

NISTIR 7628 Revision 1

Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References

**The Smart Grid Interoperability Panel
– Smart Grid Cybersecurity Committee**

March 2013

NISTIR 7628 Revision 1

Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References

*The Smart Grid Interoperability Panel
–Smart Grid Cybersecurity Committee*

March 2013



U. S. Department of Commerce

Rebecca M. Blank, Acting Secretary of Commerce and Deputy Secretary of Commerce

National Institute of Standards and Technology

Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

Reports on computer systems technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems.

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate Federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems*, as analyzed in Circular A-130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Interagency Report 7628 Rev. 1, vol. 3
230 pages (March 2013)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by Federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, Federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST publications, other than the ones noted above, are available at <http://csrc.nist.gov/publications>.

ACKNOWLEDGMENTS

This revision to the NISTIR was developed by members of the Smart Grid Interoperability Panel (SGIP) Smart Grid Cybersecurity Committee (SGCC) (formerly the Cyber Security Working Group (CSWG)), which is chaired by Marianne Swanson (NIST). Dave Dalva (Stroz Friedberg), Akhlesh Kaushiva (Department of Energy), and Scott Saunders (Sacramento Municipal Utility District) are the vice chairs and Mark Enstrom (Neustar) was formerly the secretary. Tanya Brewer of NIST is the lead editor of this report. A special note of thanks goes to the subgroup leads, Frances Cleveland (Xanthus Consulting International), Victoria Pillitteri and Nelson Hastings (NIST), Rebecca Herold (Rebecca Herold & Associates, LLC), Elizabeth Sisley (Calm Sunrise Consulting, LLC), and Doug McGinnis (Exelon) who along with their subgroup team members contributed significantly to this revision. The dedication and commitment of all the individuals in developing the original document and now this revision is significant. In addition, appreciation is extended to the various organizations that have committed these resources to supporting this endeavor. Past and current members of the CSWG are listed in Appendix J of this report.

Acknowledgement is also extended to the NIST Smart Grid Team and to Liz Lennon (NIST) for her superb technical editing of this report. Thanks is also extended to Bruce McMillin (Missouri University of Science and Technology), and to Harold Booth and Quynh Dang (NIST) for assistance in updating specific sections in the document. Finally, acknowledgment is extended to all the other individuals who have contributed their time and knowledge to ensure this report addresses the security needs of the Smart Grid.

TABLE OF CONTENTS

OVERVIEW AND REPORT ORGANIZATION.....	VII
Report Overview	vii
Audience.....	vii
Content of the Report	vii
CHAPTER SIX VULNERABILITY CLASSES.....	1
6.1 Introduction.....	1
6.2 People, Policy & Procedure	1
6.3 Platform Software/Firmware Vulnerabilities	6
6.4 Platform Vulnerabilities	22
6.5 Network	26
6.6 References.....	30
CHAPTER SEVEN BOTTOM-UP SECURITY ANALYSIS OF THE SMART GRID	32
7.1 Scope.....	32
7.2 Evident and Specific Cyber Security Problems	32
7.3 Nonspecific Cyber Security Issues	43
7.4 Design Considerations	56
7.5 References.....	63
CHAPTER EIGHT RESEARCH AND DEVELOPMENT THEMES FOR CYBERSECURITY IN THE SMART GRID	65
8.1 Introduction.....	65
8.2 Device-Level Topics—Cost-Effective Tamper-Resistant Device Architectures	66
8.3 Cryptography and Key Management	67
8.4 Systems-Level Topics - Security and Survivability Architecture of the Smart Grid	69
8.5 Networking Topics.....	73
8.6 Other Security Issues in the Smart Grid Context	75
CHAPTER NINE OVERVIEW OF THE STANDARDS REVIEW	89
9.1 Objective.....	89
9.2 Review Process	89
9.3 NIST CSWG Standards Assessment Concepts.....	90
9.4 NIST CSWG Standards Assessment Template.....	94
9.5 Standards Review List	95
CHAPTER TEN KEY POWER SYSTEM USE CASES FOR SECURITY REQUIREMENTS.....	96
10.1 Use Case Source Material	96
10.2 Key Security Requirements Considerations.....	97
10.3 Use Case Scenarios	99
APPENDIX H: LOGICAL ARCHITECTURE AND INTERFACES OF THE SMART GRID.....	143
H.1 Advanced Metering Infrastructure	143
H.2 Distribution Grid Management	147
H.3 Electric Storage.....	151
H.4 Electric Transportation.....	154
H.5 Customer Premises.....	158
H.6 Wide Area Situational Awareness	162
APPENDIX I: ANALYSIS MATRIX OF LOGICAL INTERFACE CATEGORIES	166
APPENDIX J: MAPPINGS TO THE HIGH-LEVEL SECURITY REQUIREMENTS.....	174
J.1 R&D Topics.....	174

J.2 Vulnerability Classes	178
Bottom-up Topics	184
APPENDIX K: GLOSSARY AND ACRONYMS	192
APPENDIX L: SGIP-CSWG AND SGIP 2.0-SGCC MEMBERSHIP	204

LIST OF FIGURES

Figure 9-1 ISO/OSI 7-Layer Reference Model and GWAC Stack Reference Model	91
Figure H-1 Advanced Metering Infrastructure	144
Figure H-2 Distribution Grid Management	148
Figure H-3 Electric Storage	152
Figure H-4 Electric Transportation	155
Figure H-5 Customer Premises	159
Figure H-6 Wide Area Situational Awareness.....	163

LIST OF TABLES

Figure 9-1 ISO/OSI 7-Layer Reference Model and GWAC Stack Reference Model	91
Figure H-1 Advanced Metering Infrastructure	144
Table H-1 AMI Logical Interfaces by Logical Interface Category	145
Figure H-2 Distribution Grid Management	148
Table H-2 DGM Logical Interfaces by Logical Interface Category.....	149
Figure H-3 Electric Storage	152
Table H-3 ES Logical Interfaces by Logical Interface Category	153
Figure H-4 Electric Transportation	155
Table H-4 ET Logical Interfaces by Logical Interface Category	156
Figure H-5 Customer Premises	159
Table H-5 Customer Premises by Logical Interface Category	160
Figure H-6 Wide Area Situational Awareness.....	163
Table H-6 WASA Logical Interfaces by Logical Interface Category	164
Table I-1 Interface Attributes and Descriptions.....	166
Table I-2 Analysis Matrix of Security-Related Logical Interface Categories, Defined by Attributes	168

OVERVIEW AND REPORT ORGANIZATION

REPORT OVERVIEW

This document (the original NISTIR and Revision 1) is the product of a participatory public process that, starting in March 2009, included workshops as well as weekly and bi-weekly teleconferences, all of which were open to all interested parties. Drafts of the three volumes will have undergone at least one round of formal public review before final publication. The public review cycle will be announced in The Federal Register in advance.

AUDIENCE

This report is intended for a variety of organizations that may have overlapping and different perspectives and objectives for the Smart Grid. For example—

- *Utilities/asset owners/service providers* may use this report as guidance for a specific Smart Grid information system implementation;
- *Industry/Smart Grid vendors* may base product design and development, and implementation techniques on the guidance included in this report;
- *Academia* may identify research and development topics based on gaps in technical areas related to the functional, reliability, security, and scalability requirements of the Smart Grid; and
- *Regulators/policy makers* may use this report as guidance to inform decisions and positions, ensuring that they are aligned with appropriate power system and cyber security needs.

CONTENT OF THE REPORT

- Volume 1 – Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements
 - Chapter 1 – *Cybersecurity Strategy* includes background information on the Smart Grid and the importance of cybersecurity in ensuring the reliability of the grid and the confidentiality of specific information. It also discusses the cybersecurity strategy for the Smart Grid and the specific tasks within this strategy.
 - Chapter 2 – *Logical Architecture* includes a high level diagram that depicts a composite high level view of the actors within each of the Smart Grid domains and includes an overall logical reference model of the Smart Grid, including all the major domains. The chapter also includes individual diagrams for each of the 22 logical interface categories. This architecture focuses on a short-term view (1–3 years) of the Smart Grid.
 - Chapter 3 – *High-Level Security Requirements* specifies the high-level security requirements for the Smart Grid for each of the 22 logical interface categories included in Chapter 2.
 - Chapter 4 – *Cryptography and Key Management* identifies technical cryptographic and key management issues across the scope of systems and devices found in the Smart Grid along with potential alternatives.

- Appendix A – *Crosswalk of Cybersecurity Documents*
- Appendix B – *Example Security Technologies and Procedures to Meet the High-Level Security Requirements*
- Volume 2 – Privacy and the Smart Grid
 - Chapter 5 – *Privacy and the Smart Grid* includes a privacy impact assessment for the Smart Grid with a discussion of mitigating factors. The chapter also provides an overview of some existing privacy risk mitigation standards and frameworks. Also includes a description of some methods that can be used to mitigate privacy risks, and points to privacy use cases.
 - Appendix C – *Changing Regulatory Frameworks*
 - Appendix D – *Recommended Privacy Practices for Customer/Consumer Smart Grid Energy usage Data Obtained Directly by Third Parties*
 - Appendix E – *Privacy Use Cases*
 - Appendix F - *Summary of the Smart Grid High-Level Consumer-to-Utility Privacy Impact Assessment*
 - Appendix G – *Privacy Related Definitions*
- Volume 3 – Supportive Analyses and References
 - Chapter 6 – *Vulnerability Classes* includes classes of potential vulnerabilities for the Smart Grid. Individual vulnerabilities are classified by category.
 - Chapter 7 – *Bottom-Up Security Analysis of the Smart Grid* identifies a number of specific security problems in the Smart Grid. Currently, these security problems do not have specific solutions.
 - Chapter 8 – *Research and Development Themes for Cybersecurity in the Smart Grid* includes R&D themes that identify where the state of the art falls short of meeting the envisioned functional, reliability, and scalability requirements of the Smart Grid.
 - Chapter 9 – *Overview of the Standards Review* includes an overview of the process that is being used to assess standards against the high level security requirements included in this report.
 - Chapter 10 – *Key Power System Use Cases for Security Requirements* identifies key use cases that are architecturally significant with respect to security requirements for the Smart Grid.
 - Appendix H – *Logical Architecture and Interfaces of the Smart Grid*
 - Appendix I – *Analysis Matrix of Interface Categories*
 - Appendix J – *Mappings to the High Level Security Requirements*
 - Appendix K – *Glossary and Acronyms*
 - Appendix L – *SGIP-CSWG/SGCC Membership*

1 **CHAPTER SIX**
2 **VULNERABILITY CLASSES**

3 **6.1 INTRODUCTION**

4 This section is intended to be used by those responsible for designing, implementing, operating
5 or procuring some part of the electric grid. It contains a list of five classes of potential
6 vulnerabilities with descriptions of specific areas that can make an organization vulnerable as
7 well as the possible impacts to an organization should the vulnerability be exercised. For the
8 purpose of this document, a vulnerability class is a category of weakness which could adversely
9 impact the operation of the electric grid. A “vulnerability” is a weakness in an information
10 system, system security procedures, internal controls, or implementation that could be exploited
11 or triggered by a threat source. This document contains a number of possible vulnerabilities,
12 identified by management, operational and technical categories. It is best used as a stimulus for
13 detailed risk analysis of real or proposed systems, and while it was created from many sources of
14 vulnerability information, including NIST Special Publication (SP) 800-82, *Guide to Industrial*
15 *Control Systems Security*, and 800-53 Rev. 3, *Recommended Security Controls for Federal*
16 *Information Systems and Organizations*, Open Web Application Security Project (OWASP)
17 vulnerabilities, Common Weakness Enumeration (CWE) vulnerabilities, attack documentation
18 from Idaho National Laboratory (INL), input provided by the NIST CSWG Bottom-Up group,
19 and the North American Electric Reliability Corporation Critical Infrastructure Protection
20 Standards (NERC CIP) standards, it is just a starting point for more detailed vulnerability
21 identification in future CSWG work efforts.

22 **6.2 PEOPLE, POLICY & PROCEDURE**

23 *Policies and procedures* are the documented mechanisms by which an organization operates, and
24 *people* are trained to follow them. Policies and procedures lay the groundwork for how the
25 organization will operate; adequate training ensures that people understand how to and are
26 responsible for implementing the policy and procedures. Individually, each is not effective
27 without the others and should not be implemented as discreet elements. This section discusses
28 cases where a failure in, lack of, or deficiency in policies and procedures can lead to security
29 risks for the organization. An organization’s policies and procedures are often the final protective
30 or mitigating control against security breaches, and those policies and procedures should be
31 examined closely to ensure that they are consistent with both the inherent business objectives and
32 with secure operations.

33 **6.2.1 Training**

34 This category of vulnerabilities is related to personnel security awareness training associated
35 with implementing, maintaining, and operating systems.

36 **6.2.1.1 Insufficiently Trained Personnel**

37 **Description**

38 Throughout the entire organization everyone needs to acquire a level of security awareness
39 training; the degree of training should vary based on the technical responsibilities and/or the
40 critical assets one is responsible for.

41 Through training, everyone in the organization gets a clear understanding of the importance of
42 cyber security, but more importantly everyone begins to understand the role they play and the
43 importance of each role in supporting security.

44 **Examples**

- 45 • Freely releasing information of someone's status, i.e. away on vacation, not in today, etc.,
- 46 • Opening emails and attachments from unknown sources,
- 47 • Posting passwords for all to see,
- 48 • Allowing people to dumpster-dive without alerting security, and
- 49 • Failure to notice inappropriate or suspicious network cables/devices outside the building.

50 **Potential Impact:**

51 Social engineering is used in acquiring as much information as possible about people,
52 organizations and organizational operations. Insufficiently trained personnel may inadvertently
53 provide the visibility, knowledge and opportunity to execute a successful attack.

54 **6.2.1.2 Inadequate Security Training and Awareness Program**

55 **Description**

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

61 **Potential Impact**

62 An inadequately trained workforce will not be aware of the policies and procedures necessary to
63 secure organizational information and equipment, resulting in the potential for weaknesses to be
64 exploited, for example:

- 65 • Inserting malicious USB sticks found in the parking lot into machines with access to
66 control systems providing attackers control over the control systems.
- 67 • Holding the door for potential attackers carrying a big box entering a "secured premise",
68 allowing them unauthorized access and physical proximity to critical / control systems.
- 69 • Surfing porn sites, which often includes 0-day exploits and can compromise workstations
70 with bots or worms.

- 71 • Failing to respond to someone capturing wireless network traffic on the front lawn or
72 parked in the guest parking lot, and
- 73 • Lack of care with id badges and credentials which can be leveraged to gain partial or
74 complete access to critical control systems.

75 **6.2.2 Policy & Procedure**

76 **6.2.2.1 Insufficient Identity Validation, Background Checks**

77 **Description**

78 Identity validation/background checks are based on the individual's area of responsibility, the
79 physical facilities/hardware/systems, and the type of information authorized to access. The more
80 sensitive information available to an individual, the deeper and more detailed the identity
81 validation and background check process should be.

82 Use of known references and background checks by established groups should be implemented.

83 **Potential Impact**

84 The human factor must always be considered the weakest element within any organization's
85 security posture, thus identity validation and background checks are measures that are imperative
86 in managing this risk. As the amount and sensitivity of the information and physical access to
87 critical facilities/hardware/systems one is given responsibility for increases, consideration should
88 be given to requiring separation of duties to ensure that no one individual is given "the keys to
89 the kingdom."

90 **6.2.2.2 Inadequate Security Policy**

91 **Description**

92 Security policies must be structured with several key elements, be well understood, embody a
93 practical approach, be well practiced and monitored, and be enforceable.

94 Additionally, they must be flexible enough that they can be continuously improved.

95 **Potential Impact**

96 Vulnerabilities are often introduced due to inadequate development or implementation policies
97 or the lack of policies. Policies need to drive operating requirements and procedures, including
98 security training.

99 **6.2.2.3 Inadequate Privacy Policy**

100 **Description**

101 A privacy policy should be established that documents the necessity of protecting
102 private/personal information to ensure that data is not exposed or shared unnecessarily.

103 **Potential Impact**

104 Insufficient privacy policies can lead to unwanted exposure of employee or customer/client
105 personal information, leading to both business risk and security risk.

106 **6.2.2.4 Inadequate Patch Management Process**

107 **Description**

108 A patch management process is necessary to ensure that software and firmware are kept current
109 to remediate against known vulnerabilities, or that a proper risk analysis and mitigation process
110 is in place when patches cannot be promptly installed.

111 **Potential Impact**

112 Missing patches on firmware and software have the potential to present serious risk to the
113 affected system.

114 **6.2.2.5 Inadequate Change and Configuration Management**

115 **Description**

116 Change and configuration management processes are essential to ensuring that system
117 configurations are governed appropriately in order to maximize overall system reliability.

118 **Examples**

- 119 • Changing software configuration enables an insecure profile,
- 120 • Adding vulnerable hardware,
- 121 • Changing network configuration that reduces the security profile of the system,
- 122 • Introduction of tampered devices into the system,
- 123 • Security organization not having a sign-off approval in the configuration management
124 process, and
- 125 • Making a change to network configuration or software and failing to document that
126 change.

127 **Potential Impact**

128 Improperly configured software/systems/devices added to existing software/systems/devices can
129 lead to insecure configurations and increased risk of vulnerability.

130 **6.2.2.6 Unnecessary System Access**

131 **Description**

132 As a matter of policy, it needs to be very clear that system access and information is granted only
133 on an as-needed basis. System access needs to be managed, monitored, and enforced based on
134 the individual's access requirements and the level of impact that uncontrolled access could have
135 on an organization.

136 **Potential Impact**

137 System access that is not managed can result in personnel obtaining, changing or deleting
138 information they are no longer authorized to access, as well as:

- 139 • Administrators with false assumptions of what actions any one user may be capable of;
- 140 • Individual users with sufficient access permissions to cause complete failure or failure of
- 141 large portions of the electric grid;
- 142 • The inability to prove responsibility for a given action or hold a party accountable;
- 143 • Accidental disruption of service by untrained individuals; and
- 144 • Raised value for credentials of seemingly insignificant personnel.

145 **6.2.3 Risk Management**

146 Deficiencies in a risk management program can lead to vulnerabilities throughout the
147 organization. A well documented and implemented risk management program that encompasses
148 the organization-wide level, mission and business process level, and IT and ICS system level will
149 provide an in depth defense against many potential vulnerabilities.¹

150 **6.2.3.1 Inadequate Periodic Security Audits**

151 **Description**

152 Conducting independent security audits as part of the organization's continuous monitoring
153 program should review and examine a system's records and activities to determine the adequacy
154 of system security requirements and ensure compliance with established security policies and
155 procedures. Audits should also be used to detect breaches in security services and recommend
156 changes, which may include making existing security requirements more robust and/or adding
157 new security requirements. Audits should not rely exclusively on interviews with system
158 administrators.

159 **Potential Impact**

160 The audit process is the only true measure by which it is possible to continuously evaluate the
161 status of the implemented security program in terms of conformance to policy, determine
162 whether there is a need to enhance policies and procedures, and evaluate the robustness of the
163 implemented security technologies.

164 **6.2.3.2 Inadequate Security Oversight by Management**

165 **Description**

166 An overall security program requires coordination and communication between organizational
167 operating groups, has impact across many business areas, and requires an element of human
168 resources and legal involvement. Without senior management oversight and ownership, it is very
169 difficult to maintain a successful security program. A significant challenge can exist in
170 establishing senior management oversight and ownership at the executive level within an
171 organization.

¹ For more on this topic, please see the Department of Energy *Risk Management Process* guideline at <http://energy.gov/node/368191>.

172 **Potential Impact**

173 Lack of clear senior management ownership of a security program makes it almost impossible to
174 enforce the provisions of the program in the event of a policy being compromised or abused.

175 **6.2.3.3 Inadequate Continuity of Operations or Disaster Recovery Plan**

176 **Description**

177 As part of the organization's incident response capabilities, it is essential to ensure within the
178 various control system disaster recovery plans that an associated cyber contingency plan and
179 cyber security incident response plan is developed. Each plant/system disaster recovery plan
180 should highlight the need to determine if the disaster resulted from or is related to a cyber
181 security incident. If such is the case, then part of the recovery process must be to ensure cyber
182 incident recovery and contingency activities are implemented. This means taking added steps
183 like validating backups, ensuring devices being recovered are clean before installing the backups,
184 incident reporting, etc.

185 **Potential Impact**

186 An inadequate continuity of operations or disaster recovery plan could result in longer than
187 necessary recovery from a possible plant or operational outage.

188 **6.2.3.4 Inadequate Risk Assessment Process**

189 **Description**

190 A documented risk assessment process should include consideration of business objectives, the
191 impact to the organization if vulnerabilities are exploited, and the determination of the acceptable
192 risk level by senior management is necessary to evaluate risk to the organization.

193 **Potential Impact**

194 Lack or misapplication of adequate risk assessment processes can lead to poor decisions based
195 on inadequate understanding of actual risk.

196 **6.2.3.5 Inadequate Incident Response Process**

197 **Description**

198 An incident response process is required to ensure proper notification, response, and recovery in
199 the event of an incident. Incident response capabilities should be coordinated with continuity of
200 operations and disaster recovery capabilities.

201 **Potential Impact**

202 Without a sufficient incident response process, response-time critical actions may not be
203 completed in a timely manner, leading to increased duration of risk exposure.

204 **6.3 PLATFORM SOFTWARE/FIRMWARE VULNERABILITIES**

205 Software and firmware are the programmable components of a computing environment. Errors
206 or oversights in software and firmware design, development, and deployment may result in

207 unintended functionality that allows attackers or other conditions to affect, via programmatic
208 means, the confidentiality, integrity, and/or availability of information. These errors and
209 oversights are discovered and reported as vulnerability instances in platform software and
210 firmware. Discovery and reporting of vulnerability instances occurs continuously and the
211 Common Vulnerability and Exposures (CVE) specification establishes a common identifier for
212 known vulnerability instances. [§6.6-5] The Common Weakness Enumeration (CWE) [§6.6-4]
213 and the Vulnerability Categories defined by OWASP [§6.6-1] are two taxonomies which provide
214 descriptions of common errors or oversights that can result in vulnerability instances. Using the
215 CWE and OWASP taxonomies as a guide this subsection describes classes and subclasses of
216 vulnerabilities in platform software and firmware².

217 **6.3.1 Software Development**

218 Applications being developed for use in the Smart Grid should make use of a secure software
219 development life cycle (SDLC). Vulnerabilities in this category can arise from a lack of
220 oversight in this area, leading to poor code implementation, leading to vulnerability.

221 **6.3.1.1 Code Quality Vulnerability (CWE-398)**

222 **Description**

223 “Poor code quality,” states OWASP, “leads to unpredictable behavior. From a user’s perspective
224 that often manifests itself as poor usability. For an attacker it provides an opportunity to stress
225 the system in unexpected ways.” [§6.6-1]

226 **Examples**

- 227 • Double free() errors (CWE-415),
- 228 • Failure to follow guideline/specification (CWE-573),
- 229 • Leftover debug code (CWE-489),
- 230 • Memory leak (CWE-401),
- 231 • Null dereference (CWE-476, CWE-690),
- 232 • Poor logging practice (CWE-778),
- 233 • Portability flaw (CWE-474, CWE-589),
- 234 • Undefined behavior (CWE-475),
- 235 • Uninitialized variable (CWE-457),
- 236 • Unreleased resource (CWE-404),
- 237 • Unsafe mobile code (CWE-490),
- 238 • Use of obsolete methods (CWE-477),
- 239 • Using freed memory (CWE-416), and

² The OWASP names are generally used with the exact or closest CWE-ID(s) match in parentheses. The mappings are informational only and are not to be considered authoritative.

240 • Buffer overflow (CWE-120).

241 **6.3.1.2 Authentication Vulnerability (CWE-287)**

242 **Description**

243 Authentication is the process of proving an identity to a given system. Users, applications, and
244 devices may all require authentication. This class of vulnerability leads to authentication bypass
245 or other circumvention/manipulation of the authentication process.

246 **Examples [§6.6-1]**

- 247 • CVE-2012-3024 - Tridium Niagara AX Framework through 3.6 uses predictable values for
248 (1) session IDs and (2) keys, which might allow remote attackers to bypass authentication via
249 a brute-force attack;
- 250 • CVE-2012-1799 - The web server on the Siemens Scalance S Security Module firewall S602
251 V2, S612 V2, and S613 V2 with firmware before 2.3.0.3 does not limit the rate of
252 authentication attempts, which makes it easier for remote attackers to obtain access via a
253 brute-force attack on the administrative password;
- 254 • CVE-2012-1808 - The web server in the ECOM Ethernet module in Koyo H0-ECOM, H0-
255 ECOM100, H2-ECOM, H2-ECOM-F, H2-ECOM100, H4-ECOM, H4-ECOM-F, and H4-
256 ECOM100 does not require authentication, which allows remote attackers to perform
257 unspecified functions via unknown vectors;
- 258 • Allowing password aging (CWE-263),
- 259 • Authentication bypass via assumed-immutable data (CWE-302),
- 260 • Empty string password (CWE-258),
- 261 • Failure to drop privileges when reasonable (CWE-271),
- 262 • Hard-coded password (CWE-259),
- 263 • Not allowing password aging (CWE-262),
- 264 • Often misused: authentication (CWE-247),
- 265 • Reflection attack in an auth protocol (CWE-301),
- 266 • Unsafe mobile code (CWE-490),
- 267 • Using password systems (CWE-309),
- 268 • Using referrer field for authentication or authorization (CWE-293), and
- 269 • Using single-factor authentication (CWE-308).

270 **Potential Impact**

271 Access is granted without official permission.

272 **6.3.1.3 Authorization Vulnerability (CWE-284)**

273 **Description**

274 Authorization is the process of assigning correct system permissions to an authenticated entity.
275 This class of vulnerability allows authenticated entities the ability to perform actions which
276 policy does not allow.

277 **Examples**

- 278 • Access control enforced by presentation layer (CWE-602, CWE-425),
- 279 • File access race condition: time-of-check, time-of-use (TOCTOU) (CWE-367),
- 280 • Least privilege violation (CWE-272),
- 281 • Often misused: privilege management (CWE-250),
- 282 • Using referrer field for authentication or authorization (CWE-293),
- 283 • Insecure direct object references (CWE-639, CWE-22), and
- 284 • Failure to restrict universal resource locator (URL) access (CWE-425, CWE-288).

285 **6.3.1.4 Cryptographic Vulnerability (CWE-310)**

286 **Description**

287 Cryptography is the use of mathematical principles and their implementations to ensure that
288 information is hidden from unauthorized parties, the information is unchanged, and the intended
289 party can verify the sender. This vulnerability class includes issues that allow an attacker to
290 view, modify, or forge encrypted data or impersonate another party through digital signature
291 abuse.

