…Shaping the Future of Electricity

© 2013 Electric Power Research Institute (EPRI), Inc. All rights reserved.
Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

3002001181

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