292 **Examples**

- 293 • CVE-2012-4899 - WellinTech KingView 6.5.3 and earlier uses a weak password-hashing
294 algorithm, which makes it easier for local users to discover credentials by reading an
295 unspecified file;
- 296 • CVE-2012-3025 - The default configuration of Tridium Niagara AX Framework through 3.6
297 uses a cleartext base64 format for transmission of credentials in cookies, which allows
298 remote attackers to obtain sensitive information by sniffing the network;
- 299 • Failure to encrypt data (CWE-311),
- 300 • Insecure Randomness (CWE-330),
- 301 • Insufficient Entropy (CWE-332),
- 302 • Insufficient Session-ID Length (CWE-6),
- 303 • Key exchange without entity authentication (CWE-322),
- 304 • Non-cryptographic pseudo-random number generator (CWE-338),
- 305 • Not using a random initialization vector with cipher block chaining mode (CWE-329),

- 306 • PRNG Seed Error (CWE-335),
- 307 • Password Management: Weak Cryptography (CWE-261),
- 308 • Reusing a nonce, key pair in encryption (CWE-323),
- 309 • Testing for SSL-TLS (OWASP-CM-001) (CWE-326),
- 310 • Use of hard-coded cryptographic key (CWE-321),
- 311 • Using a broken or risky cryptographic algorithm (CWE-327), and
- 312 • Using a key past its expiration date (CWE-324).

313 **6.3.1.5 Environmental Vulnerability (CWE-2)**

314 **Description**

315 “This category,” states OWASP, “includes everything that is outside of the source code but is
316 still critical to the security of the product that is being created. Because the issues covered by this
317 kingdom are not directly related to source code, we separated it from the rest of the kingdoms.”
318 [§6.6-1]

319 **Examples**

- 320 • ASP.NET misconfigurations (CWE-10),
- 321 • Empty string password (CWE-258),
- 322 • Failure of true random number generator (CWE-333),
- 323 • Information leak through class cloning (CWE-498),
- 324 • Information leak through serialization (CWE-499),
- 325 • Insecure compiler optimization (CWE-14),
- 326 • Insecure transport (CWE-319, CWE-5),
- 327 • Insufficient session-ID length (CWE-6),
- 328 • Insufficient entropy in pseudo-random number generator (CWE-332),
- 329 • J2EE misconfiguration: unsafe bean declaration (CWE-8),
- 330 • Missing error handling (CWE-7),
- 331 • Publicizing of private data when using inner classes (CWE-492),
- 332 • Relative path library search (CWE-428),
- 333 • Reliance on data layout (CWE-188),
- 334 • Relying on package-level scope (CWE-487),
- 335 • Resource exhaustion (CWE-400), and
- 336 • Trust of system event data (CWE-360).

337 **6.3.1.6 Error Handling Vulnerability (CWE-703)**

338 **Description**

339 Error handling refers to the way an application deals with unexpected conditions - generally
340 syntactical or logical. Vulnerabilities in this class provide means for attackers to use error
341 handling to access unintended information or functionality.

342 **Examples**

- 343 • ASP.NET misconfigurations (CWE-10),
- 344 • Catch NullPointerException (CWE-395),
- 345 • Empty catch block (CWE-600),
- 346 • Improper cleanup on thrown exception (CWE-460),
- 347 • Improper error handling (CWE-390),
- 348 • Information leakage (CWE-200),
- 349 • Missing error handling (CWE-7),
- 350 • Often misused: exception handling (CWE-248),
- 351 • Overly-broad catch block (CWE-396),
- 352 • Overly-broad throws declaration (CWE-397),
- 353 • Return inside finally block (CWE-584),
- 354 • Uncaught exception (CWE-248),
- 355 • Unchecked error condition (CWE-391), and
- 356 • Unrestricted File Upload (CWE-434).

357 **6.3.1.7 General Logic Error (CWE-691)**

358 **Description**

359 Logic errors are programming missteps that allow an application to operate incorrectly, but
360 usually without crashing. This vulnerability class covers those error types that have security
361 implications.

362 **Examples**

- 363 • Addition of data-structure sentinel (CWE-464),
- 364 • Assigning instead of comparing (CWE-481),
- 365 • Comparing instead of assigning (CWE-482),
- 366 • Deletion of data-structure sentinel (CWE-463),
- 367 • Duplicate key in associative list (CWE-462),
- 368 • Failure to check whether privileges were dropped successfully (CWE-273),

- 369 • Failure to de-allocate data (CWE-401),
- 370 • Failure to provide confidentiality for stored data (CWE-493),
- 371 • Guessed or visible temporary file (CWE-379),
- 372 • Improper cleanup on thrown exception (CWE-460),
- 373 • Improper error handling (CWE-390),
- 374 • Improper temp file opening (CWE-378),
- 375 • Incorrect block delimitation (CWE-483),
- 376 • Misinterpreted function return value (CWE-253),
- 377 • Missing parameter (CWE-234),
- 378 • Omitted break statement (CWE-484),
- 379 • Passing mutable objects to an untrusted method (CWE-375),
- 380 • Symbolic name not mapping to correct object (CWE-386),
- 381 • Truncation error (CWE-197),
- 382 • Undefined Behavior (CWE-475),
- 383 • Uninitialized Variable (CWE-457),
- 384 • Unintentional pointer scaling (CWE-468),
- 385 • Use of sizeof() on a pointer type (CWE-467), and
- 386 • Using the wrong operator (CWE-480).

387 **6.3.1.8 Business logic Vulnerability**

388 **Description**

389 Business logic vulnerabilities occur when the legitimate processing flow of an application is used
 390 in a way that results in an unintended consequence. Discovery and testing of this vulnerability
 391 class tends to be specific to an application under analysis and require detailed knowledge of the
 392 business process. Additional information on this vulnerability may be found at [§6.6-10].

393 **Examples**

- 394 • Purchase orders are not processed before midnight,
- 395 • Written authorization is not on file before web access is granted, and
- 396 • Transactions in excess of \$2000 are not reviewed by a person.

397 **6.3.1.9 Input and Output Validation (CWE-20 AND CWE-116)**

398 **Description**

399 Input validation is the process of ensuring that the user-supplied content contains only expected
 400 information. Input validation covers a wide assortment of potential exploitation but requires
 401 caution. Failing to properly validate external input may allow execution of unintended

402 functionality—and often “arbitrary code execution”. Output validation is encoding or escaping
403 data during the preparation of a structured message for communication with another component.
404 Improper output validation can allow attackers to change or replace the commands sent to other
405 components.

406 **Examples**

- 407 • CVE-2012-3026 - rifsrvd.exe in the Remote Interface Service in GE Intelligent Platforms
408 Proficy Real-Time Information Portal 2.6 through 3.5 SP1 allows remote attackers to
409 cause a denial of service (memory corruption and service crash) or possibly execute
410 arbitrary code via long input data,
- 411 • CVE-2012-3021 - APIFTP Server in Optimalog Optima PLC 1.5.2 and earlier allows
412 remote attackers to cause a denial of service (infinite loop) via a malformed packet,
- 413 • Buffer overflow (CWE-120),
- 414 • Format string (CWE-134),
- 415 • Improper data validation (CWE-102, CWE-103, CWE-104, CWE-105, CWE-106, CWE-
416 107, CWE-108, CWE-109, CWE-110),
- 417 • Log forging (CWE-117),
- 418 • Missing XML validation (CWE-112),
- 419 • Process control (CWE-114),
- 420 • String termination error (CWE-158),
- 421 • Unchecked return value: missing check against null (CWE-690, CWE-252),
- 422 • Unsafe Java Native Interface (JNI) (CWE-111),
- 423 • Unsafe reflection (CWE-470),
- 424 • Validation performed in client (CWE-602),
- 425 • Unvalidated redirects and forwards (CWE-819), and
- 426 • Improper Neutralization of HTTP Headers for Scripting Syntax (CWE-664).

427 **6.3.1.10 Logging and Auditing Vulnerability (CWE-778 and CWE-779)**

428 **Description**

429 Logging and auditing are common system and security functions aiding in system management,
430 event identification, and event reconstruction. This vulnerability class deals with issues that
431 either aid in an attack or increase the likelihood of its success due to logging and auditing.

432 **Examples**

- 433 • Addition of data-structure sentinel (CWE-464),
- 434 • Information leakage (CWE-200),
- 435 • Log forging (CWE-117),

- 436 • Log injection (CWE-117),
- 437 • Poor logging practice, and
- 438 • Cross-site scripting via HTML log-viewers (CWE-79, CWE-117).

439 **6.3.1.11 Password Management Vulnerability (CWE-255)**

440 **Description**

441 Passwords are the most commonly used form of authentication. This class of vulnerabilities deals
442 with mistakes in handling passwords that may allow an attacker to obtain or guess them.

443 **Examples**

- 444 • CVE-2012-4879 - The Linux Console on the WAGO I/O System 758 model 758-870,
445 758-874, 758-875, and 758-876 Industrial PC (IPC) devices has a default password of
446 wago for the (1) root and (2) admin accounts, (3) a default password of user for the user
447 account, and (4) a default password of guest for the guest account, which makes it easier
448 for remote attackers to obtain login access via a TELNET session,
- 449 • CVE-2012-3013 - WAGO I/O System 758 model 758-870, 758-874, 758-875, and 758-
450 876 Industrial PC (IPC) devices have default passwords for unspecified Web Based
451 Management accounts, which makes it easier for remote attackers to obtain
452 administrative access via a TCP session,
- 453 • CVE-2012-3014 - The Management Software application in GarrettCom Magnum MNS-
454 6K before 4.4.0, and 14.x before 14.4.0, has a hardcoded password for an administrative
455 account, which allows local users to gain privileges via unspecified vectors,
- 456 • Empty string password (CWE-258),
- 457 • Hard-coded password (CWE-259),
- 458 • Not allowing password aging (CWE-262),
- 459 • Password management: hardcoded password (CWE-259),
- 460 • Password management: weak cryptography (CWE-261),
- 461 • Password plaintext storage (CWE-256),
- 462 • Password in configuration file (CWE-260), and
- 463 • Using password systems (CWE-309).

464 **6.3.1.12 Path Vulnerability (CWE-21)**

465 **Description**

466 “This category [Path Vulnerability],” states OWASP, “is for tagging path issues that allow
467 attackers to access files that are not intended to be accessed. Generally, this is due to dynamically
468 construction of a file path using unvalidated user input.” [§6.6-1]

469 **Examples**

- 470 • Path traversal attack (CWE-22),
- 471 • Relative path traversal attack (CWE-23),
- 472 • Virtual files attack (CWE-66),
- 473 • Path equivalence attack (CWE-41), and
- 474 • Link following attack (CWE-59).

475 **6.3.1.13 Protocol Errors (CWE-254, CWE-573, CWE-668)**

476 **Description**

477 Protocols are rules of communication. This vulnerability class deals with the security issues
478 introduced during protocol design.

479 **Examples**

- 480 • Failure to add integrity check value (CWE-353),
- 481 • Failure to check for certificate revocation (CWE-299),
- 482 • Failure to check integrity check value (CWE-354),
- 483 • Failure to encrypt data (CWE-311),
- 484 • Failure to follow chain of trust in certificate validation (CWE-296),
- 485 • Failure to protect stored data from modification (CWE-766, CWE-767),
- 486 • Failure to validate certificate expiration (CWE-298),
- 487 • Failure to validate host-specific certificate data (CWE-297),
- 488 • Key exchange without entity authentication (CWE-322),
- 489 • Storing passwords in a recoverable format (CWE-257),
- 490 • Trusting self-reported domain name service (DNS) name (CWE-292),
- 491 • Trusting self-reported IP address (CWE-291),
- 492 • Use of hard-coded password (CWE-798, CWE-259),
- 493 • Insufficient transport layer protection (CWE-818),
- 494 • Use of weak secure socket layer / transport layer security (SSL/TLS) protocols (CWE-
495 757),
- 496 • SSL/TLS key exchange without authentication (CWE-322),
- 497 • SSL/TLS weak key exchange (CWE-326), and
- 498 • Low SSL/TLS cipher strength (CWE-326).

499 **Potential Impact**

500 The compromise of security protocols such as TLS.

501 **6.3.1.14 Range and Type Error Vulnerability (CWE-118, CWE-136)**

502 **Description**

503 Range and type errors are common programming mistakes. This vulnerability class covers the
504 various types of errors that have potential security consequences.

505 **Examples**

- 506 • Access control enforced by presentation layer (CWE-602, CWE-425),
- 507 • Buffer overflow (CWE-120),
- 508 • Buffer underwrite (CWE-124),
- 509 • Comparing classes by name (CWE-486),
- 510 • De-serialization of untrusted data (CWE-502),
- 511 • Doubly freeing memory (CWE-415),
- 512 • Failure to account for default case in switch (CWE-478),
- 513 • Format string (CWE-134),
- 514 • Heap overflow (CWE-122),
- 515 • Illegal pointer value (CWE-466),
- 516 • Improper string length checking (CWE-135),
- 517 • Integer coercion error (CWE-192),
- 518 • Integer overflow (CWE-190, CWE-680),
- 519 • Invoking untrusted mobile code (CWE-494),
- 520 • Log forging (CWE-117),
- 521 • Log injection (CWE-117),
- 522 • Miscalculated null termination (CWE-170),
- 523 • Null dereference (CWE-476, CWE-690),
- 524 • Often misused: string management (CWE-251),
- 525 • Reflection injection (CWE-470),
- 526 • Sign extension error (CWE-194),
- 527 • Signed to unsigned conversion error (CWE-195),
- 528 • Stack overflow (CWE-121),
- 529 • Truncation error (CWE-197),

- 530 • Trust boundary violation (CWE-501),
- 531 • Unchecked array indexing (CWE-129),
- 532 • Unsigned to signed conversion error (CWE-196),
- 533 • Using freed memory (CWE-416),
- 534 • Validation performed in client (CWE-602), and
- 535 • Wrap-around error (CWE-128).

536 **6.3.1.15 Sensitive Data Protection Vulnerability (CWE-199)**

537 **Description**

538 OWASP describes the sensitive data protection vulnerability as follows:

539 This category is for tagging vulnerabilities that lead to insecure protection of sensitive
540 data. The protection referred here includes confidentiality and integrity of data during its
541 whole life cycles, including storage and transmission.

542 Please note that this category is intended to be different from access control problems,
543 although they both fail to protect data appropriately. Normally, the goal of access control
544 is to grant data access to some users but not others. In this category, we are instead
545 concerned about protection for sensitive data that are not intended to be revealed to or
546 modified by any application users. Examples of this kind of sensitive data can be
547 cryptographic keys, passwords, security tokens or any information that an application
548 relies on for critical decisions. [§6.6-1]

549 **Examples**

- 550 • Information leakage results from insufficient memory clean-up (CWE-226),
- 551 • Inappropriate protection of cryptographic keys³ (CWE-311, CWE-326, CWE-321, CWE-
552 325, CWE-656),
- 553 • Lack of integrity protection for stored user data (CWE-693),
- 554 • Hard-coded password (CWE-259),
- 555 • Heap inspection (CWE-244),
- 556 • Information leakage (CWE-200),
- 557 • Password management: hardcoded password (CWE-259),
- 558 • Password plaintext storage (CWE-256), and
- 559 • Privacy violation (CWE-359).

³ http://www.owasp.org/index.php/Top_10_2007-Insecure_Cryptographic_Storage

560 **6.3.1.16 Session Management Vulnerability (CWE-718)**

561 **Description**

562 Session management is the way with which a client and server connect, maintain, and close a
563 connection. Primarily an issue with Web interfaces, this class covers vulnerabilities resulting
564 from poor session management.

565 **Examples**

- 566 • Applications should not use variables that include any user personal information (user
567 name, password, home address, etc.),
- 568 • Highly protected applications should not implement mechanisms that make automated
569 requests to prevent session timeouts,
- 570 • Highly protected applications should not implement "remember me" functionality,
- 571 • Highly protected applications should not use URL rewriting to maintain state when
572 cookies are turned off on the client,
- 573 • Applications should not use session identifiers for encrypted HTTPS transport that have
574 once been used over HTTP,
- 575 • Insufficient Session-ID Length (CWE-6),
- 576 • Session Fixation (CWE-384),
- 577 • Cross site request forgery (CWE-352),
- 578 • Cookie attributes not set securely (e.g. domain, secure and HTTP only) (CWE-614), and
579 • Overly long session timeout (CWE-613).

580 **6.3.1.17 Concurrency, Synchronization and Timing Vulnerability (CWE-361)**

581 **Description**

582 Concurrency, synchronization and timing deals with the order of events in a complex computing
583 environment. This vulnerability class deals with timing issues that affect security, most often
584 dealing with multiple processes or threads which share some common resource (file, memory,
585 etc.).

586 **Examples**

- 587 • Capture-replay (CWE-294),
- 588 • Covert timing channel (CWE-385),
- 589 • Failure to drop privileges when reasonable (CWE-271, CWE-653),
- 590 • Failure to follow guideline/specification (CWE-573),
- 591 • File access race condition: TOCTOU (CWE-367),
- 592 • Member field race condition (CWE-488),

- 593 • Mutable object returned (CWE-375),
- 594 • Overflow of static internal buffer (CWE-500),
- 595 • Race conditions (CWE-362),
- 596 • Reflection attack in an auth protocol (CWE-301),
- 597 • State synchronization error (CWE-373), and
- 598 • Unsafe function call from a signal handler (CWE-479).

599 **6.3.1.18 Insufficient Safeguards for Mobile Code (CWE-490)**

600 **Description**

601 Mobile code consists of programming instructions transferred from server to client that execute
 602 on the client machine without the user explicitly initiating that execution. Allowing mobile code
 603 generally increases attack surface. This subsection includes issues that permit the execution of
 604 unsafe mobile code.

605 **Examples**

- 606 • VBScript, JavaScript and Java sandbox container flaws,
- 607 • Insufficient scripting controls, and
- 608 • Insufficient code authentication.

609 **6.3.1.19 Buffer Overflow (CWE-119, CWE-120)**

610 **Description**

611 Software used to implement an industrial control system (ICS) could be vulnerable to buffer
 612 overflows; adversaries could exploit these to perform various attacks. [§6.6-3]

613 A buffer overflow condition exists when a program attempts to put more data in a buffer than it
 614 can hold, or when a program attempts to put data in a memory area outside of the boundaries of a
 615 buffer. The simplest type of error, and the most common cause of buffer overflows, is the
 616 "classic" case in which the program copies the buffer without checking its length at all. Other
 617 variants exist, but the existence of a classic overflow strongly suggests that the programmer is
 618 not considering even the most basic of security protections. [§6.6-4]

619 **Examples [§6.6-4]**

- 620 • CVE-2012-0227 - Buffer overflow in the VSFlex7.VSFlexGrid ActiveX control in
 621 ComponentOne FlexGrid 7.1, as used in Open Automation Software OPC Systems.NET,
 622 allows remote attackers to cause a denial of service and possibly execute arbitrary code via a
 623 long archive file name argument to the Archive method;
- 624 • CVE-2012-3035 = Buffer overflow in Emerson DeltaV 9.3.1 and 10.3 through 11.3.1 allows
 625 remote attackers to cause a denial of service (daemon crash) via a long string to an
 626 unspecified port;

- 627 • CVE-2012-5163 - Buffer overflow in an unspecified third-party component in the Batch
628 module for Schneider Electric CitectSCADA before 7.20 and Mitsubishi MX4 SCADA
629 before 7.20 allows local users to execute arbitrary code via a long string in a login
630 sequence.

631 **6.3.1.20 Mishandling of Undefined, Poorly Defined, or “Illegal” Conditions (CWE-388,
632 CWE-20)**

633 **Description**

634 Some ICS implementations are vulnerable to packets that are malformed or contain illegal or
635 otherwise unexpected field values [§6.6-3]

636 **6.3.1.21 Use of Insecure Protocols (CWE-720)**

637 **Description**

638 Protocols are expected patterns of behavior that allow communication among computing
639 resources. This section deals with the use of protocols for which security was not sufficiently
640 considered during the development process.

641 **Examples**

- 642 • Distributed Network Protocol (DNP) 3.0, Modbus, Profibus, and other protocols are
643 common across several industries and protocol information is freely available. These
644 protocols often have few or no security capabilities built in, [§6.6-3]
- 645 • Use of clear text protocols such as FTP and Telnet, and
- 646 • Use of proprietary protocols lacking security features

647 **6.3.1.22 Weaknesses that Affect Files and Directories CWE-632)**

648 **Description**

649 Weaknesses in this category affect file or directory resources. [§6.6-4]

650 **Examples**

- 651 • UNIX path link problems (CWE-60),
- 652 • Windows path link problems (CWE-63),
- 653 • Windows virtual file problems (CWE-68),
- 654 • Mac virtual file problems (CWE-70),
- 655 • Failure to resolve case sensitivity (CWE-178),
- 656 • Path traversal (CWE-22),
- 657 • Failure to change working directory in chroot jail (CWE-243),
- 658 • Often misused: path manipulation (CWE-785),
- 659 • Password in configuration file (CWE-260),

- 660 • Improper ownership management (CWE-282),
- 661 • Improper resolution of path equivalence (CWE-41),
- 662 • Information leak through server log files (CWE-533),
- 663 • Files or directories accessible to external parties (CWE-552),
- 664 • Improper link resolution before file access ('link following') (CWE-59),
- 665 • Improper handling of windows device names (CWE-67), and
- 666 • Improper sanitization of directives in statically saved code ('static code injection') (CWE-96).

668 **6.3.1.23 4.2.1. API Abuse (CWE-227)**

669 **Description**

670 OWASP describes the API abuse vulnerability as follows:

671 An API is a contract between a caller and a callee. The most common forms of API
672 abuse are caused by the caller failing to honor its end of this contract.

673 For example, if a program fails to call `chdir()` after calling `chroot()`, it violates the contract
674 that specifies how to change the active root directory in a secure fashion. Another good
675 example of library abuse is expecting the callee to return trustworthy DNS information to
676 the caller. In this case, the caller abuses the callee API by making certain assumptions
677 about its behavior (that the return value can be used for authentication purposes). One
678 can also violate the caller-callee contract from the other side. For example, if a coder
679 subclasses `SecureRandom` and returns a non-random value, the contract is violated.
680 [§6.6-1]

681 **Examples**

- 682 • Dangerous function (CWE-242, CWE-676),
- 683 • Directory restriction error (CWE-243),
- 684 • Failure to follow guideline/specification (CWE-573),
- 685 • Heap inspection (CWE-244),
- 686 • Ignored function return value (CWE-252),
- 687 • Object model violation: just one of `equals()` and `hashCode()` defined (CWE-581),
- 688 • Often misused: authentication (CWE-247),
- 689 • Often misused: exception handling (CWE-248),
- 690 • Often misused: file system (CWE-785),
- 691 • Often misused: privilege management (CWE-250), and
- 692 • Often misused: string management (CWE-251).

693 **6.3.1.24 Use of Dangerous API (CWE-242, CWE-676)**

694 **Description**

695 A dangerous API is one that is not guaranteed to work safely in all conditions or can be used
696 safely but could introduce a vulnerability if used in an incorrect manner.

697 **Examples**

- 698 • Dangerous function such as the C function gets() (CWE-242),
- 699 • Directory restriction error (CWE-243),
- 700 • Failure to follow guideline/specification (CWE-573),
- 701 • Heap inspection (CWE-244),
- 702 • Insecure temporary file (CWE-377),
- 703 • Object model violation: just one of equals() and hashCode() defined (CWE-581),
- 704 • Often misused: exception handling (CWE-248),
- 705 • Often misused: file system (CWE-785),
- 706 • Often misused: privilege management (CWE-250),
- 707 • Often misused: string management (CWE-251),
- 708 • Unsafe function call from a signal handler (CWE-479), and
- 709 • Use of obsolete methods (CWE-477).

710 **6.4 PLATFORM VULNERABILITIES**

711 Platforms are defined as the software and hardware units, or systems of software and hardware,
712 that are used to deliver software-based services.

713 The platform comprises the software, the operating system used to support that software, and the
714 physical hardware. Vulnerabilities arise in this part of the Smart Grid network due to the
715 complexities of architecting, configuring, and managing the platform itself. Platform areas
716 identified as being vulnerable to risk include the security architecture and design, inadequate
717 malware protection against malicious software attacks, software vulnerabilities due to late or
718 nonexistent software patches from software vendors, an overabundance of file transfer services
719 running, and insufficient alerts from log management servers and systems.

720 **6.4.1 Design**

721 **6.4.1.1 Use of Inadequate Security Architectures and Designs**

722 **Description**

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

726 **Examples**

- 727 • Security design by untrained engineers,
- 728 • Reliance on nonstandard techniques and unproven algorithms, and
- 729 • Security through obscurity.

730 **6.4.1.2 Lack of External or Peer Review for Security Design**

731 **Description**

732 Lack of understanding regarding the complexity of secure systems leads designers to believe that
733 proven techniques can be easily combined into a larger system while preserving the security of
734 the individual techniques. These kinds of errors are often discovered only through thorough,
735 external review.

736 **Examples:**

- 737 • Introduction of side-channel attacks,
- 738 • Poorly combined algorithms,
- 739 • Lack of understanding regarding identifying weakest links, and
- 740 • Insufficient analysis of cascaded risk, whereby compromise of one system leads to
741 compromise of a downstream system.

742 **6.4.2 Implementation**

743 **6.4.2.1 Whitelisting**

744 **Description**

745 An application whitelist is a list of applications and application components (libraries,
746 configuration files, etc.) that are known to be benign. The technologies used to apply application
747 whitelists—to control which applications are permitted to execute on a host—are called
748 whitelisting programs, application control programs, or application whitelisting technologies.
749 Application whitelisting technologies are intended to stop the execution of malware, unlicensed
750 software, and other unauthorized software. Unlike security technologies such as antivirus
751 software, which block known bad activity and permit all other, application whitelisting
752 technologies are designed to permit known good activity and block all other.

753 **Examples**

- 754 • Whitelisting to prevent unintentional use of software (unauthorized software, incorrect
755 software version), and
- 756 • Whitelisting could be used to restrict unauthorized software.

757 **6.4.2.2 File Integrity Monitoring**

758 **Description**

759 Establishing a “known and trusted” state based on a policy or standard and using a methodology
760 or tool that finds, assesses, and acts on changes to the known state as soon as a change occurs.
761 This ensures ongoing system integrity and automates detecting, auditing, and reconciling
762 changes.

763 **Examples**

- 764 • File system integrity checking to ensure files are not changed, and
- 765 • Configuration change setting to ensure operating system settings are not changed.

766 **6.4.2.3 Inadequate Malware Protection**

767 **Description**

768 Malicious software can result in performance degradation, loss of system availability, and the
769 capture, modification, or deletion of data. Malware protection software, such as antivirus
770 software, is needed to prevent systems from being infected by malicious software. [§6.6-3]

771 **Examples**

- 772 • Malware protection software not installed,
- 773 • Malware protection software or definitions not current, and
- 774 • Malware protection software implemented without exhaustive testing.

775 **6.4.2.4 Installed Security Capabilities Not Enabled by Default**

776 **Description**

777 Security capabilities must be turned on in order to be useful. There are many examples of
778 operating systems where protections such as firewalls are configured but not enabled out-of-the-
779 box. If protections are not enabled, the system may be unexpectedly vulnerable to attacks. In
780 addition, if the administrator does not realize that protections are disabled, the system may
781 continue in an unprotected state for some time until the omission is noticed.

782 **6.4.2.5 Absent or Deficient Equipment Implementation Guidelines**

783 **Description**

784 Unclear implementation guidelines can lead to unexpected behavior.

785 A system needs to be configured correctly in order to provide the desired security properties.
786 This applies to both hardware and software configuration. Different inputs and outputs, both
787 logical and physical, will have different security properties, and an interface that is intended for
788 internal use may be more vulnerable than an interface designed for external use. Guidelines for
789 installers, operators, and managers must be clear about the security properties expected of the
790 system and how the system is to be implemented and configured in order to obtain those
791 properties.

792 **6.4.3 Operational**

793 **6.4.3.1 Lack of Prompt Security Patches from Software Vendors**

794 **Description**

795 Software contains bugs and vulnerabilities. When a vulnerability is disclosed, there will be a race
796 between hackers and patchers to either exploit or close the loophole. The security of the system
797 using the software depends on vendors' ability to provide patches in a timely manner, and on
798 administrators' ability to implement those patches. As zero-day exploits become more
799 widespread, administrators may be faced with the alternatives of taking a system offline or
800 leaving it vulnerable.

801 **6.4.3.2 Unneeded Services Running**

802 **Description**

803 Many operating systems are shipped and installed with a number of services running by default.
804 For example, in the case of UNIX, an installation may automatically offer telnet, ftp, and http
805 servers. Every service that runs is a security risk, because intended use of the service may
806 provide access to system assets, and the implementation may contain exploitable bugs. Services
807 should run only if needed, and an unneeded service is a vulnerability with no benefit.

808 **6.4.3.3 Insufficient Log Management**

809 **Description**

810 Events from all devices should be logged to a central log management server. Alerts should be
811 configured according to the criticality of the event or a correlation of certain events. For instance,
812 when the tamper-detection mechanism on a device is triggered, an alert should be raised to the
813 appropriate personnel. When a remote power disconnect command is issued to x (organization-
814 defined) number of meters within a certain time, alerts should also be sent.

815 **Examples**

- 816 • Inadequate network security architecture [§6.6-3, Table 3-8];
- 817 • Inadequate firewall and router logs [§6.6-3, Table 3-11];
- 818 • No security monitoring on the network [§6.6-3, Table 3-11]; and
- 819 • Critical monitoring and control paths are not identified [§6.6-3, Table 3-12].

820 **Potential Impact**

- 821 • Failure to detect critical events;
- 822 • Removal of forensic evidence; and
- 823 • Log wipes.

824 **6.4.4 Poorly configured security equipment (800-82 3-8)**

825 **6.4.4.1 Inadequate Anomaly Tracking**

826 **Description**

827 Alerts and logging are two useful techniques for detecting and mitigating the risk of anomalous
828 events, but can present security risks or become vulnerabilities if not instituted thoughtfully. The
829 appropriate reaction to an event will vary according to the criticality of the event or a correlation
830 of certain events. The event may also need to be logged, and a central logging facility may be
831 necessary for correlating events. Appropriate event reactions could include automatic paging of
832 relevant personnel in the event of persistent tamper messages or may require positive
833 acknowledgement to indicate supervisory approval has been attained before executing a
834 potentially disruptive command (e.g., simultaneously disconnecting many loads from the
835 electrical grid or granting control access rights to hundreds of users).

836 **6.5 NETWORK**

837 Networks are defined by connections between multiple locations or organizational units and are
838 composed of many differing devices using similar protocols and procedures to facilitate a secure
839 exchange of information. Vulnerabilities and risks occur within Smart Grid networks when
840 policy management and procedures do not conform to required standards and compliance polices
841 as they relate to the data exchanged.

842 Network areas identified as being susceptible to risk and with policy and compliance impacts
843 are: data integrity, security, protocol encryption, authentication, and device hardware.

844 **6.5.1 Network**

845 **6.5.1.1 Inadequate Integrity Checking**

846 **Description**

847 The integrity of message protocol and message data should be verified before routing or
848 processing. Devices receiving data not conforming to the protocol or message standard should
849 not act on such traffic (e.g., forwarding to another device or changing its own internal state) as
850 though the data were correctly received.

851 Such verification should be done before any application attempts to use the data for internal
852 processes or routing to another device. Additionally, special security devices acting as
853 application-level firewalls should be used to perform logical bounds checking, such as
854 preventing the shutdown of all power across an entire neighborhood area network (NAN).

855 Most functions of the Smart Grid, such as demand response (DR), load shedding, automatic
856 meter reading (AMR), time of use (TOU), and distribution automation (DA), require that data
857 confidentiality and/or data integrity be maintained to ensure grid reliability, prevent fraud, and
858 enable reliable auditing. Failure to apply integrity and confidentiality services where needed can
859 result in vulnerabilities such as exposure of sensitive customer data, unauthorized modification
860 of telemetry data, transaction replay, and audit manipulation.

861 **Examples**

- 862 • Lack of integrity checking for communications [§6.6-3, Table 3-12],
- 863 • Failure to detect and block malicious traffic in valid communication channels,
- 864 • Inadequate network security architecture [§6.6-3, Table 3-8],
- 865 • Poorly configured security equipment [§6.6-3, Table 3-8], and
- 866 • No security monitoring on the network [§6.6-3, Table 3-11].

867 **Potential Impact**

- 868 • Compromise of smart device, head node, or utility management servers,
- 869 • Buffer overflows,
- 870 • Covert channels,
- 871 • Man-in-the-middle (MitM), and
- 872 • Denial of service or distributed denial of service (DoS /DDoS).

873 **6.5.1.2 Inadequate Network Segregation**

874 **Description**

875 Network architectures often do not clearly define security zones and control traffic between
876 security zones, providing a flat network, wherein traffic from any portion of the network is
877 allowed to communicate with any other portion of the network. Smart Grid examples of
878 inadequate network segregation might include failure to install a firewall to control traffic
879 between a head node and the utility company or failure to prevent traffic from one NAN to
880 another NAN.

881 **Examples**

- 882 • Failure to define security zones,
- 883 • Failure to control traffic between security zones,
- 884 • Inadequate firewall ruleset,
- 885 • Firewalls nonexistent or improperly configured [§6.6-3, Table 3-10],
- 886 • Improperly configured VLAN,
- 887 • Inadequate access controls applied [§6.6-3, Table 3-8],
- 888 • Inadequate network security architecture [§6.6-3, Table 3-8],
- 889 • Poorly configured security equipment [§6.6-3, Table 3-8],
- 890 • Control networks used for non-control traffic [§6.6-3, Table 3-10],
- 891 • Control network services not within the control network [§6.6-3, Table 3-10], and
- 892 • Critical monitoring and control paths are not identified [§6.6-3, Table 3-12].

893 **Potential Impact**

- 894 • Direct compromise of any portion of the network from any other portion of the network,
- 895 • Compromise of the Utility network from a NAN network,
- 896 • VLAN hopping,
- 897 • Network mapping,
- 898 • Service/Device exploit,
- 899 • Covert channels,
- 900 • Back doors,
- 901 • Worms and other malicious software, and
- 902 • Unauthorized multi-homing.

903 **6.5.1.3 Inappropriate Protocol Selection**

904 **Description**

905 It is important to note that the use of encryption is not always the appropriate choice. A full
906 understanding of the information management capabilities that are lost through the use of
907 encryption should be completed before encrypting unnecessarily.

908 Use of unencrypted network protocols or weakly encrypted network protocols exposes
909 authentication keys and data payload. This may allow attackers to obtain credentials to access
910 other devices in the network and decrypt encrypted traffic using those same keys. The use of
911 clear text protocols may also permit attackers to perform session hijacking and MitM attacks
912 allowing the attacker to manipulate the data being passed between devices.

913 **Examples**

- 914 • Standard, well-documented communication protocols are used in plain text in a manner
915 which creates a vulnerability [§6.6-3, Table 3-12], and
- 916 • Inadequate data protection is permitted between clients and access points [§6.6-3, Table
917 3-13].

918 **Potential Impact**

- 919 • Compromise of all authentication and payload data being passed,
- 920 • Session Hijacking,
- 921 • Authentication Sniffing,
- 922 • MitM Attacks, and
- 923 • Session Injection.

924 **6.5.1.4 Weaknesses in Authentication Process or Authentication Keys**

925 **Description**

926 Authentication mechanism does not sufficiently authenticate devices or exposes authentication
927 keys to attack.

928 **Examples**

- 929 • Inappropriate Lifespan for Authentication Credentials/Keys;
- 930 • Inadequate Key Diversity;
- 931 • Authentication of users, data, or devices is substandard or nonexistent [§6.6-3, Table 3-
932 12];
- 933 • Insecure key storage;
- 934 • Insecure key exchange;
- 935 • Insufficient account lockout;
- 936 • Inadequate authentication between clients and access points [§6.6-3, Table 3-13]; and
- 937 • Inadequate data protection between clients and access points [§6.6-3, Table 3-13].

938 **Potential Impact**

- 939 • DoS / DDoS,
- 940 • MitM,
- 941 • Session Hijacking,
- 942 • Authentication Sniffing, and
- 943 • Session Injection.

944 **6.5.1.5 Insufficient Redundancy**

945 **Description**

946 Architecture does not provide for sufficient redundancy, thus exposing the system to intentional
947 or unintentional denial of service.

948 **Examples**

- 949 • Lack of redundancy for critical networks [§6.6-3, Table 3-9].

950 **Potential Impact**

- 951 • DoS / DDoS.

952 **6.5.1.6 Physical Access to the Device**

953 **Description**

954 Access to physical hardware may lead to a number of hardware attacks that can lead to the
955 compromise of all devices and networks. Physical access to Smart Grid devices should be
956 limited according to the criticality or sensitivity of the device. Ensuring the physical security of
957 Smart Grid elements, such as by physically locking them in some secure building or container, is
958 preferred where practical. In other circumstances, tamper resistance, tamper detection, and
959 intrusion detection and alerting are among the many techniques that can complement physically
960 securing devices.

961 **Examples**

- 962 • Unsecured physical ports,
- 963 • Inadequate physical protection of network equipment [§6.6-3, Table 3-9],
- 964 • Loss of environmental control [§6.6-3, Table 3-9], and
- 965 • Noncritical personnel have access to equipment and network connections [§6.6-3, Table
966 3-9].

967 **Potential Impact**

- 968 • Malicious configurations,
- 969 • MitM,
- 970 • EEPROM dumping,
- 971 • Micro controller dumping,
- 972 • Bus snooping, and
- 973 • Key extraction.

974 **6.6 REFERENCES**

975 The following are cited in this chapter—

- 976 1. Open Web Application Security Project (OWASP), 2011.
977 <http://www.owasp.org/index.php/Category:Vulnerability> (accessed December 5, 2012).
- 978 2. Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53 Rev. 4,
979 *Security and Privacy Controls for Federal Information Systems and Organizations*.
980 Gaithersburg: NIST, 2012. [http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-
981 53-rev3-final_updated-errata_05-01-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf)
- 982 3. Stouffer, Keith, Joe Falco, and Karen Scarfone. NIST SP 800-82, *Guide to Industrial
983 Control Systems (ICS) Security*. Gaithersburg, MD: NIST, 2011.
984 <http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>.
- 985 4. Common Weakness Enumeration (CWE), 2012. <http://cwe.mitre.org> (accessed
986 December 5, 2012).

- 987 5. Common Vulnerabilities and Exposures (CVE), 2012. <http://cve.mitre.org/> (accessed
988 December 5, 2012).
- 989 6. North American Electric Reliability Corporation (NERC) Critical Infrastructure
990 Protection (CIP) Standards, <http://www.nerc.com/page.php?cid=2|20> (accessed
991 December 5, 2012).
- 992 7. Stoneburner, Gary, Clark Hayden, and Alexis Feringa. NIST SP 800-27 Rev. A,
993 *Engineering Principles for Information Technology Security (A Baseline for Achieving*
994 *Security)*. Gaithersburg, MD: NIST, 2004. [http://csrc.nist.gov/publications/nistpubs/800-
995 27A/SP800-27-RevA.pdf](http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf).
- 996 8. CMMI Product Team, *CMMI for Development, Version 1.3* (CMU/SEI-2010-TR-033).
997 Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2010.
998 <http://www.sei.cmu.edu/library/abstracts/reports/10tr033.cfm>.
- 999 9. ISO/IEC 21827:2008, Information technology -- Security techniques -- Systems Security
1000 Engineering -- Capability Maturity Model® (SSE-CMM®), Geneva, Switzerland:
1001 International Organization for Standardization (ISO), 2008.
1002 [http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=
1003 44716](http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=44716) (accessed December 5, 2012)
- 1004 10. OWASP, “Testing for business logic (OWASP-BL-001)”, 2012.
1005 [http://www.owasp.org/index.php/Testing_for_business_logic_%28OWASP-BL-001%29
1006 \(accessed December 5, 2012\).](http://www.owasp.org/index.php/Testing_for_business_logic_%28OWASP-BL-001%29)
1007

1008 CHAPTER SEVEN

1009 BOTTOM-UP SECURITY ANALYSIS OF THE SMART GRID

1010 7.1 SCOPE

1011 A subgroup of the CSWG is performing a bottom-up analysis of cyber security issues in the
1012 evolving Smart Grid. The goal is to identify specific protocols, interfaces, applications, best
1013 practices, etc., that could and should be developed to solve specific Smart Grid cyber security
1014 problems. The approach taken is to perform the analysis from the bottom up; that is, to identify
1015 some specific problems and issues that need to be addressed but not to perform a comprehensive
1016 gap analysis that covers all issues. This effort is intended to complement the top-down efforts
1017 being followed elsewhere in the CSWG. By proceeding with a bottom-up analysis, our hope is to
1018 more quickly identify fruitful areas for solution development, while leaving comprehensive gap
1019 analysis to other efforts of the CSWG, and to provide an independent completeness check for
1020 top-down gap analyses. This effort is proceeding simultaneously in several phases.

1021 First, we have identified a number of *evident and specific security problems* in the Smart Grid
1022 that are amenable to and should have open and interoperable solutions but which are not
1023 obviously solved by existing standards, de facto standards, or best practices. This list includes
1024 only cyber security problems that have some specific relevance to or uniqueness in the Smart
1025 Grid. Thus we do not list general cyber security problems such as poor software engineering
1026 practices, key management, etc., unless these problems have some unique twist when considered
1027 in the context of the Smart Grid. We have continued to add to this list of problems as we came
1028 across problems not yet documented.

1029 In conjunction with developing the list of specific problems, we have developed a separate list of
1030 more *abstract security issues* that are not as specific as the problems in the first list, but are
1031 nevertheless of significant importance. Considering these issues in specific contexts can reveal
1032 specific problems.

1033 Next, drawing in part from the specific problems and abstract issues enumerated in the first two
1034 lists, we are developing a third list of cyber security *design considerations* for Smart Grid
1035 systems. These design considerations discuss important cyber security issues that arise in the
1036 design, deployment, and use of Smart Grid systems and that should be considered by system
1037 designers, implementers, purchasers, integrators, and users of Smart Grid technologies. In
1038 discussing the relative merits of different technologies or solutions to problems, these design
1039 considerations stop short of recommending specific solutions or even requirements. Our
1040 intention is to highlight important issues that can serve as a means of identifying and formulating
1041 requirements and high-level designs for key protocols and interfaces that are missing and need to
1042 be developed.

1043 7.2 EVIDENT AND SPECIFIC CYBER SECURITY PROBLEMS

1044 This subsection documents specific cyber security problems in the Smart Grid insofar as possible
1045 by describing actual field cases that explain exactly the operational, system, and device issues.
1046 The problems listed herein are intentionally *not* ordered or categorized in any particular way.

1047 **7.2.1 Authenticating and Authorizing Users to Substation IEDs**

1048 The problem addressed in this subsection is how to authenticate and authorize users
1049 (maintenance personnel) to intelligent electronic devices (IEDs) in substations in such a way that
1050 access is specific to a user, authentication information (e.g., password) is specific to each user
1051 (i.e., not shared between users), and control of authentication and authorization can be centrally
1052 managed across all IEDs in the substation and across all substations belonging to the utility and
1053 updated reasonably promptly to ensure that only intended users can authenticate to intended
1054 devices and perform authorized functions.

1055 Currently many substation IEDs have a notion of “role” but no notion of “user.” Passwords are
1056 stored locally on the device, and several different passwords allow different authorization levels.
1057 These role passwords are shared amongst all users of the device performing the role in question,
1058 possibly including nonutility employees such as contractors and vendors. Furthermore, due to the
1059 number of devices, these passwords are often the same across all devices in the utility and are
1060 seldom changed.

1061 A device may be accessed locally in the sense that the user is physically present in the substation
1062 and accesses the IED from a front panel connection, a wired network connection, or possibly via
1063 a wireless connection. The device may also be accessed remotely over a low-speed (dial-up) or
1064 high-speed (network) connection from a different physical location.

1065 Substations generally have some sort of connectivity to the control center that might be used to
1066 distribute authentication information and collect audit logs, but this connectivity may be as slow
1067 as 1200 baud. Performing an authentication protocol such as Remote Authentication Dial In User
1068 Service (RADIUS) or Lightweight Directory Access Protocol (LDAP) over this connection is
1069 probably not desirable. Furthermore, reliance on central authentication servers is unwise, since
1070 authentication should continue to apply for personnel accessing devices locally in the substation
1071 when control center communications are down.

1072 A provision to ensure that necessary access is available in emergency situations may be
1073 important, even if it means bypassing normal access control—but with an audit trail.

1074 **7.2.2 Authenticating and Authorizing Users to Outdoor Field Equipment**

1075 Some newer pole-top and other outdoor field equipment supports 802.11 or Bluetooth for near-
1076 local user access from a maintenance truck. The problem is how to authenticate and authorize
1077 users (maintenance personnel) to such devices in such a way that access is specific to a user
1078 (person), authentication information (e.g. password) is specific to each user (not shared between
1079 users), and control of authentication and authorization can be centrally managed across the utility
1080 and updated reasonably promptly to ensure that only intended users can authenticate to intended
1081 devices and perform authorized functions.

1082 Pole-top and other outdoor field equipment may not have connectivity to the control center.

1083 Access will usually be local via wired connections, or near-local via short-range radio, although
1084 some devices may support true remote access.

1085 Strong authentication and authorization measures are preferable, and in cases where there is
1086 documented exception to this due to legacy and computing constrained devices, compensating
1087 controls should be given due consideration. For example, in many utility organizations, very
1088 strong operational control and workflow prioritization is in place, such that all access to field

1089 equipment is scheduled, logged, and supervised. In the general sense, the operations department
1090 typically knows exactly who is at any given field location at all times. In addition, switchgear
1091 and other protective equipment generally have tamper detection on doors as well as connection
1092 logging and reporting such that any unexpected or unauthorized access can be reported
1093 immediately over communications.

1094 **7.2.3 Authenticating and Authorizing Maintenance Personnel to Meters**

1095 Like IED equipment in substations, current smart meter deployments use passwords in meters
1096 that are not associated with individual users. Passwords are shared between users, and the same
1097 password is typically used across the entire meter deployment. The problem is how to
1098 authenticate and authorize users who are maintenance personnel to meters in such a way that
1099 access is specific to a user, authentication information (e.g., password) is specific to each user
1100 (i.e., not shared between users), and control of authentication and authorization can be centrally
1101 managed and updated reasonably promptly to ensure that only intended users can authenticate to
1102 intended devices and perform authorized functions.

1103 Access may be local through the optical port of a meter or remote through the advanced metering
1104 infrastructure (AMI) infrastructure.

1105 Meters generally have some sort of connectivity to an AMI head end, but this connectivity may
1106 be as slow as 1200 baud or lower (e.g., some power line carrier devices have data rates measured
1107 in millibaud). This connectivity cannot be assumed to be present in a maintenance scenario.

1108 **7.2.4 Authenticating and Authorizing Consumers to Meters**

1109 Where meters act as home area network gateways for providing energy information to
1110 consumers and/or control for demand response programs, will consumers be authenticated to
1111 meters? If so, authorization would likely be highly limited. What would the roles be?
1112 Authorization and access levels need to be carefully considered, i.e., a consumer capable of
1113 supplying energy to the power grid may have different access requirements than one who does
1114 not.

1115 **7.2.5 Authenticating Meters to/from AMI Head Ends**

1116 It is important for a meter to authenticate any communication from an AMI head end in order to
1117 ensure that an adversary cannot issue control commands to the meter, update firmware, etc. It is
1118 important for an AMI head end to authenticate the meter, since usage information retrieved from
1119 the meter will be used for billing and commands must be assured of delivery to the correct meter.

1120 As utilities merge and service territories change, a utility will eventually end up with a collection
1121 of smart meters from different vendors. Meter to/from AMI head end authentication should be
1122 interoperable to ensure that authentication and authorization information need not be updated
1123 separately on different vendor's AMI systems.

1124 **7.2.6 Authenticating HAN Devices to/from HAN Gateways**

1125 Demand response HAN devices must be securely authenticated to the HAN gateway and vice
1126 versa. It is important for a HAN device to authenticate any demand-response commands from the
1127 DR head end in order to prevent control by an adversary. Without such authentication,
1128 coordinated falsification of control commands across many HAN devices and/or at rapid rates

1129 could lead to grid stability problems. It is important that the DR head end authenticate the HAN
1130 device both to ensure that commands are delivered to the correct device and that responses from
1131 that device are not forged.

1132 Interoperability of authentication is essential in order to ensure competition that will lead to low-
1133 cost consumer devices. This authentication process must be simple and fairly automatic, since to
1134 some degree it will be utilized by consumers who buy/rent HAN devices and install them. HAN
1135 devices obtained by the consumer from the utility may be preprovisioned with authentication
1136 information. HAN devices obtained by the consumer from retail stores may require provisioning
1137 through an Internet connection or may receive their provisioning through the HAN gateway.

1138 Should a HAN device fail to authenticate, it will presumably be unable to respond to DR signals.
1139 It should not be possible for a broad denial of service (DoS) attack to cause a large number of
1140 HAN devices to fail to authenticate and thereby not respond to a DR event.

1141 **7.2.7 Authenticating Meters to/from AMI Networks**

1142 Meters and AMI networks are more susceptible to widespread compromise and DoS attacks if no
1143 authentication and access control is provided in AMI access networks such as neighborhood area
1144 networks (NANs) and HANs. The vulnerability exists even if the rest of the AMI network is
1145 secured, and encryption and integrity are provided by an AMI application protocol. Network
1146 access authentication tied with access control in the AMI access networks can mitigate the threat
1147 by ensuring that only authenticated and authorized entities can gain access to the NANs or
1148 HANs. In mesh networks, this “gatekeeper” functionality must be enforced at each node. The
1149 network access authentication must be able to provide mutual authentication between a meter
1150 and an access control enforcement point. A trust relationship between the meter and the
1151 enforcement point may be dynamically established using a trusted third party such as an
1152 authentication server.

1153 Providing network access authentication for mesh networks can be more challenging than for
1154 non-mesh networks due to the difference in trust models between mesh and non-mesh networks.
1155 One trust model for mesh networks is based on a dynamically created hop-by-hop chain of trust
1156 between adjacent mesh nodes on the path between a leaf mesh node and the gateway to the AMI
1157 network where access control is performed on each intermediate mesh node and the gateway.
1158 Another trust model for mesh networks is end-to-end trust between a leaf mesh node and the
1159 gateway where intermediate mesh nodes are considered untrusted to the leaf node and a secured
1160 tunnel may be created between each leaf node and the gateway. These two trust models can
1161 coexist in the same mesh network. When two or more interconnected mesh networks are
1162 operated in different trust models, end-to-end security across these mesh networks is the only
1163 way to provide data security for applications running across the mesh networks. There has been
1164 some research done in the area of wireless sensor networks that is relevant to mesh networks. For
1165 instance, there are scalable key pre-distribution schemes [§7.5-11] that are resistant to node
1166 capture and operate well on devices with limited computational capabilities.

1167 **7.2.8 Securing Serial SCADA Communications**

1168 Many substations and distribution communication systems still employ slow serial links for
1169 various purposes, including supervisory control and data acquisition (SCADA) communications
1170 with control centers and distribution field equipment. Furthermore, many of the serial protocols
1171 currently in use do not offer any mechanism to protect the integrity or confidentiality of

1172 messages, i.e., messages are transmitted in cleartext form. Solutions that simply wrap a serial
1173 link message into protocols like Secure Socket Layer (SSL) or Internet Protocol Security (IPSec)
1174 over Point-to-Point Protocol (PPP) will suffer from the overhead imposed by such protocols
1175 (both in message payload size and computational requirements) and would unduly impact
1176 latency and bandwidth of communications on such connections. A solution is needed to address
1177 the security and bandwidth constraints of this environment.

1178 **7.2.9 Securing Engineering Dial-up Access**

1179 Dial-up is often used for engineering access to substations. Broadband is often unavailable at
1180 many remote substation locations. Security is limited to modem callback and passwords in the
1181 answering modem and/or device connected to the modem. Passwords are not user-specific and
1182 are seldom changed. A solution is needed that gives modern levels of security while providing
1183 for individual user attribution of both authentication and authorization.

1184 **7.2.10 Secure End-to-End Meter to Head End Communication**

1185 Secure end-to-end communications protocols such as transport layer security (TLS) and IPSec
1186 ensure that confidentiality and integrity of communications is preserved regardless of
1187 intermediate hops. End-to-end security between meters and AMI head ends is desirable, and
1188 even between HAN devices and DR control services.

1189 **7.2.11 Access Logs for IEDs**

1190 Not all IEDs create access logs. Due to limited bandwidth to substations, even where access logs
1191 are kept, they are often stranded in the substation. In order for a proper security event
1192 management (SEM) paradigm to be developed, these logs will need to become centralized and
1193 standardized so that other security tools can analyze their data. This is important in order to
1194 detect malicious actions by insiders as well as systems deeply penetrated by attackers that might
1195 have subtle misconfigurations as part of a broader attack. A solution is needed that can operate
1196 within the context of bandwidth limitations found in many substations as well as the massively
1197 distributed nature of the power grid infrastructure.

1198 **7.2.12 Remote Attestation of Meters**

1199 Remote attestation provides a means to determine whether a remote field unit has an expected
1200 and approved configuration. For meters, this means the meter is running the correct version of
1201 untampered firmware with appropriate settings and has *always* been running untampered
1202 firmware. Remote attestation is particularly important for meters given the easy physical
1203 accessibility of meters to attackers.

1204 **7.2.13 Protection of Routing Protocols in AMI Layer 2/3 Networks**

1205 In the AMI space, there is increasing likelihood that mesh routing protocols will be used on
1206 wireless links. Wireless connectivity suffers from several well-known and often easily
1207 exploitable attacks, partly due to the lack of control to the physical medium (the radio waves).
1208 Modern mechanisms like the IEEE 802.11i and 802.11w security standards have worked to close
1209 some of these holes for standard wireless deployments. However, wireless mesh technology
1210 potentially opens the door to some new attacks in the form of route injection, node
1211 impersonation, L2/L3/L4 traffic injection, traffic modification, etc. Most current on-demand and

1212 link-state routing mechanisms do not specify a scheme to protect the data or the routes the data
1213 takes, because it is outside of the scope of routing protocols. They also generally lack schemes
1214 for authorizing and providing integrity protection for adjacencies in the routing system. Without
1215 end-to-end security (like IPsec), attacks such as eavesdropping, impersonation, and man-in-the-
1216 middle (MITM) could be easily mounted on AMI traffic. With end-to-end security in place,
1217 routing security is still required to prevent denial of service (DoS) attacks.

1218 **7.2.14 Protection of Dial-up Meters**

1219 Reusing older, time-proven technologies such as dial-up modems to connect to collectors or
1220 meters without understanding the subtle differences in application may provide loss of service or
1221 worse. Dial-up technology using plain old telephone service (POTS) has been a preferred method
1222 for connecting to network gear, particularly where a modem bank providing 24, 48, or even 96
1223 modems / phone numbers and other anti-attack intelligence is used. However, dialing into a
1224 collector or modem and connecting, even without a password, can tie up a line and effectively
1225 become a denial of service attack. Consider a utility which, for the sake of manageability places
1226 all their collectors or modems on phone numbers in a particular prefix. Every collector then can
1227 be hit by calling 202-555-WXYZ.

1228 **7.2.15 Outsourced WAN Links**

1229 Many utilities are leveraging existing communications infrastructure from telecommunications
1230 companies to provide connectivity between generation plants and control centers, between
1231 substations and control centers (particularly SCADA), and increasingly between pole-top AMI
1232 collectors and AMI head end systems, and pole-top distribution automation equipment and
1233 distribution management systems.

1234 Due to the highly distributed nature of AMI, it is more likely that an AMI wide area network
1235 (WAN) link will be over a relatively low bandwidth medium such as cellular band wireless (e.g.,
1236 Evolution Data Optimized (EvDO), General Packet Radio Service (GPRS)), or radio networks
1237 like FlexNet. The link layer security supported by these networks varies greatly. Later versions
1238 of WiMax can utilize Extensible Authentication Protocol (EAP) for authentication, but NIST
1239 Special Publication (SP) 800-127, *Guide to Security for Worldwide Interoperability for*
1240 *Microwave Access (WiMAX) Technologies*, provides a number of recommendations and cautions
1241 about WiMax authentication. With cellular protocols, the AirCards used by the collector modems
1242 are no different than the ones used for laptops. They connect to a wireless cloud typically shared
1243 by all local wireless users with no point-to-point encryption and no restrictions on whom in the
1244 wireless cloud can connect to the collector modem's interface. From the wireless, connectivity to
1245 the head end system is usually over the Internet, sometimes (hopefully always) using a virtual
1246 private network (VPN) connection. Given the proliferation of botnets, it is not farfetched to
1247 imagine enough wireless users being compromised to launch a DoS attack via a collector
1248 modem.

1249 Regardless of the strength of any link layer security implemented by the communications service
1250 provider, without end-to-end VPN security the traffic remains accessible to insiders at the service
1251 provider. This can permit legitimate access such as lawful intercept but also can allow
1252 unscrupulous insiders at the service provider access to the traffic.

1253 Additionally, like the mesh wireless portion, cellular networks are subject to intentional and
1254 unintentional interference and congestion. Cellular networks were significantly disrupted in

1255 Manhattan during the 9/11 attacks by congestion and were rendered mostly unusable to first
1256 responders. Similar congestion events could disrupt utility communications relying on
1257 commercial WAN links.

1258 **7.2.16 Insecure Firmware Updates**

1259 The ability to perform firmware updates on meters in the field allows for the evolution of
1260 applications and the introduction of patches without expensive physical visits to equipment.
1261 However, it is critical to ensure that firmware update mechanisms are not used to install
1262 malware. This can be addressed by a series of measures that provide a degree of defense in
1263 depth. First, measures can be taken to ensure that software is created without flaws such as buffer
1264 overflows that can enable protection measures to be circumvented. Techniques for programming
1265 languages and static analysis provide a foundation for such measures. Second, principals
1266 attempting updates must be properly authenticated and authorized for this function at a suitable
1267 enforcement point such as on the meter being updated. Third, software can be signed in a way
1268 that it can be checked for integrity at any time. Fourth, remote attestation techniques can provide
1269 a way to assess existing and past software configuration status so that deviations from expected
1270 norms can generate a notification or alarm event. Fifth, there must be a suitable means to detect a
1271 penetration of a meter or group of meters in a peer-to-peer mesh environment and isolate and
1272 contain any subsequent attempts to penetrate other devices. This is important, as it must be
1273 assumed that if an attacker has the capability to reverse engineer a device that any inbuilt
1274 protections can eventually be compromised as well. It is an open and challenging problem to do
1275 intrusion detection in a peer-to-peer mesh environment.

1276 **7.2.17 Side Channel Attacks on Smart Grid Field Equipment**

1277 A side-channel attack is based on information gained from the physical implementation of a
1278 cryptosystem and is generally aimed at extracting cryptographic keys. For example, early smart
1279 card implementations were particularly vulnerable to power analysis attacks that could determine
1280 the key used by a smart card to perform a cryptographic operation by analysis of the card's
1281 power consumption. TEMPEST attacks similarly can extract data by analyzing various types of
1282 electromagnetic radiation emitted by a central processing unit (CPU), display, keyboard, etc. Van
1283 Eck phreaking in particular can reconstruct the contents of a screen from the radiation emitted by
1284 the cathode ray tube (CRT) or liquid crystal display (LCD), and can be performed at some
1285 distance. TEMPEST attacks are nearly impossible to detect. Syringe attacks use a needle syringe
1286 as a probe to tap extremely fine wire traces on printed circuit boards. Timing attacks exploit the
1287 fact that cryptographic primitives can take different lengths of time to execute for different
1288 inputs, including keys. In any side-channel attack, it is not necessary for an attacker to determine
1289 the entire key; the attacker needs only enough of the key to facilitate the use of other code-
1290 breaking methods.

1291 Smart Grid devices that are deployed in the field, such as substation equipment, pole-top
1292 equipment, smart meters and collectors, and in-home devices, are at risk of side-channel attacks
1293 due to their accessibility. Extraction of encryption keys by side-channel attacks from Smart Grid
1294 equipment could lead to compromise of usage information, personal information, passwords, etc.
1295 Extraction of authentication keys by side-channel attacks could allow an attacker to impersonate
1296 Smart Grid devices and/or personnel, and potentially gain administrative access to Smart Grid
1297 systems.

1298 **7.2.18 Securing and Validating Field Device Settings**

1299 Numerous field devices contain settings. A prominent example is relay settings that control the
1300 conditions such as those under which the relay will trip a breaker. In microprocessor devices,
1301 these settings can be changed remotely. One potential form of attack is to tamper with relay
1302 settings and then attack in some other way. The tampered relay settings would then exacerbate
1303 the consequences of the second attack..

1304 A draft NERC white paper on identifying cyber-critical assets recognizes the need for protecting
1305 the system by which device settings are determined and loaded to the field devices themselves.
1306 This can include the configuration management process by which the settings are determined. It
1307 should likely extend to ongoing surveillance of the settings to ensure that they remain the same
1308 as intended in the configuration management process.

1309 **7.2.19 Absolute & Accurate Time Information**

1310 Absolute time is used by many types of power system devices for different functions. In some
1311 cases, time may be only informational, but increasingly more and more advanced applications
1312 will critically depend on an accurate absolute time reference. According to the draft NERC
1313 Control Systems Security Working Group (CSSWG) document, *Security Guideline for the*
1314 *Electricity Sector: Time Stamping of Operational Data Logs*, “these applications include, but are
1315 not limited to, Power Plant Automation Systems, Substation Automation Systems,
1316 Programmable Logic Controllers (PLC), Intelligent Electronic Devices (IED), sequence of event
1317 recorders, digital fault recorders, intelligent protective relay devices, Energy Management
1318 Systems (EMS), Supervisory Control and Data Acquisition (SCADA) Systems, Plant Control
1319 Systems, routers, firewalls, Intrusion Detection Systems (IDS), remote access systems, physical
1320 security access control systems, telephone and voice recording systems, video surveillance
1321 systems, and log collection and analysis systems.” [§7.5-14] Some detailed examples follow.

1322 **7.2.19.1 Security Protocols**

1323 Time has impact on multiple security protocols, especially in regard to the integrity of
1324 authentication schemes and other operations, if it is invalid or tampered with. For example, some
1325 protocols can rely on time stamp information to ensure against replay attacks or in other cases
1326 against time-based revoked access. Due care needs to be taken to ensure that time cannot be
1327 tampered with in any system or if it is, to ensure that the breach can be detected, responded to,
1328 and contained.

1329 **7.2.19.2 Synchrophasors**

1330 Synchrophasor measurement units are increasingly being deployed throughout the grid. A phasor
1331 is a vector consisting of magnitude and angle. The angle is a relative quantity and can be
1332 interpreted only with respect to a time reference. A synchrophasor is a phasor that is calculated
1333 from data samples using a standard time signal as the reference for the sampling process.

1334 Initial deployments of synchrophasor measurement units use synchrophasors to measure the
1335 current state of the power system more accurately than it can be determined through state
1336 estimation. If the time references for enough synchrophasor measurements are incorrect, the
1337 measured system state will be incorrect, and corrective actions based on this inaccurate
1338 information could lead to grid destabilization.

1339 Synchrophasor measurements are beginning to be used to implement wide area protection
1340 schemes. With inaccurate time references, these protection schemes may take inappropriate
1341 corrective actions that may further destabilize the system.

1342 **7.2.19.3 Certificates Time & Date Issues**

1343 Certificates are typically used to bind an identity to a public key or keys, facilitating such
1344 operations as digital signatures and data encryption. They are widely used on the Internet, but
1345 there are some potential problems associated with their use.

1346 Absolute time matters for interpretation of validity periods in certificates. If the system time of a
1347 device interpreting a certificate is incorrect, an expired certificate could be treated as valid or a
1348 valid certificate could be rejected as expired. This could result in incorrect authentication or
1349 rejection of users, incorrect establishment or rejection of VPN tunnels, etc. The Kerberos
1350 network authentication protocol (on which Windows domain authentication is based) also
1351 depends critically on synchronized clocks.

1352 **7.2.19.4 Event Logs and Forensics**

1353 Time stamps in event logs must be based on accurate time sources so that logs from different
1354 systems and locations can be correlated to reconstruct historical sequences of events. This
1355 applies both to logs of power data and to logs of cyber security events. Correlating power data
1356 from different locations can lead to an understanding of disturbances and anomalies—and
1357 difficulties in correlating logs was a major issue in investigating the August 14, 2003, blackout.
1358 Correlating cyber security events from different systems is essential to forensic analysis to
1359 determine if and how a security breach occurred and to support prosecution.

1360 **7.2.20 Personnel Issues in Field Service of Security Technology**

1361 Device security features or security devices themselves may add to labor complexity if field
1362 personnel have to interact with these devices in any way to accomplish maintenance and
1363 installation operations. This complexity may mean significant increases in costs that can lead to
1364 barriers for security features and devices being used. Thus due care must be taken when
1365 introducing any security procedures and technology to ensure that their management requires
1366 minimum disruption to affected labor resources.

1367 For instance, some utilities operate in regulated labor environments. Contractual labor
1368 agreements can impact labor costs if field personnel have to take on new or different tasks to
1369 access, service, or manage security technology. This can mean a new class or grade of pay and
1370 considerable training costs for a large part of the organization. In addition, there are further
1371 complexities introduced by personnel screening, clearance, and training requirements for
1372 accessing cyber assets.

1373 Another potential ramification of increased labor complexity due to security provisions can occur
1374 if employees or subcontractors have a financial incentive to bypass or circumvent the security
1375 provisions. For example, if a subcontractor is paid by the number of devices serviced, anything
1376 that slows down production, including both safety and security measures, directly affects the
1377 bottom line of that subcontractor, thus giving rise to an unintended financial motivation to
1378 bypass security or safety measures.

1379 **7.2.21 Weak Authentication of Devices in Substations**

1380 Inside some substations, where the components are typically assumed to be in a single building
1381 or enclosure, access control protection may be weak in that physical security is assumed to exist.
1382 For example, some systems may provide access control by MAC address filtering. When a
1383 substation is extended to incorporate external components such as solar panels, wind turbines,
1384 capacitor banks, etc., that are not located within the physical security perimeter of the substation,
1385 this protection mechanism is no longer sufficient.

1386 An attacker who gains physical access to an external component can then eavesdrop on the
1387 communication bus and obtain (or guess) MAC addresses of components inside the substation.
1388 Indeed, the MAC addresses for many components are often physically printed or stamped on the
1389 component. Once obtained, the attacker can fabricate packets that have the same MAC addresses
1390 as other devices on the network. The attacker may therefore impersonate other devices, reroute
1391 traffic from the proper destination to the attacker, and perform MITM attacks on protocols that
1392 are normally limited to the inside of the substation.

1393 **7.2.22 Weak Security for Radio-Controlled Distribution Devices**

1394 Remotely controlled switching devices that are deployed on pole-tops throughout distribution
1395 areas have the potential to allow for faster isolation of faults and restoration of service to
1396 unaffected areas. Some of these products that are now available on the market transmit open and
1397 close commands to switches over radio with limited protection of the integrity of these control
1398 commands. In some cases, no cryptographic protection is used, while in others the protection is
1399 weak in that the same symmetric key is shared among all devices.

1400 **7.2.23 Weak Protocol Stack Implementations**

1401 Many IP stack implementations in control systems devices are not as evolved as the protocol
1402 stacks in modern general-purpose operating systems. Improperly formed or unexpected packets
1403 can cause some of these control systems devices to lock up or fault in unexpected ways.

1404 **7.2.24 Insecure Protocols**

1405 Few if any of the control systems communication protocols currently used (primarily DNP3 and
1406 sometimes IEC 61850) are typically implemented with security measures. This applies to both
1407 serial protocols and IP protocols, such as Distributed Network Protocol (DNP) over
1408 Transmission Control Protocol (TCP). IEC 62351 (which is the security standard for these
1409 protocols) is now available but implementation adoption and feasibility is not yet clear. There is
1410 a secure authentication form of DNP3 under development.

1411 **7.2.25 License Enforcement Functions**

1412 Vendors and licensors are known to have embedded functions in devices and applications to
1413 enforce terms and conditions of licenses and other contracts. When exercised either intentionally
1414 or inadvertently, these functions can affect a DoS or even destroy data on critical systems. These
1415 functions occur in four general categories:

- 1416 • **Misuse of authorized maintenance access.** The classic case involves a major consumer
1417 product warehouse system where there is a software dispute and the vendor disables the
1418 system through a previously authorized maintenance port.

1419 • **Embedded shutdown functions.** Some applications contain shutdown functions that
1420 operate on a predetermined schedule unless the user performs a procedure using
1421 information supplied by the vendor. The necessary information is supplied to the user if
1422 the vendor believes the terms and conditions are being met. If the functions contain
1423 errors, they can shut down prematurely and cause DoS. This has reportedly happened on
1424 at least one mission-critical hospital-related system.

1425 • **Embedded capability for the licensor to intrude and shut down the system.** Authority
1426 for such intrusions is contained in the Uniform Computer Information Transactions Act
1427 (UCITA).⁴ This uniform state law was promulgated by the Conference of Commissioners
1428 on Uniform State Laws, and was highly controversial. It was enacted in Maryland and
1429 Virginia, but several states enacted “bomb-shelter” legislation preventing its applicability
1430 to consumers and businesses in their states. The intrusion authority is termed “self-help,”
1431 which is the term used in commercial law for repossession of automobiles and other
1432 products by lenders where the purchaser has defaulted. For the licensor to be able to
1433 intrude if they believe there is noncompliance with license terms, it is necessary for the
1434 operating system or application to have an embedded backdoor.

1435 • **Requiring the application or device to contact a vendor system over the public**
1436 **Internet.** This may occur to authorize initial startup or regularly during operation. It is
1437 problematic if the application or device has security requirements that prevent access to
1438 the public Internet.

1439 **7.2.26 Unmanaged Call Home Functions**

1440 Many recent commercial off-the-shelf (COTS) software applications and devices attempt to
1441 connect to public IP addresses in order to update software or firmware, synchronize time,
1442 provide help/support/diagnostic information, enforce licenses, or utilize Internet resources such
1443 as mapping tools, search systems, etc. In many cases, use of such call home functions is not
1444 obvious and is poorly documented, if any documentation exists. Configuration options to modify
1445 or disable call home functions are often hard to find if available. Examples of such call home
1446 functions include:

- 1447 • Operating system updaters;
- 1448 • Application updaters, including Web browsers, rendering tools for file formats such as
1449 PDF, Flash, QuickTime, Real, etc., printing software and drivers, digital camera
1450 software, etc.;
- 1451 • Network devices that obtain time from one or more Network Time Protocol (NTP)
1452 servers;
- 1453 • Voice-over-Internet-Protocol (VoIP) devices that register with a public call manager;
- 1454 • Printers that check for updates and/or check a Web database to ensure valid ink
1455 cartridges;
- 1456 • Applications that link to Web sites for documentation; and

⁴ <http://www.ucitaonline.com/>

1457 • Applications that display information using mapping tools or Google Earth.
1458 Some call home functions run only when an associated application is used; some are installed as
1459 operating system services running on a scheduled basis; and some run continuously on the device
1460 or system. Some call home updaters request confirmation from the user before installing updates,
1461 while others quietly install updates without interaction. Some call home functions use insecure
1462 channels.

1463 Unexpected call home functions that are either unknown to or not anticipated by the Smart Grid
1464 system designer can have serious security consequences. These include:

- 1465 • Network information leakage;
- 1466 • Unexpected changes in system configuration through software, firmware, or settings
1467 updates;
- 1468 • Risk of network compromise via compromise of the call home channel or external
1469 endpoint;
- 1470 • Unexpected dependence on external systems, including not only the systems that the call
1471 home function calls, but also public DNS and public time sources;
- 1472 • False positives on IDS systems when outbound connection attempts from call home
1473 functions are blocked by a firewall;
- 1474 • System resource consumption; and
- 1475 • Additional resource consumption when call home functions continuously attempt to retry
1476 connections that are blocked by a firewall.

1477 For the specific case of software or firmware updaters, best practices for patch management
1478 recommend deploying patch servers that provide patches to endpoints rather than having those
1479 endpoints reach out to the Internet. This provides better control of the patching process.
1480 However, most applications use custom updating mechanisms, which can make it difficult to
1481 deploy a comprehensive patch system for all operating systems, applications, and devices that
1482 may be used by the Smart Grid system. Further, not all applications and devices provide a way to
1483 change their configuration to direct them to a patch server.

1484 **7.3 NONSPECIFIC CYBER SECURITY ISSUES**

1485 This subsection lists cyber security issues that are too abstract to describe in terms of specific
1486 security problems but when considered in different contexts (control center, substation, meter,
1487 HAN device, etc.) are likely to lead to specific problems.

1488 **7.3.1 IT vs. Smart Grid Security**

1489 The differences between information technology (IT), industrial, and Smart Grid security need to
1490 be accentuated in any standard, guide, or roadmap document. NIST SP 800-82, *Guide to*
1491 *Industrial Control Systems (ICS) Security*, can be used as a basis, but more needs to be addressed
1492 in that control system security operates in an industrial campus setting and is not the same as an
1493 environment that has the scale, complexity, and distributed nature of the Smart Grid.

1494 **7.3.2 Patch Management**

1495 Specific devices such as IEDs, PLCs, smart meters, etc., will be deployed in a variety of
1496 environments and critical systems, and their accessibility may necessitate undertaking complex
1497 activities to enable software upgrades or patches because of how distributed and isolated the
1498 equipment can be. Also, many unforeseen consequences can arise from changing firmware in a
1499 device that is part of a larger engineered system. Control systems require considerable testing
1500 and qualification to maintain reliability factors.

1501 The patch, test, and deploy life cycle is fundamentally different in the electrical sector. It can
1502 take a year or more (for good reason) to go through a qualification of a patch or upgrade. Thus
1503 there are unique challenges to be addressed in how security upgrades to firmware need to be
1504 managed.

1505 Deployment of a security upgrade or patch is unlikely to be as rapid as in the IT industry. Thus
1506 there needs to be a process whereby the risk and impact of vulnerability can be determined in
1507 order to prioritize upgrades. A security infrastructure also needs to be in place that can mitigate
1508 possible threats until needed upgrades can be qualified and deployed so that the reliability of the
1509 system can be maintained.

1510 **7.3.3 Authentication**

1511 There is no centralized authentication in the decentralized environment of the power grid, and
1512 authentication systems need to be able to operate in this massively distributed and locally
1513 autonomous setting. For example, substation equipment such as IEDs needs to have access
1514 controls that allow only authorized users to configure or operate them. However, credential
1515 management schemes for such systems cannot rest on the assumption that a constant network
1516 connection to a central office exists to facilitate authentication processes. What is called for are
1517 secure authentication methods that allow for local autonomy when needed and yet can provide
1518 for revocation and attribution from a central authority as required. Equally important is the
1519 recognition that any authentication processes must securely support emergency operations and
1520 not become an impediment at a critical time.

1521 **7.3.4 System Trust Model**

1522 There has to be a clear idea of what elements of the system are trusted—and to what level and
1523 why. Practically speaking, there will always be something in the system that has to be trusted;
1524 the key is to identify the technologies, people, and processes that form the basis of that trust. For
1525 example, we could trust a private network infrastructure more than an open public network,
1526 because the former poses less risk. However, even here there are dependencies based on the
1527 design and management of that network that would inform the trust being vested in it.

1528 **7.3.5 User Trust Model**

1529 Today and in the future, many operational areas within the Smart Grid are managed and
1530 maintained by small groups of trusted individuals operating as close-knit teams. These
1531 individuals are characterized by multi-decade experience and history in their companies.
1532 Examples include distribution operations departments, field operations, and distribution
1533 engineering/planning. Security architectures designed for large-scale, public access systems such
1534 as credit card processing, database applications, etc., may be completely inappropriate in such
1535 settings and actually weaken security controls. IT groups will almost always be required for

1536 proper installation of software and security systems on user PCs. However, for these unique
1537 systems, administration of security assets, keys, passwords, etc., that require heavy ongoing
1538 dependence on IT resources may create much larger and unacceptable vulnerabilities.

1539 In terms of personnel security, it may be worthwhile considering what is known as “two-person
1540 integrity,” or “TPI.” TPI is a security measure to prevent single-person access to key
1541 management mechanisms. This practice comes from national security environments but may
1542 have some applicability to the Smart Grid where TPI security measures might be thought of as
1543 somewhat similar to the safety precaution of having at least two people working in hazardous
1544 environments.

1545 Another area of concern related to personnel issues has to do with not having a backup to
1546 someone having a critical function; in other words, a person (actor) as a single point of failure
1547 (SPOF).

1548 **7.3.6 Security Levels**

1549 A security model needs to be built with different security levels that depend on the design of the
1550 network/system architecture, security infrastructure, and how trusted the overall system and its
1551 elements are. This model can help put the choice of technologies and architectures within a
1552 security context and guide the choice of security solutions.

1553 **7.3.7 Distributed vs. Centralized Model of Management**

1554 There are unique issues respecting how to manage something as distributed as the Smart Grid
1555 and yet maintain good efficiency and reliability factors that imply centralization. Many grid
1556 systems are highly distributed, are geographically isolated, and require local autonomy—as
1557 commonly found in modern substations. Yet these systems need to have a measure of centralized
1558 security management in terms of event logging/analysis, authentication, etc. There needs to be a
1559 series of standards in this area that can strike the right balance and provide for the “hybrid”
1560 approach necessary for the Smart Grid.

1561 **7.3.8 Local Autonomy of Operation**

1562 Any security system must have local autonomy; for example, it cannot always be assumed there
1563 is a working network link back to a centralized authority, and particularly in emergency-oriented
1564 operations, it cannot be the security system that denies critical actions from being taken.

1565 **7.3.9 Intrusion Detection for Power Equipment**

1566 One issue specific to power systems is handling specialized protocols like Modbus, DNP3,
1567 61850, etc., and standardized IDS and security event detection and management models need to
1568 be built for these protocols and systems. More specifically, these models need to represent a deep
1569 contextual understanding of device operation and state to be able to detect when anomalous
1570 commands might create an unforeseen and undesirable impact.

1571 **7.3.10 Network and System Monitoring and Management for Power Equipment**

1572 Power equipment does not necessarily use common and open monitoring protocols and
1573 management systems. Rather, those systems often represent a fusion of proprietary or legacy-
1574 based protocols with their own security issues. There is a need for openly accessibility

1575 information models and protocols that can be used over a large variety of transports and devices.
1576 There might even be a need for bridging power equipment into traditional IT monitoring systems
1577 for their cyber aspects. The management interfaces themselves must also be secure, as early
1578 lessons with the Simple Network Management Protocol (SNMP) have taught the networking
1579 community. Also, and very importantly, the system monitoring and management will have to
1580 work within a context of massive scale, distribution, and often, bandwidth-limited connections.

1581 **7.3.11 Security Event Management**

1582 Building on more advanced IDS forms for Smart Grid, security monitoring data/information
1583 from a wide array of power and network devices/systems must start to become centralized and
1584 analyzed for detecting events on a correlated basis. There also need to be clear methods of
1585 incident response to events that are coordinated between control system and IT groups. Both of
1586 these groups must be involved in security event definition and understanding as only they have
1587 the necessary operational understanding for their respective domains of expertise to understand
1588 what subtleties could constitute a threat.

1589 **7.3.12 Cross-Utility / Cross-Corporate Security**

1590 Unfortunately, many Smart Grid deployments are going forward without much thought to what
1591 happens behind the head end AMI systems and further on down the line for SCADA and other
1592 real-time control systems supporting substation automation and other distribution automation
1593 projects, as well as the much larger transmission automation functions. Many utilities have not
1594 thought about how call centers and DR control centers will handle integration with head end
1595 systems. Moreover, in many markets, the company that controls the head end to the meter
1596 portion is different than the one who decides what load to shed for a demand response. In many
1597 cases, those interconnections and the processes that go along with them have yet to be built or
1598 even discussed. Even in a completely vertically integrated system, there are many challenges
1599 with respect to separation of duties and least privilege versus being able to get the job done when
1600 needed. This also means designing application interfaces that are usable for the appropriate user
1601 population and implement threshold controls, so someone can't disconnect hundreds of homes in
1602 a matter of a few seconds either accidentally or maliciously.

1603 **7.3.13 Trust Management**

1604 Appropriate trust of a device must be based on the physical and logical ability to protect that
1605 device, and on protections available in the network. There are many devices that are physically
1606 accessible to adversaries by the nature of their locations, such as meters and pole-top devices,
1607 which also have limited anti-tamper protections due to cost. Systems that communicate with
1608 these devices should use multiple methods to validate messages received, should be designed to
1609 account for the possibility that exposed devices may be compromised in ways that escape
1610 detection, and should never fully trust those devices.

1611 For example, even when communicating with meters authenticated by public key methods and
1612 with strong tamper resistance, unexpected or unusual message types, message lengths, message
1613 content, or communication frequency or behavior could indicate that the meter's tamper
1614 resistance has been defeated and its private keys have been compromised. Such a successful
1615 attack on a meter must not result in possible compromise of the AMI head end.

1616 Similarly, because most pole-top devices have very little physical protection, the level of trust for
1617 those devices must be limited accordingly. An attacker could replace the firmware, or, in many
1618 systems, simply place a malicious device between the pole-top device and the network
1619 connection to the Utility network since these are often designed as separate components with
1620 RJ45 connectors. If the head end system for the pole-top devices places too much trust in them, a
1621 successful attack on a pole-top device can be used as a stepping stone to attack the head end.

1622 Trust management lays out several levels of trust based on physical and logical access control
1623 and the criticality of the system (i.e., most decisions are based on how important the system is).
1624 In this type of trust management, each system in the Smart Grid is categorized not only for its
1625 own needs (CI&A, etc.) but according to the required trust and/or limitations on trust mandated
1626 by our ability to control physical and logical access to it and the desire to do so (criticality of the
1627 system). This will lead to a more robust system where compromise of a less trusted component
1628 will not easily lead to compromise of more trusted components.

1629 **7.3.14 Management of Decentralized Security Controls**

1630 Many security controls, such as authentication and monitoring, may operate in autonomous and
1631 disconnected fashion because of the often remote nature of grid elements (e.g., remote
1632 substations). However, for auditing and centralized security management (e.g., revocation of
1633 credentials) requirements, this presents unique challenges.

1634 **7.3.15 Password Management**

1635 Passwords for authentication and authorization present many problems when used with highly
1636 distributed, decentralized, and variedly connected systems such as the Smart Grid. Unlike
1637 enterprise environments where an employee typically accesses organization services from one, or
1638 at most a few, desktop, laptop, or mobile computing systems, maintenance personnel may need
1639 to access hundreds of different devices, including IEDs, RTUs, relays, meters, etc. These devices
1640 may sometimes be accessed remotely from a central site, such as a control center, using simple
1641 tools such as terminal emulators, sometimes from a front panel with keyboard, sometimes from a
1642 locally connected laptop using a terminal emulator, or sometimes from specialized local access
1643 ports such as the optical port on a meter. Access must be able to operate without relying on
1644 communications to a central server (e.g., RADIUS, Active Directory) since access may be
1645 required for power restoration when communications are out. Setting different passwords for
1646 every device and every user may be impractical—see Sections 7.2.1, 7.2.2, 7.2.3, and 7.2.9.

1647 NIST SP 800-118, *DRAFT Guide to Enterprise Password Management*, gives reasonable
1648 guidance regarding password complexity requirements, but the password management
1649 techniques it describes will often be inapplicable due to the nature of power system equipment as
1650 discussed above. Suitable password management schemes need to be developed—if possible—
1651 that take into account both the nature of Smart Grid systems and of users. Alternatively, multi-
1652 factor authentication approaches should be considered.

1653 **7.3.16 Authenticating Users to Control Center Devices and Services**

1654 Control center equipment based on modern operating systems such as UNIX or Windows
1655 platforms is amenable to standard Enterprise solutions such as RADIUS, LDAP, or Active
1656 Directory. Nevertheless, these mechanisms may require modification or extension in order to
1657 incorporate “break glass” access or to interoperate with access mechanisms for other equipment.

1658 Some access policies commonly used in enterprise systems, such as expiring passwords and
1659 locking screen savers, are not appropriate for operator consoles.

1660 **7.3.17 Authentication of Devices to Users**

1661 When accessing Smart Grid devices locally, such as connecting to a meter via its optical port,
1662 authentication of the device to the user is generally not necessary due to the proximity of the
1663 user. When accessing Smart Grid devices via a private secure network such as a LAN in a
1664 substation tunneled to the control center, or an AMI network with appropriate encryption, non-
1665 secure identification of devices, such as by IP address, may be sufficient.

1666 A similar problem to this is that of ensuring that the correct Web server is reached via a Web site
1667 address. In Web systems, this problem is solved by SSL certificates that include the Domain
1668 Name Service (DNS) identity.

1669 **7.3.18 Tamper Evidence**

1670 In lieu of or in addition to tamper resistance, tamper evidence will be desirable for many devices.
1671 Both tamper resistance and tamper evidence must be resistant to false positives in the form of
1672 both natural actions, such as earthquakes, and adversarial actions. Tamper evidence for meters
1673 cannot require physical inspection of the meter since this would conflict with zero-touch after
1674 installation, but physical indicators might be appropriate for devices in substations.

1675 **7.3.19 Challenges with Securing Serial Communications**

1676 Cryptographic protocols such as TLS can impose too much overhead on bandwidth-constrained
1677 serial communications channels. Bandwidth-conserving and latency-sensitive methods are
1678 required in order to secure many of the legacy devices that will continue to form the basis of
1679 many systems used in the grid.

1680 **7.3.20 Legacy Equipment with Limited Resources**

1681 The life cycle of equipment in the electricity sector typically extends beyond 20 years. Compared
1682 to IT systems, which typically see 3–5 year life cycles, this is an eternity. Technology advances
1683 at a far more rapid rate, and security technologies typically match the trend. Legacy equipment,
1684 being 20 years old or more, is resource-limited, and it would be difficult and in some cases
1685 impractical to add security to the legacy device itself without consuming all available resources
1686 or significantly impacting performance to the point that the primary function and reliability of
1687 the device is hindered. In many cases, the legacy device simply does not have the resources
1688 available to upgrade security on the device through firmware changes. Security needs to be
1689 developed in such a manner that it has a low footprint on devices so that it can scale beyond 20
1690 years, and more needs to be done to provide a systemic and layered security solution to secure
1691 the system from an architectural standpoint.

1692 **7.3.21 Costs of Patch and Applying Firmware Updates**

1693 The costs associated with applying patches and firmware updates to devices in the electricity
1694 sector are significant. The balance of cost versus benefit of the security measure in the risk
1695 mitigation and decision process can prove prohibitive for the deployment if the cost outweighs
1696 the benefits of the deployed patch. Decision makers may choose to accept the risk if the cost is
1697 too high compared to the impact.

1698 The length of time to qualify a patch or firmware update, and the lack of centralized and remote
1699 patch/firmware management solutions, contributes to higher costs associated with patch
1700 management and firmware updates in the electricity sector. Upgrades to devices in the electricity
1701 sector can take a year or more to qualify. Extensive regression testing is extremely important to
1702 ensure that an upgrade to a device will not negatively impact reliability, but that testing also adds
1703 cost. Once a patch or firmware update is qualified for deployment, asset owners typically need to
1704 perform the upgrade at the physical location of the device due to a lack of tools for centralized
1705 and remote patch/firmware management.

1706 **7.3.22 Forensics and Related Investigations**

1707 It is already well known that industrial control systems do not generate a lot of security event
1708 data and typically do not report it back to a centralized source on a regular basis. Depending on
1709 the device, system health, usage, and other concerns, little data may get relayed back to data
1710 historians and/or maintenance management systems. Furthermore, as a matter of business policy,
1711 when faced with potential cyber security threats, electric utilities prioritize their obligation to
1712 maintain electric service over the requirements of the evidence collection needed to properly
1713 prosecute the perpetrators. With Smart Grid technology, additional threats are arising that may
1714 require a greater capability for generating and capturing data. Technologically sophisticated
1715 devices such as smart meters are being publicly exposed. At minimum, the meters should be
1716 capable of detecting and reporting physical tampering to identify energy theft or billing fraud.
1717 Moreover, HAN-level equipment will need to interact with the meter to support demand
1718 response. That necessitates having the tools and data to diagnose any problems resulting from
1719 either intentional manipulation or other causes. While it is rare that computer forensics is ever
1720 the sole basis for a successful prosecution or civil suit, it is critical that reliable means be defined
1721 to gather evidentiary material where applicable and that the tools be provided to maintain chain
1722 of custody, reduce the risk of spoliation, and ensure that the origin of the evidence can be
1723 properly authenticated. Tools should be capable of retrieving data from meters, collectors, and
1724 head end systems, as well as other embedded systems in substations, commercial and industrial
1725 customer equipment, and sensors along the lines in a read-only manner either at the source or
1726 over the network.

1727 **7.3.23 Roles and Role-Based Access Control**

1728 A *role* is a collection of permissions that may be granted to a user. An individual user may be
1729 given several roles or may be permitted different roles in different circumstances and may
1730 thereby exercise different sets of permissions in different circumstances.

1731 Roles clearly need to relate to the structure of the using entity and its policies regarding
1732 appropriate access. Both the structure and access policies properly flow down from regulatory
1733 requirements and organizational governance (i.e., from the high, nontechnical levels of the
1734 GridWise Architecture Council [GWAC] stack).

1735 Issues in implementing role-based access control (RBAC) include the following:

- 1736 1. The extent to which roles should be predefined in standards versus providing the
1737 flexibility for individual entities to define their own. Is there a suitable default set of roles
1738 that is applicable to the majority of the utility industry but can be tailored to the needs of
1739 a specific entity? Such roles might include—

- 1740 – Auditors: users with the ability to only read/verify the state of the devices (this
1741 may include remote attestation);
 - 1742 – System dispatchers: users who perform system operational functions in control
1743 centers;
 - 1744 – Protection engineers: users who determine and install/update settings of protective
1745 relays and retrieve log information for analysis of disturbances;
 - 1746 – Substation maintainers: users who maintain substation equipment and have access
1747 requirements to related control equipment;
 - 1748 – Administrators: users who can add, remove, or modify the rights of other users;
1749 and
 - 1750 – Security officers: users who are able to change the security parameters of the
1751 device (e.g., authorize firmware updates).
- 1752 2. Management and usability of roles. How many distinct roles become administratively
1753 unwieldy?
 - 1754 3. Policies need to be expressed in a manner that is implementable and relates to an entity's
1755 implemented roles. Regulators and entity governance need guidance on how to express
1756 implementable policies.
 - 1757 4. Support for nonhierarchical roles. The best example is originator and checker (e.g., of
1758 device settings). Any of a group of people can originate and check, but the same person
1759 cannot do both for the same item.
 - 1760 5. Approaches to expressing roles in a usable manner.
 - 1761 6. Support for emergency access that may need to bypass normal role assignment.
 - 1762 7. Which devices need to support RBAC? Which do not?

1763 **7.3.24 Limited Sharing of Vulnerability and/or Incident Information**

1764 There is a significant reticence with respect to sharing information about vulnerabilities or
1765 incidents in any critical infrastructure industry. This is based on many sound reasons—not the
1766 least of which may be that lives could be on the line and that it can take a considerable amount of
1767 time to qualify an upgrade or patch to fix any issue in complex control systems. There needs to
1768 exist a better framework for securely sharing such information and quickly coming to field-level
1769 mitigations until infrastructure can be upgraded. There also needs to be a better system of
1770 accountability and confidentiality when sharing sensitive vulnerability information with any third
1771 party, be it government or private institution.

1772 **7.3.25 Data Flow Control Vulnerability Issue**

1773 The power grid will encompass many networks and subnetworks, and the challenge will be to
1774 regulate which system can access or talk to another system.

1775 If a user on system A is authorized to perform a device firmware upgrade on device A, if device
1776 A is moved (stolen, replaced, etc.) to system B, how is the authorization tracked? How do you
1777 ensure that the control information is not being diverted to another unauthorized device/system?

1778 There is probably a need for intersection of security at various layers.

1779 **7.3.26 Public vs. Private Network Use**

1780 There is ongoing debate in the industry over the use of public network infrastructures such as the
1781 Internet or of the public cellular or WiMax networks that telecommunication companies provide.
1782 (Here the term *public network* should not be confused with the use of the Internet Protocol or IP
1783 in a *private network* infrastructure.) The reality is that many elements of the Smart Grid might
1784 already or will in future make use of public networks. The cyber security risks that this
1785 introduces need to be addressed by a risk management framework and model that takes this
1786 reality into account. It should be clear that if critical real-time command and control functions
1787 are carried over public networks such as the Internet (even if technically possible), such a
1788 scheme carries significantly more risk of intrusion, disruption, tampering, and general reliability
1789 regardless of the countermeasures in place. This is true because of the sheer accessibility of the
1790 system by anyone in the world regardless of location and the fact that countermeasures are
1791 routinely defeated because of errors in configuration, implementation, and sometimes design.
1792 These should be self-evident facts in a risk metric that a model would produce.

1793 Any risk management framework would be well served to address this issue by—

- 1794 • Building a model that takes the nature of the network, its physical environment, and its
1795 architecture into account (e.g., is it private or public, is critical infrastructure sufficiently
1796 segmented away from general IT networks, are there physical protection/boundaries,
1797 etc.);
- 1798 • Assigning criticality and impact levels to Smart Grid functions/applications (e.g.,
1799 retrieval of metering data is not as critical as control commands); and
- 1800 • Identifying countermeasure systems (e.g., firewalls, IDS/IPS, SEM, encrypted links and
1801 data, etc.) and assigning mitigating levels as well as which Smart Grid functions they can
1802 reasonably be applied to and how.

1803 The end goal for the model should be to make the best security practices self-evident through a
1804 final quantitative metric without giving a specific prohibition.

1805 **7.3.27 Traffic Analysis**

1806 Traffic analysis is the examination of patterns and other communications characteristics to glean
1807 information. Such examination is possible, even if the communication is encrypted. Examples of
1808 relevant characteristics include—

- 1809 • The identity of the parties to the communication (possibly determined from address or
1810 header information sent “in the clear” even for otherwise encrypted messages);
- 1811 • Message length, frequency, and other patterns in the communications; and
- 1812 • Characteristics of the signals that may facilitate identification of specific devices, such as
1813 modems. An example of such a characteristic might be the detailed timing or shape of the
1814 waveforms that represent bits.

1815 Regulations such as Federal Energy Regulatory Commission (FERC) Order No. 889 establish
1816 “Standards of Conduct” that prohibit market participants from having certain information on the
1817 operational state of the grid as known to grid control centers. In the Smart Grid, future

1818 regulations could possibly extend this concept to information outside the bulk power domain.
1819 Traffic analysis could enable an eavesdropper to gain information prohibited by such regulations.
1820 In addition, even if operational information were encrypted, traffic analysis could provide an
1821 attacker with enough information on the operational situation to enable more sophisticated
1822 timing of physical or cyber attacks.

1823 **7.3.28 Poor Software Engineering Practices**

1824 Poor software engineering practices, such as those identified in NISTIR 7628, Chapter 6,
1825 “Vulnerability Classes,” can lead to software that misoperates and may represent a security
1826 problem. Such problems are well known in software, but it should be recognized that embedded
1827 firmware may also be susceptible to such vulnerabilities [§7.5-12], and that many of the same
1828 good software engineering practices that help prevent these vulnerabilities in software may also
1829 be used for that purpose with firmware.

1830 **7.3.29 Attribution of Faults to the Security System**

1831 When communications or services fail in networks, there is sometimes a tendency to assume this
1832 failure is caused by the security system. This can lead to disabling the security system
1833 temporarily during problem resolution—or even permanently if re-enabling security is forgotten.
1834 Security systems for the Smart Grid need to allow and support troubleshooting.

1835 **7.3.30 Need for Unified Requirements Model**

1836 Within each operating domain (such as distribution operations, control center operations, etc.)
1837 multiple, ambiguous, or potentially conflicting implementation requirements must be resolved
1838 and settled upon. If security advisors cannot know what to expect from products meeting a
1839 certain standard, then each acquisition cycle will involve a unique security specification. Under
1840 such circumstances, it will be nearly impossible for suppliers to provide products in a timely
1841 fashion, and diverse systems will be difficult or impossible for customers to administer. The
1842 scope of this effort should cover such things as password complexity, required security roles,
1843 minimum numbers of supported user IDs, etc.

1844 **7.3.31 Broad Definition of Availability**

1845 One of the stated goals of the NIST cyber security effort is to assure “availability” at the
1846 application level. “Availability” according to the DHS *Catalog of Control Systems Security:
1847 Recommendations for Standards Developers* [§7.5-13], is—

1848 Availability— The property of a system or a system resource being accessible and usable
1849 upon demand by an authorized system entity, according to performance specifications for
1850 the system.

1851 Presenting such a broad definition to the power delivery organization responsible for achieving
1852 that availability, considering the complexity of the Smart Grid, represents a very substantial and
1853 perhaps impractical challenge, for several reasons—

- 1854 • The system, being so broadly defined, could be considered many different systems or
1855 many different combinations of systems. Does the system need to be defined as including
1856 all of the Smart Grid applications? Does it include future applications?

- 1857 • As a result, just defining what the “system” is that is being protected could be difficult to
1858 reach consensus on.
- 1859 • “Performance specifications” even for well-defined systems such as a SCADA system
1860 will often not be stated in a way that allows underlying media and subsystems to be
1861 evaluated. For example, most SCADA systems are designed with certain maximum poll
1862 rates and response times, but not necessarily with any requirement for availability in
1863 terms of communication interruptions or interference effects. These systems are usually
1864 purchased in pieces, with master stations, communications, and field equipment as
1865 entirely separate components without any overall specification of the system performance
1866 requirements. Thus, the traceability of the performance of all of the individual
1867 components and features to system availability as a whole may prove to be extremely
1868 difficult.
- 1869 • Availability in power system reliability means something different from availability (or
1870 non-denial of service) in security.
- 1871 • “Usable upon demand” in the definition of availability could mean many things in terms
1872 of response time.

1873 If these systems were used for different purposes, perhaps some very general, functional
1874 requirements would suffice to guide the use of the Roadmap by the power delivery
1875 organizations. However, all of these systems deliver power; they are all structured similarly, with
1876 generation, transmission, and distribution as separate but interconnected systems.

1877 **7.3.32 Utility Purchasing Practices**

1878 Unlike many other industries, many customers (utilities) in the utility industry are large enough,
1879 and have enough purchasing power and longevity (these companies have very long histories and
1880 steady income) to be able to specify unique, often customer-specific product features and
1881 requirements. For example, prior to the advent of the DNP3 communication protocol, in North
1882 America alone, there were over 100 different SCADA protocols developed over the period from
1883 roughly 1955 to 1990. Many of these protocols were unique due to a customer requirement for
1884 what may have appeared to be a minor change but one which made their protocol
1885 implementation unique.

1886 Recently there have been efforts by region, state, and regulatory entities to create purchasing
1887 requirements. If not carefully coordinated, these efforts could have similar harmful effects.

1888 With regard to cyber security requirements, if security requirements are subject to interpretation,
1889 customers will each use their own preferences to specify features that will re-create the problem
1890 of the SCADA protocols. For the Smart Grid, this would be a serious problem, since the time and
1891 effort necessary to analyze, negotiate, implement, test, release, and maintain a collection of
1892 customer-specific implementations will greatly delay deployment of the Smart Grid.

1893 Specifically, with regard to the Smart Grid, recent procurements have shown little consistency,
1894 with each calling out different requirements. This can have an adverse affect on both
1895 interoperability and security.

1896 **7.3.33 Cyber Security Governance**

1897 From the IT Governance Institute (ITGI), and adopted by the Chartered Institute of Management
1898 Accountants (CIMA) and the International Federation of Accountants (IFAC), *governance* is
1899 defined as follows:

1900 Governance is the set of responsibilities and practices exercised by the board and
1901 executive management with the goal of providing strategic direction, ensuring that
1902 objectives are achieved, ascertaining that risks are managed appropriately and verifying
1903 that the enterprise's resources are used responsibly.

1904 Cyber security governance is really a subset of enterprise governance. What's included in
1905 enterprise governance that directly impacts cyber security governance for the Smart Grid is
1906 strategic direction: ensuring that goals and objectives are achieved, that business risk (including
1907 security risk) is managed appropriately, that resource utilization is efficiently and effectively
1908 managed in a responsible fashion, and that enterprise security activities are monitored to ensure
1909 success or risk mitigation as needed if there are failures in security.

1910 Since cyber security (information security), as opposed to IT security, encompasses an overall
1911 perspective on all aspects of data/information (whether spoken, written, printed, electronic, etc.)
1912 and how it is handled—from its creation to how it is viewed, transported, stored, and/or
1913 destroyed—it is up to the utility's board and executive management to ensure that the Smart
1914 Grid, as well as the overall electric grid, is protected as much as feasibly possible.

1915 The utility's board of directors and its executive management must be cognizant of the risks that
1916 must be taken into account regarding what vulnerabilities to security threats of any sort may
1917 ensue if Smart Grid systems are not created and managed carefully and how such risks may be
1918 mitigated.⁵

1919 Borrowing again from ITGI and its guide to "Information Security Governance: Guidance for
1920 Boards of Directors and Executive Management, 2nd Edition," the following represents a
1921 slightly edited perspective on the responsibilities of a utility's board of directors and executive
1922 management team regarding cyber security:

1923 *Utility's Boards of Directors/Trustees*

1924 It is a fundamental responsibility of Senior Management to protect the interests of the
1925 utility's stakeholders. This includes understanding risks to the business and the electric
1926 grid to ensure they are adequately addressed from a governance perspective. Doing so
1927 effectively requires risk management, including cyber security risks, by integrating cyber
1928 security governance into the overall enterprise governance framework of the utility.

1929 Cyber security governance for the electric grid as a whole requires strategic direction and
1930 impetus. It requires commitment, resources and assignment of responsibility for cyber
1931 and information security management, as well as a means for the Board to determine
1932 that its intent has been met for the electric grid as part of the critical infrastructure of the
1933 United States. Experience has shown that effectiveness of cyber security governance is
1934 dependent on the involvement of senior management in approving policy, and
1935 appropriate monitoring and metrics coupled with reporting and trend analysis regarding
1936 threats and vulnerabilities to the electric grid.

⁵ See Title XIII, Section 1309 of the Energy Independence and Security Act of 2007 (EISA), U.S Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE).

1937
1938
1939
1940
1941
1942
1943
1944

Members of the Board need to be aware of the utility's information assets and their criticality to ongoing business operations of the electric grid. This can be accomplished by periodically providing the board with the high-level results of comprehensive risk assessments and business impact analysis. It may also be accomplished by business dependency assessments of information resources. A result of these activities should include Board Members validating/ratifying the key assets they want protected and confirming that protection levels and priorities are appropriate to a recognized standard of due care.

1945
1946
1947
1948
1949
1950

The tone at the top (top-down management) must be conducive to effective security governance. It is unreasonable to expect lower-level personnel to abide by security policies if senior management does not. Visible and periodic board member endorsement of intrinsic security policies provides the basis for ensuring that security expectations are met at all levels of the enterprise and electric grid. Penalties for non-compliance must be defined, communicated and enforced from the board level down.

1951

Utility Executives

1952
1953
1954
1955
1956
1957
1958
1959
1960

Implementing effective cyber security governance and defining the strategic security objectives of the utility are complex, arduous tasks. They require leadership and ongoing support from executive management to succeed. Developing an effective cyber security strategy requires integration with and cooperation of business unit managers and process owners. A successful outcome is the alignment of cyber security activities in support of the utility's objectives. The extent to which this is achieved will determine the effectiveness of the cyber security program in meeting the desired objective of providing a predictable, defined level of management assurance for business processes and an acceptable level of impact from adverse events.

1961
1962
1963
1964

An example of this is the foundation for the U.S. federal government's cyber security, which requires assigning clear and unambiguous authority and responsibility for security, holding officials accountable for fulfilling those responsibilities, and integrating security requirements into budget and capital planning processes.

1965

Utility Steering Committee

1966
1967
1968
1969
1970
1971
1972

Cyber security affects all aspects of the utility. To ensure that all Stakeholders affected by security considerations are involved, a Steering Committee of Executives should be formed. Members of such a committee may include, amongst others, the Chief Executive Officer (CEO) or designee, business unit executives, Chief Financial Officer (CFO), Chief Information Officer (CIO)/IT Director, Chief Security Officer (CSO), Chief Information Security Officer (CISO), Human Resources, Legal, Risk Management, Audit, Operations and Public Relations.

1973
1974
1975
1976
1977

A Steering Committee serves as an effective communication channel for Management's aims and directions and provides an ongoing basis for ensuring alignment of the security program with the utility's organizational objectives. It is also instrumental in achieving behavior change toward a culture that promotes good security practices and policy compliance.

1978

Chief Information Security Officer

1979
1980
1981
1982
1983
1984
1985

All utility organizations have a CISO whether or not anyone actually holds that title. It may be the CIO, CSO, CFO, or, in some cases, the CEO, even when there is an Information Security Office or Director in place. The scope and breadth of cyber security concerns are such that the authority required and the responsibility taken inevitably end up with a C-level officer or Executive Manager. Legal responsibility, by default, extends up the command structure and ultimately resides with Senior Management and the Board of Directors.

1986
1987

Failure to recognize this and implement appropriate governance structures can result in Senior Management being unaware of this responsibility and the attendant liability. It

1988 usually results in a lack of effective alignment of security activities with organizational
 1989 objectives of the utility.

1990 Increasingly, prudent and proactive management is elevating the position of Information
 1991 Security Officer to a C-level or Executive Position as utilities begin to understand their
 1992 dependence on information and the growing threats to it. Ensuring that the position
 1993 exists, and assigning it the responsibility, authority and required resources, demonstrates
 1994 Management's and Board of Directors' awareness of and commitment to sound cyber
 1995 security governance.

1996 **7.4 DESIGN CONSIDERATIONS**

1997 This subsection discusses cyber security considerations that arise in the design, deployment, and
 1998 use of Smart Grid systems and should be taken into account by system designers, implementers,
 1999 purchasers, integrators, and users of Smart Grid technologies. In discussing the relative merits of
 2000 different technologies or solutions to problems, these design considerations stop short of
 2001 recommending specific solutions or even requirements.

2002 **7.4.1 Break Glass Authentication**

2003 Authentication failure must not interfere with the need for personnel to perform critical tasks
 2004 during an emergency situation. An alternate form of “break glass” authentication may be
 2005 necessary to ensure that access can be gained to critical devices and systems by personnel when
 2006 ordinary authentication fails for any reason. A “break glass” authentication mechanism should
 2007 have the following properties—

- 2008 • Locally autonomous operation—to prevent failure of the “break glass” authentication
 2009 mechanism due to failure of communications lines or secondary systems;
- 2010 • Logging—to ensure that historical records of use of the “break glass” mechanism,
 2011 including time, date, location, name, employee number, etc., are kept;
- 2012 • Alarming—to report use of the “break glass” mechanism in real-time or near real-time to
 2013 an appropriate management authority, e.g., to operators at a control center or security
 2014 desk;
- 2015 • Limited authorization—to enable only necessary emergency actions and block use of the
 2016 “break glass” mechanism for non-emergency tasks; disabling logging particularly should
 2017 not be allowed; and
- 2018 • Appropriate policies and procedures—to ensure the “break glass” authentication is used
 2019 only when absolutely necessary and does not become the normal work procedure.

2020 Possible methods for performing “break glass” authentication include but are not limited to—

- 2021 • Backup authentication via an alternate password that is not normally known or available
 2022 but can be retrieved by phone call to the control center, by opening a sealed envelope
 2023 carried in a service truck, etc.;
- 2024 • Digital certificates stored in two-factor authentication tokens; and
- 2025 • One-time passwords.

2026 **7.4.2 Biometrics**

2027 **7.4.3 Password Complexity Rules**

2028 Password complexity rules are intended to ensure that passwords cannot be guessed or cracked
2029 by either online or offline password-cracking techniques. Offline password cracking is a
2030 particular risk for field equipment in unmanned substations or on pole-tops where the equipment
2031 is vulnerable to physical attack that could result in extraction of password hash databases and for
2032 unencrypted communications to field equipment where password hashes could be intercepted.

2033 Incompatible password complexity requirements can make reuse of a password across two
2034 different systems impossible. This can improve security since compromise of the password from
2035 one system will not result in compromise of password of the other system. Incompatible
2036 password complexity requirements might be desirable to force users to choose different
2037 passwords for systems with different security levels, e.g., corporate desktop vs. control system.
2038 However, forcing users to use too many different passwords can cause higher rates of forgotten
2039 passwords and lead users to write passwords down, thereby reducing security. Due to the large
2040 number of systems that utility engineers may need access to, reuse of passwords across multiple
2041 systems may be necessary. Incompatible password complexity requirements can also cause
2042 interoperability problems and make centralized management of passwords for different systems
2043 impossible. NIST SP 800-63, *Electronic Authentication Guideline*, contains some guidance on
2044 measuring password strength and recommendations for minimum password strengths.

2045 Some considerations for password complexity rules—

- 2046 1. Are the requirements based on a commonly recognized standard?
- 2047 2. Are the requirements strong enough to measurably increase the effort required to crack
2048 passwords that meet the rules?
- 2049 3. Are there hard constraints in the requirements (e.g., minimum and maximum lengths, min
2050 and max upper and lowercase, etc.) or soft constraints that simply measure password
2051 strength?
- 2052 4. Are any hard constraints "upper bounds" that can make selecting a password that meets
2053 two or more different complexity requirement sets impossible? For example, "must start
2054 with a number" and "must start with a letter" are irreconcilable requirements, whereas
2055 "must contain a number" and "must contain a letter" do not conflict.
- 2056 5. Are there alternatives to password complexity rules (such as running password-cracking
2057 programs on passwords as they are chosen) or two-factor authentication that can
2058 significantly increase security over that provided by password complexity rules while
2059 minimizing user burden?

2060 Draft NIST SP 800-118 gives further guidance on password complexity.

2061 **7.4.4 Authentication**

2062 There is no standard currently in the Smart Grid Framework and Roadmap that supports or
2063 provides guidance on how to accomplish strong authentication. The initial release of the NERC
2064 Critical Infrastructure Protection (CIP) standards did not require strong authentication. In
2065 accepting that version of the standards, FERC Order 706 requested NERC to incorporate strong
2066 authentication into a future version of the standards.

2067 During the drafting of IEEE-1686, the *IEEE Standard for Substation Intelligent Electronic*
2068 *Devices (IEDs) Cyber Security Capabilities*, an effort was made to incorporate strong
2069 authentication. The best source of information on strong authentication was found to be NIST
2070 SP 800-63, but the format of that document was found unsuitable as a normative reference for an
2071 IEEE standard. However, the technical material in NIST SP 800-63 provides some useful
2072 advantages for the following reasons:

- 2073 • The NERC CIP standards are moving from a concept of critical and noncritical assets to
2074 three levels of impact: High, Medium, Low;
- 2075 • NIST SP 800-63-1 provides four levels of authentication assurance, potentially mappable
2076 to both the NERC CIP impact levels and the similar approach being taken in the High-
2077 Level Requirements of NISTIR 7628;
- 2078 • NIST SP 800-63 provides a framework of requirements but is not overly prescriptive
2079 regarding implementation; and
- 2080 • The multilevel approach taken in NIST SP 800-63 is compatible with similar approaches
2081 previously taken in guidelines produced for the Bulk Electric System by the NERC
2082 Control Systems Security Working Group.

2083 NIST SP 800-63 is a performance specification with four levels of authentication assurance,
2084 selectable to match risk. The alternative levels range from Level 1, that allows a simple user ID
2085 and password, to Level 4, that is “intended to provide the highest practical remote network
2086 authentication assurance.” [§7.5-15] Multi-factor authentication is required at Levels 3 and 4.
2087 The NIST document grades the levels in terms of protection against increasingly sophisticated
2088 attacks.

2089 **7.4.5 Network Access Authentication and Access Control**

2090 Several link-layer and network-layer protocols provide network access authentication using
2091 Extensible Authentication Protocol [§7.5-1]. EAP supports a number of authentication
2092 algorithms—so called EAP methods.

2093 Currently EAP-TLS [§7.5-2] and EAP-GPSK (Generalized Pre-Shared Key) [§7.5-3] are the
2094 IETF Standard Track EAP methods generating key material and supporting mutual
2095 authentication. EAP can also be used to provide a key hierarchy to allow confidentiality and
2096 integrity protection to be applied to link-layer frames.

2097 EAP IEEE 802.1X [§7.5-4] provides port access control and transports EAP over Ethernet and
2098 Wi-Fi. In WiMAX, PKMv2 (Privacy Key Management version 2) in IEEE 802.16e [§7.5-5]
2099 transports EAP. PANA (Protocol for carrying Authentication for Network Access) [§7.5-6]
2100 transports EAP over UDP/IP (User Datagram Protocol/Internet Protocol). TNC (Trusted
2101 Network Connect) [§7.5-7] is an open architecture to enable network operators to enforce
2102 policies regarding endpoint integrity using the above mentioned link-layer technologies. There
2103 are also ongoing efforts in ZigBee[®] Alliance [§7.5-8] to define a network access authentication
2104 mechanism for ZigBee Smart Energy 2.0.

2105 In a large-scale deployment, EAP is typically used in pass-through mode where an EAP server is
2106 separated from EAP authenticators, and an AAA (Authentication, Authorization, and
2107 Accounting) protocol such as RADIUS [§7.5-9] is used by a pass-through EAP authenticator for
2108 forwarding EAP messages back and forth between an EAP peer to the EAP server. The pass-

2109 through authenticator mode introduces a three-party key management, and a number of security
2110 considerations so called EAP key management framework [§7.5-10] have been made. If an AMI
2111 network makes use of EAP for enabling confidentiality and integrity protection at link-layer, it is
2112 expected to follow the EAP key management framework.

2113 **7.4.6 Use of Shared/Dedicated and Public/Private Cyber Resources**

2114 The decision whether to use the public Internet or any shared resource, public or private, will
2115 have significant impact on the architecture, design, cost, security, and other aspects of any part of
2116 the Smart Grid. This section provides a checklist of attributes with which architects and
2117 designers can conduct a cost/trade analysis of these different types of resources.

2118 The objective of any such analysis is to understand the types of information that will be
2119 processed by the cyber resources under consideration, and to evaluate the information needs
2120 relative to security and other operational factors. These needs should be evaluated against the
2121 real costs of using different types of resources. For example, use of the public Internet may be
2122 less costly than developing, deploying, and maintaining a new infrastructure, but it may carry
2123 with it performance or security considerations to meet the requirements of the Smart Grid
2124 information that would have to be weighed against the cost savings.

2125 Each organization should conduct its own analyses—there is not one formula that is right for all
2126 cases.

2127 **7.4.6.1 Definitions**

2128 There are two important definitions to keep in mind when performing the analysis—

- 2129 1. Cyber Equipment—anything that processes or communicates Smart Grid information or
2130 commands.
- 2131 2. Internet—An element of Smart Grid data is said to have used the Internet if at any point
2132 while traveling from the system that generates the data-containing message to its ultimate
2133 destination it passes through a resource with an address within an RIR (Regional Internet
2134 Registry) address space.

2135 **7.4.6.2 Checklist/Attribute Groupings**

2136 There following five lists contain attributes relevant to one dimension of the cost/trade
2137 analysis—

- 2138 1. Attributes related to Smart Grid Information—this list could be viewed as the
2139 requirements of the information that is to be processed by the Smart Grid cyber resource;
 - 2140 a. Sensitivity and Security Requirements;
 - 2141 – Integrity,
 - 2142 – Confidentiality,
 - 2143 – Timeliness considerations—how long is the information sensitive?
 - 2144 – Availability, and
 - 2145 – Strategic vs. tactical information—aggregation considerations/impacts;
 - 2146 b. Ownership—who owns the data;

- 2147 c. Who has a vested interest in the data (e.g., customer use data);
- 2148 d. Performance/Capacity/Service-level requirements; and
- 2149 - Latency,
- 2150 - Frequency of transmission,
- 2151 - Volume of data,
- 2152 - Redundancy/Reliability, and
- 2153 - Quality of Service; and
- 2154 e. Legal/Privacy considerations—in this context, privacy is not related to protection
- 2155 of the data as it moves through the Smart Grid. It is related to concerns
- 2156 stakeholders in the information would have in its being shared. For example,
- 2157 commercial entities might not wish to have divulged how much energy they use.
- 2158 2. Attributes of a Smart Grid Cyber Resource—cyber resources have capabilities/attributes
- 2159 that must be evaluated against the requirements of the Smart Grid information;
- 2160 a. Ownership
- 2161 - Dedicated, and
- 2162 - Shared;
- 2163 b. Controlled/managed by
- 2164 - Internal management,
- 2165 - Outsourced management to another organization, and
- 2166 - Outsourced management where the resource can be shared with others;
- 2167 c. Geographic considerations—jurisdictional consideration;
- 2168 d. Physical Protections that can be used
- 2169 - Media,
- 2170 1. Wired, and
- 2171 2. Wireless.
- 2172 a. Not directed, and
- 2173 b. Directed
- 2174 - Equipment, and
- 2175 - Site;
- 2176 e. Performance/Scale Characteristics
- 2177 - Capacity per unit time (for example, a measure of bandwidth),
- 2178 - Maximum utilization percentage,

- 2179
 - 2180
 - 2181
 - Ability to scale—are forklift upgrades needed? Related to this is the likelihood of a resource being scaled—what are the factors (economic and technical) driving or inhibiting upgrade?
 - 2182
 - Latency, and
 - 2183
 - Migration—ability to take advantage of new technologies;
 - 2184
 - f. Reliability;
 - 2185
 - g. Ability to have redundant elements; and
 - 2186
 - h. Known security vulnerabilities.
 - 2187
 - Insider attacks,
 - 2188
 - DOS,
 - 2189
 - DDOS, and
 - 2190
 - Dependency on other components.
- 2191
 - 3. Attributes related to Security and Security Properties—given a type of information and the type of cyber resource under consideration, a variety of security characteristics could be evaluated—including different security technologies and appropriate policies given the information processed by, and attributes of, the cyber resource.
- 2192
 - 2193
 - 2194
 - a. Physical security and protection;
 - 2195
 - 2196
 - b. Cyber protection
 - 2197
 - Application level Controls,
 - 2198
 - Network level controls, and
 - 2199
 - System;
 - 2200
 - c. Security/Access policies
 - 2201
 - Inter organizational, and
 - 2202
 - Intra organizational;
 - 2203
 - d. Cross-administrative domain boundary policies; and
 - 2204
 - e. Specific technologies.
- 2205
 - 4. Attributes related to Operations and Management—one of the most complex elements of a network is the ongoing operations and management necessary after it has been deployed. This set of attributes identifies key issues to consider when thinking about different types of Smart Grid cyber resources (e.g., public/private and shared/dedicated).
- 2206
 - 2207
 - 2208
 - a. Operations
 - 2209
 - People,
 - 2210
 - 1. Domain Skills (e.g., knowledge of control systems), and
 - 2211
 - 2. IT Operations Skills (e.g., systems and network knowledge).
 - 2212
 - Processes
 - 2213

- 2214 1. Coordination
- 2215 a. Within a department,
- 2216 b. Across departments, and
- 2217 c. Across organizations/enterprises.
- 2218 2. Access Controls
- 2219 a. Third Party, and
- 2220 - Frequency,
- 2221 - Control, and
- 2222 - Trusted/Untrusted party (e.g., vetting process).
- 2223 b. Employees; and
- 2224 3. Auditing.
- 2225 b. System-level and Automated Auditing;
- 2226 c. Monitoring
- 2227 - Unit(s) monitored—granularity,
- 2228 - Frequency,
- 2229 - Alarming and events,
- 2230 - Data volume,
- 2231 - Visibility to data,
- 2232 - Sensitivity, and
- 2233 - Archival and aggregation; and
- 2234 d. Management.
- 2235 - Frequency of change,
- 2236 - Granularity of change,
- 2237 - Synchronization changes,
- 2238 - Access control,
- 2239 - Rollback and other issues, and
- 2240 - Data management of the configuration information.
- 2241 5. Attributes related to Costs—the cost attributes should be investigated against the different
- 2242 types of cyber resources under consideration. For example, while a dedicated resource
- 2243 has a number of positive performance attributes, there can be greater cost associated with
- 2244 this resource. Part of the analysis should be to determine if the benefits justify the cost.
- 2245 The cost dimension will cut across many other dimensions.
- 2246 a. Costs related to the data
- 2247 - Cost per unit of data,

- 2248 – Cost per unit of data over a specified time period, and
- 2249 – Oversubscription or SLA costs;
- 2250 b. Costs related to resources (cyber resources)
- 2251 – Resource acquisition cost (properly apportioned),
- 2252 – Resource installation cost,
- 2253 – Resource configuration,
- 2254 – Resource operation and management cost, and
- 2255 – Monitoring cost;
- 2256 c. Costs related to operational personnel
- 2257 – Cost of acquisition,
- 2258 – Cost of ongoing staffing, and
- 2259 – Cost of Training;
- 2260 d. Costs related to management software
- 2261 – Infrastructure costs,
- 2262 – Software acquisition costs,
- 2263 – Software deployment and maintenance costs, and
- 2264 – Operational cost of the software—staff, etc.; and
- 2265 e. How are the common costs being allocated and shared?

2266 7.5 REFERENCES

- 2267 1. Aboba, B., L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowitz, "Extensible
2268 Authentication Protocol (EAP)", RFC3748. The Internet Society, 2004.
2269 <http://www.ietf.org/rfc/rfc3748.txt> (accessed December 5, 2012).
- 2270 2. D. Simon, B. Aboba and R. Hurst, "The EAP-TLS Authentication Protocol", RFC 5216,
2271 The Internet Society, 2008. <http://www.ietf.org/rfc/rfc5216.txt> (accessed December 5,
2272 2012).
- 2273 3. Clancy, T. and H. Tschofenig, "Extensible Authentication Protocol - Generalized Pre-
2274 Shared Key (EAP-GPSK) Method", RFC5433, The Internet Society, 2009.
2275 <http://www.ietf.org/rfc/rfc5433.txt> (accessed December 5, 2012).
- 2276 4. *IEEE Standard for Local and Metropolitan Area Networks Port-based Network Access*
2277 *Control*, IEEE Std 802.1X-2004. New York, NY: The Institute of Electrical and
2278 Electronics Engineers, Inc. (IEEE), 2004.
- 2279 5. *IEEE Draft Standard for Local and metropolitan area networks Part 16: Air Interface for*
2280 *Broadband Wireless Access Systems ((Revision of IEEE Std 802.16-2004 and*
2281 *consolidates material from IEEE Std 802.16e-2005, IEEE Std 802.16-2004/Cor1-2005,*
2282 *IEEE Std 802.16f-2005 and IEEE Std 802.16g-2007)), IEEE Unapproved Draft Standard*
2283 *P802.16Rev2_D4*, New York, NY: IEEE, 2008..

2284 6. D. Forsberg and others, "Protocol for Carrying Authentication for Network Access
2285 (PANA)", RFC5191, The Internet Society, 2008. <http://www.ietf.org/rfc/rfc5191.txt>
2286 (accessed December 5, 2012).

2287 7. Trusted Network Connect (TNC), the Trusted Computing Group.
2288 http://www.trustedcomputinggroup.org/developers/trusted_network_connect (accessed
2289 [December 5, 2012](http://www.trustedcomputinggroup.org/developers/trusted_network_connect)).

2290 8. ZigBee[®] Alliance, <http://www.zigbee.org/>

2291 9. Rigney C, Willens S, Rubens A and Simpson W, "Remote authentication dial in user
2292 service (RADIUS)", RFC 2865, <http://www.ietf.org/rfc/rfc2865.txt>, June 2000.

2293 10. B. Aboba, D. Simon and P. Eronen, "Extensible Authentication Protocol (EAP) Key
2294 Management Framework", RFC 5247, <http://www.ietf.org/rfc/rfc5247.txt>, August 2008.

2295 11. Donggang Liu, Peng Ning, "Establishing Pairwise Keys in Distributed Sensor Networks,"
2296 in Proceedings of the 10th ACM Conference on Computer and Communications Security
2297 (CCS '03), pages 52--61, Washington D.C., October, 2003.

2298 12. Katie Fehrenbacher "Smart Meter Worm Could Spread Like a Virus",
2299 <http://earth2tech.com/2009/07/31/smart-meter-worm-could-spread-like-a-virus/>.

2300 13. Department of Homeland Security, National Cyber Security Division, *Catalog of Control*
2301 *Systems Security: Recommendations for Standards Developers*, March 2010.

2302 14. NERC Control Systems Security Working Group (CSSWG) document, *Security*
2303 *Guideline for the Electricity Sector: Time Stamping of Operational Data Logs*, v. 0.995,
2304 http://www.nerc.com/docs/cip/sgwg/Timestamping_Guideline_009-11-11_Clean.pdf

2305 15. Burr, William E. and others. NIST Special Publication (SP) 800-63-1, *Electronic*
2306 *Authentication Guideline*, Gaithersburg, MD: NIST, 2011.

2307 16. Stouffer, Keith, Joe Falco, and Karen Scarfone, NIST SP 800-82, *Guide to Industrial*
2308 *Control Systems (ICS) Security*, Gaithersburg, MD: NIST, 2011.

2309 17. Scarfone, Karen and Murugiah Souppaya, DRAFT NIST SP 800-118, *Guide to*
2310 *Enterprise Password Management*, Gaithersburg, MD: NIST, 2009.

2311 18. Scarfone, Karen, Cyrus Tibbs, and Matthew Sexton, NIST SP 800-127, *Guide to*
2312 *Securing WiMAX Wireless Communications*, Gaithersburg, MD: NIST, 2010.

2313

2314 **CHAPTER EIGHT**
2315 **RESEARCH AND DEVELOPMENT THEMES FOR**
2316 **CYBERSECURITY IN THE SMART GRID**

2317 **8.1 INTRODUCTION**

2318 Cyber security is one of the key technical areas where the state of the art falls short of meeting
2319 the envisioned functional, reliability, and scalability requirements of the Smart Grid. This
2320 chapter is the deliverable produced by the R&D subgroup of SGIP-CSWG based on the inputs
2321 from various group members. In general, *research* involves discovery of the basic science that
2322 supports a product’s viability (or lays the foundation for achieving a target that is currently not
2323 achievable), *development* refers to turning something into a useful product or solution, and
2324 *engineering* refines a product or solution to a cost and scale that makes it economically viable.
2325 Another differentiation is basic research, which delves into scientific principles (usually done in
2326 universities), and applied research, which uses basic research to better human lives. Research can
2327 be theoretical or experimental. Finally, there is long-term (5–10 years) and short-term (less than
2328 5 years) research. This chapter stops short of specifying which of the above categories each
2329 research problem falls into. That is, we do not discuss whether something is research,
2330 development, engineering, short-term, or long-term, although we might do so in future revisions.
2331 In general, this chapter distills research and development themes that are meant to present
2332 paradigm changing directions in Cyber Security that will enable higher levels of reliability and
2333 security for the Smart Grid as it continues to become more technologically advanced.

2334 The topics are based partly on the experience of members of the SGIP-CSWG R&D group and
2335 research problems that are widely publicized. The raw topics submitted by individual group
2336 members were collected in a flat list and iterated over to disambiguate and re-factor them to a
2337 consistent set. The available sections were then edited, consolidated, and reorganized as the
2338 following five high-level theme areas:

- 2339 • Device Level
- 2340 • Cryptography and Key Management
- 2341 • Systems and Distributed Systems Level
- 2342 • Networking Issues
- 2343 • Other Security Issues in the Smart Grid Context

2344 These five groups collectively represent an initial cut at the thematic issues requiring immediate
2345 research and development to make the Smart Grid vision a viable reality. We expect that this
2346 R&D group will continue to revise and update this document as new topics are identified by
2347 other SGIP-CSWG subgroups such as bottom-up, vulnerability, and privacy; by comments from
2348 readers; and by tracking government, academic, and industry research efforts that are related to
2349 Smart Grid cyber security. These research efforts include the U.S. Department of Energy Control
2350 System Security and the National SCADA Testbed programs, U.S. Department of Homeland
2351 Security Control System Security program and Cyber Physical Systems Security efforts,⁶ the

⁶ See <https://www.enstg.com/Signup/files/DHS%20ST%20Cyber%20Workshop%20Final%20Report-v292.pdf>.

2352 industry Roadmap to Secure Control Systems, the UCA International Users group focusing on
2353 AMI security, and the North American Synchrophasor Initiative.

2354 This document is written as an independent collection of research themes, and as such, the
2355 sections do not necessarily flow from introduction to summary.

2356 **8.2 DEVICE-LEVEL TOPICS—COST-EFFECTIVE TAMPER-RESISTANT DEVICE** 2357 **ARCHITECTURES**

2358 **8.2.1 Improve Cost-Effective High Tamper-Resistant & Survivable Device Architectures**

2359 With intelligent electronic devices (IEDs) playing more critical roles in the Smart Grid, there is
2360 an increasing need to ensure that those IEDs are not easily attacked by firmware updates,
2361 commandeered by a spoofed remote device, or swapped out by a rogue device. At the same time,
2362 because of the unique nature and scale of these devices, protection measures need to be cost-
2363 effective as to deployment and use, and the protection measures must be mass-producible. Some
2364 initial forms of these technologies are in the field, but there is a growing belief that further
2365 improvement is needed, as security researchers have already demonstrated penetrations of these
2366 devices—even with some reasonable protections in place. Further, it is important to assume
2367 devices *will be* penetrated, and there must be a method for their containment and implementing
2368 secure recovery measures using remote means. This is of great importance to maintain the
2369 reliability and overall survivability of the Smart Grid.⁷

2370 Research is needed in devising scalable, cost-effective device architectures that can form a robust
2371 hardware and software basis for overall systems-level survivability and resiliency. Such
2372 architectures must be highly tamper-resistant and evident, and provide for secure remote
2373 recovery. Research into improved security for firmware/software upgrades is also needed.
2374 Without these R&D advances, local attacks can become distributed/cascading large-scale attack
2375 campaigns.

2376 Potential starting points for these R&D efforts are

- 2377 • NIST crypto tamper-evident requirements;
- 2378 • Mitigating (limiting) the value of attacks at end-points (containment regions in the Smart
2379 Grid architecture); and
- 2380 • Expiring lightweight keys.

2381 **8.2.2 Intrusion Detection with Embedded Processors**

2382 Research is needed to find ways to deal with the special features and specific limitations of
2383 embedded processors used in the power grid. A large number of fairly powerful processors, but
2384 with tighter resources than general-purpose computers and strict timeliness requirements,
2385 embedded in various types of devices, are expected to form a distributed internetwork of
2386 embedded systems. Intrusion detection in such systems does not merely consist in adapting the
2387 types of intrusion detection developed for classical IT systems.⁸

⁷ Please see Chapter 2 for discussion of defense-in-depth on a system-wide basis that would begin to address these issues.

⁸ Subsection 8.6.3 of this report discusses this issue in the context of protecting cyber-power systems.

2388 This work should also investigate the possible applications of advanced intrusion detection
2389 systems and the types of intrusion detection that may be possible for embedded processors, such
2390 as real-time intrusion detection.

2391 **8.3 CRYPTOGRAPHY AND KEY MANAGEMENT**

2392 **8.3.1 Topics in Cryptographic Key Management**

2393 Smart Grid deployments such as AMI will entail remote control of a large number of small
2394 processors acting as remote sensors, such as meters and smart devices. Home Area Networks
2395 (HANs) provide local sensing and actuation of smart appliances. HANs and devices may
2396 communicate and negotiate in a peer-to-peer manner. Security for such systems entails both key
2397 management on a scale involving possibly tens of millions of credentials and keys, and local
2398 cryptographic processing on the sensors such as encryption and digital signatures. This calls for
2399 research on large-scale, economic key management in conjunction with cryptography that can be
2400 carried out effectively on processors with strict limits on space and computation. This
2401 cryptography and key management should ideally be strong and open (free of intellectual
2402 property issues) to foster the necessary interoperability standards of the Smart Grid. Existing key
2403 management systems and methods could be explored as a basis of further innovation; examples
2404 can include public key infrastructure (PKI), identity-based encryption (IBE), and hierarchical,
2405 decentralized, and delegated schemes and their hybridization.

2406 There are also problems of ownership (e.g., utility vs. customer-owned) and trust, and how both
2407 can be optimally managed in environments where there is little physical protection and access
2408 may happen across different organizational and functional domains (e.g., a hub of multiple
2409 vendors/service providers, in-home gateway, aggregator, etc.) with their own credentials and
2410 security levels. This requires research into new forms of trust management, partitioning, tamper-
2411 proofing/detection, and federated ID management that can scale and meet reliability standards
2412 needed for the Smart Grid.

2413 The various devices/systems that will be found in the areas of distributed automation, AMI,
2414 distributed generation, substations, etc., will have many resource-constraining factors that have
2415 to do with limited memory, storage, power (battery or long sleep cycles), bandwidth, and
2416 intermittent connections. All of these factors require research into more efficient, *ad hoc*, and
2417 flexible key management that requires less centralization and persistent connectivity and yet can
2418 retain the needed security and trust levels of the entire infrastructure as compared to conventional
2419 means.

2420 Emergency (bypass) operations are a critical problem that must optimally be addressed. We
2421 cannot afford to have security measures degrade the reliability of the system by, for example,
2422 “locking out” personnel/systems during a critical event. Similarly, restoring power may require
2423 systems to “cold boot” their trust/security with little to no access to external
2424 authentication/authorization services. This requires research into key management and
2425 cryptography schemes that can support bypass means and yet remain secure in their daily
2426 operations.

2427 We must ensure that encrypted communications do not hinder existing power system and
2428 information and communication systems monitoring for reliability and security requirements
2429 (possibly from multiple parties of different organizations). Depending on the system context, this

2430 problem may require research into uniquely secure and diverse escrow schemes and supporting
2431 key management and cryptography that meet the various Smart Grid requirements discussed in
2432 this report.

2433 **8.3.2 Advanced Topics in Cryptography**

2434 Several security and privacy requirements for the Smart Grid may benefit from advanced
2435 cryptographic algorithms.

2436 **8.3.2.1 Privacy-enhancing cryptographic algorithms**

2437 Privacy-enhancing cryptographic algorithms can mitigate privacy concerns related to the
2438 collection of consumer data by computing functions on ciphertexts. This can be beneficial for
2439 third-party providers who want to access encrypted databases and would like to compute
2440 statistics over the data. Similarly, while utilities need to collect individual measurements for
2441 billing, they do not require real-time individual data collection to operate their network.
2442 Therefore, they can use aggregated data representing the consumption at a data aggregator.
2443 Homomorphic encryption schemes can provide privacy-preserving meter aggregation by
2444 performing additive computations on encrypted data. Using aggregated data limits the ability of
2445 the utility or any third party from learning individual consumer usage profiles. Research is
2446 needed on extending the efficiency and generality of current homomorphic encryption schemes
2447 to provide universal computation.

2448 **8.3.2.2 Cryptographic in-network aggregation schemes**

2449 Cryptographic in-network aggregation schemes have the potential of improving the efficiency of
2450 many-to-one communications in the Smart Grid, like those generated from multiple sensors to a
2451 single or a small number of designated collection points. To achieve efficient in-network
2452 aggregation, intermediate nodes in the routing protocol need to modify data packets in transit; for
2453 this reason, standard signature and encryption schemes are not applicable, and it is a challenge to
2454 provide resilience to tampering by malicious nodes. Therefore, we require homomorphic
2455 encryption and signature schemes tailored for efficient in-network aggregation.

2456 **8.3.2.3 Identity-Based Encryption**

2457 Key distribution and key revocation are some of the most fundamental problems in key
2458 distribution for systems. IBE is a new cryptographic primitive that eliminates the need for
2459 distributing public keys (or maintaining a certificate directory) because identities are
2460 automatically bound to their public keys. This allows, for example, a third party for energy
2461 services to communicate securely to their customers without requiring them to generate their
2462 keys. IBE also eliminates the need for key revocation because IBE can implement time-
2463 dependent public keys by attaching a validity period to each public key. In addition, for
2464 enterprise systems, a key escrow is an advantage for recovering from errors or malicious
2465 insiders. IBE provides this service because the private-key generator (PKG) can obtain the secret
2466 key of participants. This property suggests that IBE schemes are suitable for applications where
2467 the PKG is unconditionally trusted. Extending this level of trust for larger federated systems is
2468 not possible; therefore, very large deployments require hybrid schemes with traditional public
2469 key cryptography and certificates for the IBE parameters of each enterprise or domain.
2470 Alternatively, we can extend pure IBE approaches with further research on certificate-based
2471 encryption.

2472 **8.3.2.4 Access control without a mediated, trusted third party**

2473 The limited (or intermittent) connectivity of several Smart Grid devices requires further research
2474 into access control mechanisms without an online third party. Attribute-Based Encryption (ABE)
2475 is an emerging crypto-system that can be thought of as a generalization of IBE. In ABE schemes,
2476 a trusted entity distributes attribute or predicate keys to users. Data owners encrypt their data
2477 using the public parameters and attributes provided by the trusted entity or an attribute policy of
2478 their choosing. In ABE, users are able to decrypt ciphertexts only if the attributes associated with
2479 the ciphertext (or the keys of the users) satisfy the policy associated with the ciphertext (or the
2480 predicate associated with their keys); therefore, access control can be achieved without an online
2481 trusted server.

2482 **8.3.2.5 Interoperability with limited (or no) online connectivity**

2483 The limited (or intermittent) connectivity of Smart Grid devices may require local (e.g., HAN)
2484 mechanisms for key and content management. Proxy re-encryption and proxy re-signature
2485 schemes can alleviate this problem. In these schemes, a semi-trusted proxy (e.g., a HAN
2486 interoperability device) can convert a signature or a ciphertext computed under one key (e.g., the
2487 public key of device A) to another (e.g., the public key of device B), without the proxy learning
2488 any information about the plaintext message or the secret keys of the delegating party.

2489 **8.4 SYSTEMS-LEVEL TOPICS - SECURITY AND SURVIVABILITY ARCHITECTURE OF**
2490 **THE SMART GRID**

2491 While it is not uncommon for modern distribution grids to be built to withstand some level of
2492 tampering to meters and other systems that cannot be physically secured, as well as a degree of
2493 invalid or falsified data from home area networks, the envisioned Smart Grid will be a ripe target
2494 for malicious, well-motivated, well-funded adversaries. The increased dependence on
2495 information and distributed and networked information management systems in SCADA,
2496 WAMS, and PLCs imply that the Smart Grid will need much more than device authentication,
2497 encryption, failover, and models of normal and anomalous behavior, all of which are problems
2498 on their own given the scale and timeliness requirement of the Smart Grid. The Smart Grid is a
2499 long-term and expensive resource that must be built future-proof. It needs to be built to adapt to
2500 changing needs in terms of scale and functionality, and at the same time, it needs to be built to
2501 tolerate and survive malicious attacks of the future that we cannot even think of at this time.
2502 Research is clearly needed to develop an advanced protection architecture that is dynamic (can
2503 evolve) and focuses on resiliency (tolerating failures, perhaps of a significant subset of
2504 constituents). A number of research challenges that are particularly important in the Smart Grid
2505 context are described in the following subsections.

2506 **8.4.1 Scalability**

2507 The introduction of smart appliances and home area networks (HANs) increases the number of
2508 devices that a utility must manage by orders of magnitude. A utility with 1million customers
2509 currently monitoring 1million meters will conservatively see the number of devices two orders of
2510 magnitude higher (perhaps 100 million devices). The ability to control and schedule these
2511 through a central SCADA system will be severely limited. As such reliance will need to be on
2512 scheduling through HANs and distributed peer-to-peer energy management, or, an “energy

2513 internet.” System vulnerabilities will be increased through the addition of potential attack points.
2514 The increased number of devices will impact system reliability and system reliability models.

2515 **8.4.2 Architecting for bounded recovery and reaction**

2516 Effective recovery requires containing the impact of a failure (accidental or malicious); enough
2517 resources and data (e.g., state information) positioned to regenerate the lost capability; and real-
2518 time decision making and signaling to actuate the reconfiguration and recovery steps. Even then,
2519 guaranteeing the recovery within a bounded time is a hard problem and can be achieved only
2520 under certain conditions. To complicate things further, different applications in the Smart Grid
2521 will have different elasticity and tolerance, and recovery mechanisms may themselves affect the
2522 timeliness of the steady state, not-under-attack operation.

2523 With the presence of renewable energy sources that can under normal operation turn on or off
2524 unpredictably (cloud cover or lack of wind) and mobile energy sinks (such as the hybrid vehicle)
2525 whose movement cannot be centrally controlled, the Smart Grid becomes much more dynamic in
2526 its operational behavior. Reliability will increasingly depend on the ability to react to these
2527 events within a bounded time while limiting the impact of changes within a bounded spatial
2528 region. How does one architect a wide area distributed system of the scale of the Smart Grid such
2529 that its key components and designated events have a bounded recovery and reaction time and
2530 space? What resources need to be available? What cryptographic/key material needs to be
2531 escrowed or made available? How much data needs to be checkpointed and placed at what
2532 location? What is the circle of influence that needs to be considered to facilitate bounded
2533 recovery and reaction? These are the questions that the R&D task should answer.

2534 **8.4.3 Architecting Real-time security**

2535 In the context of Smart Grid, the power industry will increasingly rely on real-time systems for
2536 advanced controls. These systems must meet requirements for applications that have a specific
2537 window of time to correctly execute. Some “hard real-time” applications must execute within a
2538 few milliseconds. Wide area protection and control systems will require secure communications
2539 that must meet tight time constraints. Cyber physical systems often entail temporal constraints on
2540 computations because control must track the dynamic changes in a physical process. Typically
2541 such systems have been treated as self-contained and free of cyber security threats. However,
2542 increasing openness and interoperability, combined with the threat environment today, requires
2543 that such systems incorporate various security measures ranging from device and application
2544 authentication, access control, redundancy and failover for continued operation, through
2545 encryption for privacy and leakage of sensitive information. Real-time requirements must
2546 include the overhead resulting from insertion of these mechanisms. In some cases, security
2547 mechanisms have the potential to violate the real-time requirements by introducing
2548 uncontrollable or unbounded delays.

2549 Research in this area should provide strategies for minimizing and making predictable the timing
2550 impacts of security protections such as encryption, authentication, and rekeying and exploiting
2551 these strategies for grid control with security.

2552 **8.4.4 Calibrating assurance and timeliness trade-offs**

2553 There are various sources of delay in the path between two interacting entities in the Smart Grid
2554 (e.g., from the sensor that captures the measurement sample such as the PMU to the application

2555 that consumes it, or from the applications at the control center that invoke operations, upload
2556 firmware, or change parameter values to the affected remote smart device). Some such delay
2557 sources represent security mechanisms that already exist in the system, and many of these can be
2558 manipulated by a malicious adversary. To defend against potential attacks, additional security
2559 mechanisms are needed—which in turn may add more delay. On the other hand, security is not
2560 absolute, and quantifying cyber security is already a hard problem. Given the circular
2561 dependency between security and delay, the various delay sources in the wide area system, and
2562 the timeliness requirements of the Smart Grid applications, there is a need and challenge to
2563 organize and understand the delay-assurance tradespace for potential solutions that are
2564 appropriate for grid applications. As the smart grid scales, the ability of humans to react to
2565 systems operating in the millisecond time scale becomes limited. As such, there will need to be
2566 more reliance on embedded monitors and distributed embedded monitors to provide diagnosis
2567 and recovery actions. Only at the highest level of control can human operators become effective.
2568 Without an understanding of delay-assurance tradeoffs, at times of crisis operators will be ill-
2569 prepared and will have to depend on individual intuition and expertise. On the other hand, if the
2570 trade-offs are well understood, it will be possible to develop and validate contingency plans that
2571 can be quickly invoked or offered to human operators at times of crisis.

2572 **8.4.5 Legacy system integration**

2573 Integrating with legacy systems is a hard and inescapable reality in any realistic implementation
2574 of the Smart Grid. This poses a number of challenges to the security architecture of the Smart
2575 Grid:

- 2576 • Compatibility problems when new security solutions are installed in new devices
2577 resulting in mismatched expectations that may cause the devices to fail or malfunction
2578 (an anecdotal story tells of a network scan using tools like the Network MAPper [NMAP]
2579 tripping IEDs because they do not fully implement the TCP/IP stack); and
- 2580 • Backwards compatibility, which may often be a requirement (regulator, owner
2581 organization) and may prevent deployment of advanced features.

2582 **Relevant effort:**

- 2583 • Not just linking encryptors but conducting research in legacy systems beyond SCADA
2584 encryption; American Gas Association (AGA), AGA 12 Cryptography Working Group.

2585 **Potential avenues of investigation include:**

- 2586 • Compositionality (enhanced overlays, bump-in-the-wire⁹, adapters) that contain and mask
2587 legacy systems; and
- 2588 • Ensuring that the weakest link does not negate new architectures through formal analysis
2589 and validation of the architectural design, possibly using red team methodology.

2590 **8.4.6 Resiliency Management and Decision Support**

2591 Research into resiliency management and decision support will look at threat response escalation
2592 as a method to maintain system resiliency. While other Smart Grid efforts are targeted at

⁹ An implementation model that uses a hardware solution to implement IPsec.

2593 improving the security of devices, this research focuses on the people, processes, and technology
2594 options available to detect and respond to threats that have breached those defenses in the
2595 context of the Smart Grid’s advanced protection architecture. Some of the responses must be
2596 autonomic—timely response is a critical requirement for grid reliability. However, for a quick
2597 response to treat the symptom locally and effectively, the scope and extent of the impact of the
2598 failure needs to be quickly determined and mitigated. Not all responses can be autonomic,
2599 however. New research is needed to measure and identify the scope of a cyber attack and the
2600 dynamic cyber threat response options available in a way that can serve as a decision support
2601 tool for the human operators.

2602 **8.4.7 Efficient Composition of Mechanisms**

2603 It can sometimes be the case that even though individual components work well in their domains,
2604 compositions of them can fail to deliver the desired combination of attributes, or fail to deliver
2605 them efficiently. For example, a protocol in the X.509 draft standard was found to have a flaw
2606 which allowed an old session key to be accepted as new. Formal methods for cryptographic
2607 algorithm composition have helped but tend to concentrate on small, specific models of
2608 individual protocols rather than the composition of multiple algorithms as is typically the case in
2609 real implementations. In other circumstances, the composition of two useful models can cause
2610 unintended and unwanted inefficiencies. An example of this is the combination of the congestion
2611 control of TCP overlaid upon *ad hoc* mobile radio networks.

2612 Research that systematizes the composition of communications and/or cryptographic
2613 mechanisms and which assists practitioners in avoiding performance, security, or efficiency
2614 pitfalls would greatly aid the creation and enhancement of the Smart Grid.

2615 **8.4.8 Risk Assessment and Management**

2616 A risk-based approach is a potential way to develop viable solutions to security threats and
2617 measure the effectiveness of those solutions. Applying risk-based approaches to cyber security in
2618 the Smart Grid context raises a number of research challenges. The following subsections
2619 describe three important ones.

2620 **8.4.8.1 Advanced Attack Analysis**

2621 While it is clear that cyber attacks or combined cyber/physical attacks pose a significant threat to
2622 the power grid, advanced tools and methodologies are needed to provide a deep analysis of cyber
2623 and cyber/physical attack vectors and consequences on the power grid. For example, answering
2624 questions such as, “Can a cyber or combined cyber/physical attack lead to a blackout such as
2625 described in 8.6.5?”

2626 **8.4.8.2 Local Privacy**

2627 Detailed management of home devices (in a HAN) has the potential to divulge private
2628 information both through cyber channels and also through physical channels. Recent work in
2629 Non Intrusive Appliance Load Monitoring (NIALM) has shown very high fidelity event
2630 reconstruction through techniques such as hidden Markov models. Significant threats to

2631 individual privacy can be envisioned (in addition to the enterprise concerns in 8.6.1.1).¹⁰ Privacy
2632 cannot be ensured through cryptographic methods, alone.

2633 **8.4.8.3 Measuring Risk**

2634 The state of the art in the risk measurement area is limited to surveys and informal analysis of
2635 critical assets and the impact of their compromise or loss of availability. Advanced tools and
2636 techniques that provide quantitative notions of risks—that is, threats, vulnerabilities, and attack
2637 consequences for current and emerging power grid systems—will allow for better protection and
2638 regulation of power systems.

2639 **8.4.8.4 Risk-based Cyber/Physical Security Investment**

2640 When cyber security solutions are deployed, they mitigate risks. However, it is hard to assess the
2641 extent to which risk has been mitigated. A related question is how much investment in cyber
2642 security is appropriate for a given entity in the electric sector? Research into advanced tools and
2643 technologies based on quantitative risk notions that take into account not only cyber risks and
2644 physical risks, but combined cyber-physical risks in which cyber/physical vulnerabilities become
2645 interdependent. These include physical attacks informed by cyber in which uncovering cyber
2646 decisions leads to knowledge of physical system vulnerabilities such as congestion. These can
2647 also include cyber attacks enhancing physical attacks or a cyber system used to cause physical
2648 harm.

2649 **8.5 NETWORKING TOPICS**

2650 **8.5.1 Safe use of COTS / Publicly Available Systems and Networks**

2651 Economic and other drivers push the use of COTS (commercial off-the-shelf) components,
2652 public networks like the Internet, or available Enterprise systems. Research is needed to
2653 investigate if such resources can be used in the Smart Grid reliably and safely, and how they
2654 would be implemented.

2655 **8.5.1.1 Internet Usage in Smart Grid**

2656 A specific case is the use of the existing Internet in Smart Grid–related communications,
2657 including possibly as an emergency out-of-band access infrastructure. The Internet is readily
2658 available, evolving, and inherently fault tolerant. But it is also shared, containing numerous
2659 instances of malicious malware and malicious activities. Research into methods to deal with
2660 denial of service as well as to identify other critical issues will serve our understanding of the
2661 strengths and weaknesses as well as the cautions inherent in using the existing Internet for
2662 specific types of Smart Grid applications. In particular, this is a quality of service issue; how can
2663 enough bandwidth be guaranteed to a distributed embedded application such as a smart grid.
2664 What are the effects of delays on the physical control, for example, when physical delay or
2665 computation delay cannot be easily bounded, particularly in the face of changing network
2666 topologies and state.

¹⁰ For more on the privacy concerns related to NIALM, please see Volume 2, Section 5.3.1.

2667 **8.5.1.2 TCP/IP Security and Reliability Issues**

2668 Security/reliability issues surrounding the adoption of TCP/IP for Smart Grid networks is a
2669 related research topic separate from the subject of Internet use. Research into the adoption of
2670 Internet protocols for Smart Grid networks could include understanding the current state of
2671 security designs proposed for advanced networks. Features such as quality of service (QoS),
2672 mobility, multi-homing, broadcasting/multicasting, and other enhancements necessary for Smart
2673 Grid applications must be adequately secured and well managed if TCP/IP is to be adopted.

2674 **8.5.2 Advanced Networking**

2675 The prevalent notion is that Smart Grid communications will be primarily TCP/IP-based.
2676 Advanced networking technologies independent of the Internet protocols are being explored in
2677 multiple venues under the auspices of the National Science Foundation (NSF), Defense
2678 Advanced Research Projects Agency (DARPA), and others. Advanced networking development
2679 promises simpler approaches to networking infrastructures that solve by design some of the
2680 issues now affecting the Internet protocols. The work, although not complete, should be
2681 understood in the context of providing secure networks with fewer complexities that can be more
2682 easily managed and offer more predictable behavior.

2683 A wide variety of communication media and protocols are currently available and being used
2684 today—leased lines, microwave links, wireless, power line communication, etc. Two substation
2685 automation protocols and protocol suites, DNP3 and IEC 61850, are in use today. Any advanced
2686 networking technology that aims to provide a uniform abstraction for Smart Grid communication
2687 must also need support these various physical, data link, and transport layers for SCADA,
2688 substation automation, and peer-to-peer communication.

2689 **8.5.3 IPv6**

2690 It is very difficult to predict the consequences of large-scale deployments of networks. As the
2691 Smart Grid will likely be based on IPv6 in the future, and it is predicted that millions of devices
2692 will be added to the Smart Grid, it is not obvious that the backbone will function flawlessly.
2693 Research is needed to ensure that the IPv6-based network will be stable, reliable, and secure.

2694 In particular, these issues need more research—

- 2695 • Will current and future protocols scale to millions of devices?
- 2696 • Is current modeling, simulation, and emulation technology sufficient to model future
2697 networks using IPv6?
- 2698 • How is the accuracy of projected performance validated?
- 2699 • Will devices interoperate properly in multi-vendor environments?
- 2700 • Are the routing protocols suitable? Do new standards need to be developed?
- 2701 • Are there any security concerns? How will the network be partitioned?
- 2702 • Should NAT (Network Addresses Translation) be used?
- 2703 • Is a fundamentally new network architecture needed?

2704 **8.6 OTHER SECURITY ISSUES IN THE SMART GRID CONTEXT**

2705 If the Smart Grid is viewed as a cyber-physical system, then the cyber cross section of the Smart
2706 Grid will look like a large federated, distributed environment where information systems from
2707 various organizations with very different characteristics and purpose will need to interoperate.
2708 Among the various interacting entities are utilities, power generators, regulating authorities,
2709 researchers, and institutions—even large industrial consumers if the likes of Google are allowed
2710 to buy electricity directly; and with the advent of home-based renewable-energy and electric
2711 vehicles, residential customers may possibly be included. Effectively securing the interfaces
2712 between environments will become an increasing challenge as users seek to extend Smart Grid
2713 capabilities. Scalable and secure interorganizational interaction is a key security and
2714 management issue. Privacy policies involving data at rest, in transit, and in use will have to be
2715 enforced within and across these environments. Research is needed in the areas discussed in the
2716 following subsections.

2717 **8.6.1 Privacy and Access Control in Federated Systems**

2718 **8.6.1.1 Managed Separation of Business Entities**

2719 Research in the area of managed separation will focus on the network and systems architecture
2720 that enables effective communication among various business entities without inadvertent
2721 sharing/leaking of their trade secrets, business strategies, or operational data and activities. It is
2722 anticipated that fine-grained energy data and various other types of information will be collected
2723 (or will be available as a byproduct of interoperability) from businesses and residences to realize
2724 some of the advantages of Smart Grid technology. Research into managing the separation
2725 between business entities needs to address multiple areas:

- 2726 • Techniques to specify and enforce the appropriate sharing policies among entities with
2727 various cooperative, competing, and regulatory relationships are not well understood
2728 today. Work in this area would mitigate these risks and promote confidence among the
2729 participants that they are not being illegitimately monitored by their energy service
2730 provider, regulatory bodies, or competitors. Architectural solutions will be important for
2731 this objective, but there are also possibilities for improvements, for example, by using
2732 privacy-enhancing technologies based on cryptography or work on anonymity
2733 protections.
 - 2734 • As they collect more information, energy service providers will need to manage large
2735 amounts of privacy-sensitive data in an efficient and responsible manner. Research on
2736 privacy policy and new storage management techniques will help to diminish risk and
2737 enhance the business value of the data collected while respecting customer concerns and
2738 regulatory requirements. Such work would contribute to improved tracking of the
2739 purpose for which data was collected and enable greater consumer discretionary control.
 - 2740 • Verifiable enforcement of privacy policies regardless of the current state and location of
2741 data will provide implicit or explicit trust in the Smart Grid. Research is needed to
2742 develop better mechanisms for such enforcement.
- 2743

2744 **8.6.1.2 Authentication and Access Control in a Highly Dynamic Federated Environment**

2745 Collaborating autonomous systems in a federated environment must need to invoke operations
2746 on each other, other than accessing collected data (e.g., an ISO asking for more power from a
2747 plant). Access control (authentication and authorization), especially when the confederates enter
2748 into dynamic relationships such as daily buying/selling, long-term contracts, etc., is an issue that
2749 needs added research.

2750 **8.6.2 Auditing and Accountability**

2751 The concept of operation of the envisioned Smart Grid will require collecting audit data from
2752 various computer systems used in the Smart Grid. The existence of multiple autonomous
2753 federated entities makes auditing and accountability a complex problem: Who is responsible for
2754 auditing whom? How are the audit trails collected at various points to be linked? What
2755 mechanism can be used to mine the data thus collected? Such data will be needed to assess
2756 status, including evidence of intrusions and insider threats. Research is needed on a range of
2757 purposes for which audit data will be needed and on finding the best ways to assure
2758 accountability for operator action in the system. This will include research on forensic techniques
2759 to support tracing and prosecuting attackers and providing evidence to regulatory agencies
2760 without interrupting operations.

2761 **8.6.3 Infrastructure Interdependency Issues**

2762 Maintaining the resiliency and continuous availability of the power grid itself as a critical
2763 national infrastructure is an important mandate. There are also other such critical national
2764 infrastructure elements, such as telecommunications, oil and natural gas pipelines, water
2765 distribution systems, etc., with as strong a mandate for resiliency and continuous availability.
2766 However, the unique nature of the electrical grid is that it supplies key elements toward the well-
2767 being of these other critical infrastructure elements. And additionally, there are reverse
2768 dependencies emerging on Smart Grid being dependent on the continuous well-being of the
2769 telecommunications and digital computing infrastructure, as well as on the continuing flow of the
2770 raw materials to generate the power. These interdependencies are sometimes highly visible and
2771 obvious, but many remain hidden below the surface of the detailed review for each. There is little
2772 current understanding of the cascading effect outages and service interruptions might have,
2773 especially those of a malicious and judiciously placed nature with intent to cause maximum
2774 disruption and mass chaos. Research into interdependency issues would investigate and identify
2775 these dependencies and work on key concepts and plans toward mitigating the associated risks
2776 from the perspective of the Smart Grid. Such research should lead to techniques that show not
2777 only how communication failures could impact grid efficiency and reliability, how power
2778 failures could affect digital communications, and how a simultaneous combination of failures in
2779 each of the systems might impact the system as a whole, but should also apply a rigorous
2780 approach to identifying and highlighting these key interdependencies across all of these critical
2781 common infrastructure elements. The research would lead to developing and applying new
2782 system-of-systems concepts and design approaches toward mitigating the risks posed by these
2783 interdependencies on a nationwide scale.

2784 **8.6.4 Cross-Domain (Power/Electrical to Cyber/Digital) Security Event Detection,**
2785 **Analysis, and Response**

2786 The implication of failures or malicious activity in the cyber domain on the electrical domain, or
2787 vice versa, in the context of a large-scale and highly dynamic distributed cyber-physical system
2788 like the Smart Grid, is not well understood. Without further research, this is going to remain a
2789 dark area that carries a big risk for the operational reliability and resiliency of the power grid.

2790 As mentioned throughout various sections of this report, there is a need to better integrate the
2791 cyber and power system view. This is especially important in regard to detecting security events
2792 such as intrusions, unauthorized accesses, misconfigurations, etc., as well as anticipating cyber
2793 and power system impacts and forming a correct and systematic response on this basis. This is
2794 driven by the goal of using the modern IT and communications technologies in the Smart Grid to
2795 enhance the reliability of the power system while not offering a risk of degrading it. This will
2796 require research into new types of risk and security models as well as methods and technologies.

2797 There is need to further research and develop models, methods, and technologies in the following
2798 areas:

- 2799 • Unified risk models that have a correlated view of cyber and power system reliability
2800 impacts;
- 2801 • Response and containment models/strategies that use the above unified risk models;
- 2802 • Security and reliability event detection models that use power and IT and communication
2803 system factors in a cross-correlated manner and can operate on an autonomous, highly
2804 scaled, and distributed basis (e.g., security event detection in mesh networks with
2805 resource-constrained devices, distributed and autonomous systems with periodic
2806 connectivity, or legacy component systems with closed protocols). New security
2807 models need to be developed to overcome the limitations of purely cryptographic
2808 solutions. These models must embrace power, IT, and communications in a unified
2809 fashion;
- 2810 • Unified intrusion detection/prevention systems that use the models/methods above and
2811 have a deep contextual understanding of the Smart Grid and its various power system and
2812 operations interdependencies;
- 2813 • Very large-scale wide area security event detection and response systems for the Smart
2814 Grid that can interoperate and securely share event data across organizational boundaries
2815 and allow for intelligent, systematic, and coordinated responses on a real-time or near
2816 real-time basis;
- 2817 • Development of distributed IED autonomous security agents with multi-master Security
2818 Information and Event Management (SIEM) reporting for wide area situational
2819 awareness;
- 2820 • Development of distributed IED autonomous security agents with continuous event and
2821 state monitoring and archiving in the event of islanding, security state restoration and
2822 forensics when isolated from master SIEM systems;
- 2823 • Advanced Smart Grid integrated security and reliability analytics that provide for event
2824 and impact prediction, and continual infrastructure resiliency improvement; and

- 2825 • Advanced security visual analytics for multidimensional, temporal, and geo-spatial views
2826 of real-time security data capable of digesting structured and unstructured data analysis
2827 for system and security operation control center operators.

2828 To develop and refine the modeling and systems necessary for much of the proposed research,
2829 there would also be a need for developing new simulation capabilities for the distribution grid
2830 that incorporate communications with devices/models for distribution control, distributed
2831 generation, storage, PEV, etc., to provide a representative environment for evaluating the impact
2832 of various events. To provide a realistic assessment of impact, the simulation capabilities should
2833 be similar in fidelity to the transmission grid simulation capabilities that currently exist.
2834 However, both the distribution and transmission grid system simulations need to be further
2835 developed to integrate cyber elements and evaluate their possible cross-impacts on each other.

2836 **8.6.5 Covert network channels in the Smart Grid: Creation, Characterization, Detection**
2837 **and Elimination**

2838 The idea of covert channels was introduced by Lampson in 1973 as an attack concept that allows
2839 for secret transfer of information over unauthorized channels. These channels demonstrate the
2840 notion that strong security models and encryption/authentication techniques are not sufficient for
2841 protection of information and systems. Earlier research on covert channels focused on multilevel,
2842 secure systems but more recently a greater emphasis has been placed on "covert network
2843 channels" that involve network channels and can exist in discretionary access control systems
2844 and Internet-like distributed networks. Given that many Smart Grid networks are being designed
2845 with Internet principles and technologies in mind, the study of covert network channels for the
2846 Smart Grid becomes an interesting research problem. Like the more general covert channels,
2847 covert network channels are typically classified into storage and timing channels. Storage
2848 channels involve the direct/indirect writing of object values by the sender and the direct/indirect
2849 reading of the object values by the receiver. Timing channels involve the sender signaling
2850 information by modulating the use of resources (e.g., CPU usage) over time such that the
2851 receiver can observe it and decode the information.

2852 The concern over covert network channels stems from the threat of miscreants using such
2853 channels for communication of sensitive information and coordination of attacks. Adversaries
2854 will first compromise computer systems in the target organization and then establish covert
2855 network channels. Typically, such channels are bandwidth-constrained as they aim to remain
2856 undetected. Sensitive information that may be sent over such channels include Critical Energy
2857 Infrastructure Information (CEII), FERC 889 involving the leakage of operational information to
2858 power marketing entities, and cryptographic keying material that protects information and
2859 systems. In addition, information exchange for coordination of attacks such as management and
2860 coordination of botnets, and spreading worms and viruses are also important concerns.

2861 For example, covert network channels have been created using IP communication systems by a
2862 variety of means including the use of unused header bits, modulating packet lengths, and
2863 modifying packets rates/timings. Similarly, such channels have been shown to be possible with
2864 routing protocols, wireless LAN technologies, and HTTP and DNS protocols. For the Smart
2865 Grid, an interesting research challenge is to identify new types of covert network channels that
2866 may be created. For example, given that the Smart Grid involves an extensive cyber-physical
2867 infrastructure, perhaps the physical infrastructure can be leveraged to design covert network
2868 channels. Additional challenges include identification of other covert network channels that can

2869 be established on Smart Grid networks, for example, using relevant weaknesses in Smart Grid
2870 protocols. For all created channels, it is important to characterize the channels. This includes
2871 estimating channel capacity and noise ratios.

2872 Covert channels can be detected at the design/specification level and also while they are being
2873 exploited. A variety of formal methods-based techniques have been developed in the past. An
2874 example is those based on information flow analysis. For runtime identification, several
2875 techniques specific to the type of covert network channel have been developed. Research
2876 challenges include identification of covert network channels for Smart Grid systems both at the
2877 design level and while they may be exploited. Once identified, the next challenge lies in
2878 eliminating them, limiting their capacity, and being able to observe them for potential
2879 exploitation. Means for doing so include the use of host and network security measures, and
2880 traffic normalization at hosts and network endpoints, such as firewalls or proxies. Again,
2881 research challenges include developing means for eliminating covert network channels, and in a
2882 case where that is not feasible, the objective is to limit their capacity and be able to monitor their
2883 use. Potential avenues of research include analyzing and modifying garbage collection processes
2884 in Smart Grid systems, and developing signature and anomaly-based detection techniques.

2885 Covert channels are not limited to network observations. The power system itself, in a cyber-
2886 physical environment, provides covert channel information. Power line changes resulting from
2887 cyber actions on smart devices divulge those cyber actions.

2888 **8.6.6 Denial of Service Resiliency**

2889 **8.6.6.1 Overview**

2890 Smart Grid communications are progressing toward utilizing IP-based transport protocols for
2891 energy utility information and operational services. As IP-based nodes propagate, more
2892 opportunities for exploitation by miscreants are evolving. If a network component can be probed
2893 and profiled as part of the Smart Grid or other critical infrastructures, it is most likely to be
2894 targeted for some form of intrusion by miscreants. This is especially relevant with the growing
2895 use of wireless IP communications.

2896 **8.6.6.2 DoS/DDoS Attacks**

2897 Denial of Service and Distributed Denial of Service (DoS/DDoS) attacks have become an
2898 effective tool to take advantage of vulnerabilities. The attack objective is to take actions that
2899 deprive authorized individuals access to a system, its resources, information stored thereon, or
2900 the network to which it is connected.

2901 A simple DoS attack attempts to consume resources in a specific application, operating system,
2902 or specific protocols or services, or a particular vendor's implementation of any of these targets
2903 to deny access by legitimate users. It may also be used in conjunction with other actions (attacks)
2904 to gain unauthorized access to a system, resources, information, or network.

2905 The DDoS attack seeks to deplete resource capacity, such as bandwidth or processing power, in
2906 order to deny access to authorized users and can be levied against the infrastructure layer or the
2907 application layer. This technique utilizes a network of attack agents (a "botnet" comprised of
2908 systems that have had attack software installed surreptitiously) to amass a large, simultaneous

2909 assault of messages on the target. As with the DoS attack, DDoS may be combined with other
2910 techniques for malicious purposes.

2911 IP-based networks are vulnerable to other attacks due to deficiencies of underlying protocols and
2912 applications. A man-in-the-middle, session-based hijack, or other technique may accompany the
2913 DoS/DDoS attack to inflict further damage on the target. Wireless networks in the AMI/HAN
2914 environment can be difficult to secure and are of particular concern as the object of an attack or
2915 an entry point to the upstream network and systems.

2916 **8.6.6.3 Research and Development Requirements**

2917 The SGIP CSWG R&D subgroup desires to highlight and seek further research and development
2918 support in order to improve DoS/DDoS resiliency. We have identified the following areas of
2919 work as offering potential solutions worthy of further pursuit by Smart Grid stakeholders:

2920 1. **Network architectures for survivability:** The Smart Grid networks and the public
2921 Internet will have several interface points which might be the target of DoS/DDoS attacks
2922 originating from the public Internet. A survivable Smart Grid network will minimize the
2923 disruption to Smart Grid communications, even when publicly addressable interfaces are
2924 subject to DDoS attacks;

2925 2. **Policy-based routing and capabilities:** Policy-based routing is a fundamental redesign
2926 of routing with the goal of allowing communications if, and only if, all participants
2927 (source, receiver, and intermediaries) approve. A particular policy of interest for
2928 defending against DDoS attacks is the use of Capabilities. In this framework, senders
2929 must obtain explicit authorization (a capability) from the receiver before they are allowed
2930 to send significant amounts of traffic (enforced by the routing infrastructure). Smart Grid
2931 networks provide a good opportunity to design from the ground up a new routing
2932 infrastructure supporting capabilities;

2933 3. **Stateless dynamic packet filtering:** Filtering and rate-limiting are basic defenses against
2934 DDoS attacks. We require further research in stateless packet filtering techniques to
2935 significantly reduce packet-processing overhead.

2936 An example of this is “Identity-Based Privacy-Protected Access Control Filter” (IPACF)
2937 which is advertised as having the “capability to resist massive denial of service attacks.”
2938 IPACF shows promise for using “stateless, anonymous and dynamic” packet filtering
2939 techniques without IP/MAC address, authentication header (AH) and cookie
2940 authentication dependencies, especially for resource-constrained devices (RCDs).

2941 When compared to stateful filtering methods, IPACF may significantly reduce packet
2942 processing overhead and latencies even though it is dynamically applied to each packet.
2943 IPACF describes the ability to utilize discarded packets for real-time intrusion detection
2944 (ID) and forensics without false positives.

2945 Initial modeling reveals that embedded stateless packet filtering techniques may
2946 significantly mitigate DoS/DDoS and intrusion and could be evolved to defend man-in-
2947 the-middle attacks, while offering considerable device implementation options and
2948 economies of scale; and

2949 4. **Lightweight authentication and authorization:** There is a distinct need for an
2950 embedded-level, lightweight, secure, and efficient authentication and authorization (AA)

2951 protocol to mitigate intrusion and DDoS attacks targeting resource-intense AA
2952 mechanisms. See Item 3 above.

2953 5. **Power system DDoS:** The smart grid elements, themselves, can initiate denial of service
2954 by advertising energy that they do not possess or creating demand that does not exist
2955 (fake supply or fake demand attacks). . This can deplete stored energy or cause shortages
2956 in reactive power during periods of high demand and can have the potential to destabilize
2957 the grid.

2958 **8.6.7 Cloud Security**

2959 With the advent of cloud computing in the Smart Grid, special attention should be given to the
2960 use of cloud computing resources and the implications of leveraging those resources. There are
2961 several organizations that are focusing on security and appropriate use of cloud computing
2962 resources, including the Cloud Security Alliance. They have produced a document that addresses
2963 security areas for cloud computing that provides valuable guidelines to security in this
2964 environment. Work has also been done by NIST's cloud computing group that provides some
2965 guidelines for cloud computing use in government agencies.

2966 As with any shared resource that will host potentially sensitive information, security mechanisms
2967 must be deployed that provide the appropriate protection and auditing capabilities throughout the
2968 cloud. Cloud computing must be evaluated with consideration of the unique constraints and
2969 consequences of control systems in the context of the Smart Grid. Impact of cloud provider
2970 engagement must also be considered in terms of liabilities for data existing in the cloud, in what
2971 is likely to be a multi-tenancy environment.

2972 Data security issues must be addressed such as data ownership, data protection both in and out of
2973 the cloud for storage and transit, access control to the data and the cloud, and authorization
2974 considerations for trust and permissions. Trust models must be put in place to provide these
2975 guarantees in a manner that is verifiable and compliant with emerging regulations like NERC
2976 CIPs, FERC 889, user data privacy concerns, and other emerging compliance regulations. These
2977 types of regulations may have corollaries in industries like the health sector that could be
2978 considered, but differ enough that there are unique concerns.

2979 WAN security and optimization issues must also be addressed depending on the data access
2980 patterns and flow of information in the cloud. This could include new work in encryption, key
2981 management, data storage, and availability model views. For instance, securely moving
2982 synchrophasor data from end nodes into the cloud on a global basis could be overly resource
2983 intensive. This might make real-time use infeasible with current cloud computing technology
2984 without further research in this area. Current distributed file system approaches may not be
2985 appropriately optimized to operate in a secure WAN environment, favoring network-expensive
2986 replication in a LAN environment as a trade-off for speed.

2987 **8.6.8 Security Design & Verification Tools (SD&VT)**

2988 Complexity breeds security risks. This is most evident with the Smart Grid, as it is a collection of
2989 many complex, interconnected systems and networks that represent a fusion of IT,
2990 telecommunications, and power system domains. Each of these domains represents distinct
2991 forms of technology and operations that have unique interdependencies on each other and can

2992 indeed lead to elements of the cyber system (i.e., IT and communications) impacting the
2993 reliability of elements of the power system and vice-versa.

2994 Correctly designing security for each of the domains is primarily done from the perspective of
2995 only the power or cyber domain. For example, designing certain security controls (without an
2996 adequate understanding of an overall power system context) to prevent excessive failed
2997 authentication attempts by lockout on a communication/control device might in fact create a
2998 denial of service condition that is more likely to degrade the reliability of the broader system
2999 than mitigate the original security risk that one was trying to address. System-wide security
3000 design and implementation is not commonly done using formal methods that can be verified, nor
3001 can it give any deterministic analysis of expected performance or behavior for given system
3002 states, faults, or threat events.

3003 Research and development should be conducted into SD&VT that can—

- 3004 a. Formally model Smart Grid cyber and power systems, their interactions, and their
3005 underlying components using a formal language. Candidates for examination and further
3006 adaptation can include: SysML, Formal ontologies and knowledge representation based
3007 on semantic Web technologies such as OWL, or other novel forms. The language should
3008 allow one to communicate certain assertions about the expected function of a
3009 device/system and its security controls and risks, as well as the relationship between
3010 components, systems, and system communication. Most importantly, the model must
3011 provide a basis to represent multiple concurrent and independently interacting complex
3012 processes with distributed system states;
- 3013 b. Provide automatic, intelligent methods of verification that discover reliability and
3014 security issues in component and system states for the Smart Grid, in a formal design
3015 model (as represented using the methods in (a.)) using any number of machine learning or
3016 knowledge/logic inference techniques; and
- 3017 c. Simulate any number of scenarios based on the intelligent model built using (a.) and (b.),
3018 and provide predictive analytics that can optimize a security design that minimizes risks
3019 and costs, as well as maximizing security and reliability in the power and cyber domain.

3020 **8.6.9 Distributed versus Centralized Security**

3021 Several models for designing intelligent and autonomous actions have been advanced for the
3022 Smart Grid, particularly in automated distribution management. Several models have also been
3023 deployed in the advanced metering space, where, for example, there is ongoing debate regarding
3024 the functions and processing which should be carried out by the meter, versus centralized
3025 systems (such as Meter Data Management or Load Control applications in the Control Center).
3026 Some approaches offer embedded security controls, while some externalize security and some
3027 offer combinations of both approaches. In the larger context of advanced distribution automation,
3028 there is a similar debate regarding how much “intelligence” should be deployed within IEDs,
3029 distributed generation endpoints, etc., versus reliance on centralized systems.

3030 Also, Wide Area Situational Awareness (WASA) systems and actors are distributed by nature,
3031 yet most security mechanisms in place today are centralized. What is an appropriate security
3032 mechanism to place in a distributed environment that will not compromise an existing security
3033 framework, yet allow third-party WASA systems and actor’s visibility into security intelligence,

3034 as well as allow appropriate functional capability to act and respond to distributed security
3035 events?

3036 We propose advanced security research be conducted to determine an underlying security model
3037 to support these various approaches to distributed versus centralized security intelligence and
3038 functionality in the grid. Some factors to consider include the following:

- 3039 • Communication with centralized security mechanisms may be interrupted. Research
3040 should be conducted into hybrid approaches and the appropriate layering of security
3041 controls between centralized and distributed systems. For example, centralized security
3042 mechanisms may be supplemented with local “break glass” security mechanisms for
3043 many devices, but does this “local” control support a distributed model?
- 3044 • Externalized security mechanisms, such as in some control system protocol
3045 implementations (e.g., ANSI C12.22), may be desirable because they can be scaled and
3046 upgraded independently in response to evolving threats and technology changes, possibly
3047 without retrofitting or upgrading (perhaps millions of) devices deployed in the field. On
3048 the other hand, some mechanisms should be deployed locally, such as bootstrap trusted
3049 code verification modules for firmware, logging, etc. Research should be conducted in
3050 best practices to determine the appropriate model for deployment.
- 3051 • Rapid changes of cryptographic keys and authentication credentials may be needed to
3052 contain security incidents or provide ongoing assurance, and centralized security systems
3053 may be needed. Would a distributed or centralized model be more efficient and secure?
- 3054 • Functionality of some components (e.g., breakers, IEDs, relays, etc.) and
3055 communications functions should not fail due to failure of a security mechanism. Is a
3056 distributed model appropriate for WASA?
- 3057 • Integration of security mechanisms between security domains is needed (for example,
3058 between logical and physical security mechanisms of remote sensors). How does a
3059 distributed vs. centralized model effect the integration?
- 3060 • Edge devices such as distributed generation controllers and substation gateways need to
3061 be capable of autonomous action (e.g., self-healing), but these actions should be governed
3062 by business rules and under certain circumstances data from the devices should not be
3063 trusted by decision support systems and systems that have more than local control of the
3064 grid. Does a distributed model manage edge devices more efficiently and securely than a
3065 centralized model?
- 3066 • A trust model is needed to govern autonomous actions, especially by systems outside the
3067 physical control of the utility. Will there be a centralized trust model or will the industry
3068 evolve to a distributed trust model allowing numerous Smart Grid actors to interact
3069 trustfully in regards to security interactions?
- 3070 • Do distributed or centralized trust models force over-reliance by control systems support
3071 groups on IT groups?
- 3072 • What are the actions to be taken during a security event; are they centralized or
3073 distributed?

3074 While it is not be clear which security functions should be centralized or decentralized for a
3075 particular implementation, research into coherent reference models and taxonomies for layering
3076 these controls following best practice should be conducted. The model should contain a standard
3077 approach by which Smart Grid actors can make better security architecture decisions based on
3078 risks to their environment and efficiencies of security operations.

3079 **8.6.10 System Segmentation and Virtualization**

3080 The first principles of cyber security are isolation and defense-in-depth. The objective of this
3081 research is to develop methods to protect network end-points through Intense System
3082 Segmentation. The research should seek to create a platform that implements the characteristics
3083 of time-tested and recognized security principles. These principles include isolation, a minimal
3084 trusted computing base, high usability and user transparency, a limited privilege capability that
3085 provides for user, process, and application class of service definitions, and a default-deny rules
3086 engine enforcing such privileges.

3087 The requirement for continuous availability of Utility Grid operations necessitates a high degree
3088 of reliability within and across domains. Many domain end-points, such as legacy substation
3089 equipment, rely on outdated operating systems with little or no encryption capabilities, posing
3090 numerous challenges to the overall security of the Smart Grid. By enclosing an Intense System
3091 Segmentation framework around the existing computer architecture of these localized end-
3092 points, the legacy infrastructure should gain a layer of redundancy and security. Intense System
3093 Segmentation within a single Virtual Machine (VM) should provide granular isolation to reduce
3094 the attack surface to a single file and/or single application, and reduce the ability of threats to
3095 virally propagate. End-point protection must also be customizable to address the specific needs
3096 of subsectors within individual Energy Sector Domains.

3097 Traditional virtualization techniques that use sandboxing have known, exploitable
3098 vulnerabilities. This is largely the result of the communication that traditional VMs require in
3099 order to perform sharing functions between applications and administrative requirements.
3100 Sandboxing also relies on binary decisions for processes and communication that might
3101 compromise security. Intense System Segmentation should allow communication between
3102 isolated environments to occur while eliminating any execution of code outside of an isolated
3103 environment. An Intense System Segmentation platform may use some of the tools of
3104 virtualization, such as a sealed hypervisor to provide protection of end-point resources, and
3105 sealed VMs to perform computing in intense isolation. Hypervisors are designed to streamline
3106 communication between a wide range of applications and processes, and utilize APIs and other
3107 communication entry points. A sealed hypervisor should block these communication entry
3108 points, for both the hypervisor and an attestable kernel.

3109 Maintaining the resiliency and continuous availability of the power grid should be one of the
3110 primary goals in creating a system segmentation platform. As this platform assumes that end-
3111 points will be penetrated, secure recovery, containment, and resiliency should be a focus of
3112 continued research. The inherent redundancy of hypervisor-driven segmentation can be utilized
3113 to enclose legacy systems and should allow customizable interoperability between the DHS-
3114 defined critical infrastructure sectors. An open platform that uses a secure computing
3115 architecture and leverages the tools of virtualization will enhance the resiliency of existing
3116 Energy Sector critical infrastructure. The use of virtualization has also been recognized as
3117 building block to implement resiliency through agility (a “moving target” paradigm). This can be

3118 used to increase uncertainty and cost to attackers. Thus this research should help to leverage
3119 “moving target” paradigm in Smart Grid systems as well as improving security of Smart Grid
3120 legacy systems.

3121 **8.6.11 Vulnerability Research**

3122 Vulnerabilities may be caused by many things in computer devices. Poor coding is the primary
3123 cause of vulnerabilities in computer systems today, but physical attacks have much higher value
3124 in Smart Grid devices than in standard computing environments. Both design and
3125 implementation vulnerabilities represent varying and potentially great risks to the power grid.
3126 While future code revisions and hardware versions may introduce new vulnerabilities, many
3127 vulnerabilities may exist in the current systems that require significant time to identify and
3128 address. For many years, SCADA systems have been quarantined from security scans for fear of
3129 causing outages. While care and prudence should be taken with critical systems, the fragility of
3130 these systems represents a great existing risk to the grid. Newer Smart Grid systems such as
3131 advanced metering infrastructure, hybrid/electric vehicles and supporting infrastructure, and
3132 demand response all represent new unknowns. A few significant projects have undertaken
3133 security research on some of these devices, and positive results have resulted but more research
3134 is necessary. Security research grants are key to ensuring greater scrutiny of the existing systems
3135 to find vulnerabilities that may currently exist in Smart Grid equipment.

3136 **8.6.12 Vulnerability Research Tools**

3137 Smart Grid networks represent a great deal of proprietary, obtuse systems and protocols. Before
3138 security can be reasonably well tested, tools must be created to maximize the value of security
3139 research. Several freely available tools have already been in active development but lack
3140 resources. Other tools are important but nonexistent.

3141 Examples of existing security research tools include:

- 3142 • GoodFET—Hardware analysis tool allowing debugging of numerous platforms/chipsets,
3143 largely focused on the predictability of power-glitching to bypass hardware security
3144 mechanisms; <http://goodfet.sourceforge.net/>
- 3145 • KillerBee—ZigBee® analysis tool allowing for capture and analysis of ZigBee® networks
3146 and interaction with devices.

3147 Examples of security research tools yet to be started:

- 3148 • Devices to easily interact with, capture, and analyze traffic of metering networks for
3149 different vendors. Currently, the best toolset available is the software-defined radio
3150 named USRP2 from Ettus Research, costing roughly \$2k. This toolset allows for RF
3151 analysis and indeed can capture data bits. However, the ideal toolset would allow an
3152 analyst's computer to interface to the metering networks and provide an appropriate
3153 network stack in a popular operating system such as Linux. The tools would allow the
3154 customers (mostly IOU's due to funding) to perform their own security research against
3155 the platforms, and allow them to validate their own security;
- 3156 • Open-source Protocol analysis tools, such as the protocol parsers included in the open-
3157 source tool Wireshark. Protocols like IEC61850, IEC61968/ANSI C12.*, proprietary
3158 AMI protocols, DNP3, Modbus, and other popular power grid protocols being included

3159 in the Smart Grid should be freely available for analysis by asset-owners and researchers;
3160 and

- 3161 • Firmware analysis tools that can be configured to understand address/IO mapping and
3162 input vectors, and can identify potential vulnerabilities for a given platform.

3163 **8.6.13 Data Provenance**

3164 We cannot assume that the Smart Grid will never be compromised. Once we assume that there
3165 are insiders who have access, operational data can no longer be trusted. In addition, while
3166 traditional security-related protocols reject data if the security fails, we cannot afford to ignore
3167 operational data because the data is suspect.

3168 Therefore, we need methods to deal with such data while maintaining the operational integrity
3169 and state of many systems. Some of the issues include:

- 3170 • Measuring the quality of the data from a security perspective. This may include both
3171 subjective and objective viewpoints, and may have to deal with uncertainty about the
3172 data.
- 3173 • How do we make operational decisions based on data that may have questionable
3174 attributes of confidentiality, integrity, authenticity, non-repudiation, and timeliness?
- 3175 • How do organizations coordinate their beliefs with other organizations? What happens if
3176 the other organizations are suffering from a significant security breach? How should one
3177 organization react with data of uncertain trustworthiness?

3178 **8.6.14 Security and Usability**

3179 One of the issues with the implementation of security is the usability of security, or the ease of
3180 use and impact on convenience. Some organizations weaken their security for various reasons
3181 (e.g., operational cost, profit, effort, lack of understanding). To encourage users to deploy strong
3182 security, certain issues must be overcome. These include:

- 3183 • Security must be self-configuring. That is, the systems should be able to configure
3184 themselves to maximize security without requiring expert knowledge of security.
- 3185 • Security options should be simple and understandable by users who lack a background in
3186 security. Concepts like certificates and keys are not well understood by end users. These
3187 details should be hidden.
- 3188 • The relationship between a security policy, the protection the policy provides, and the
3189 security configuration should be clear. If a system is “misconfigured” in a way that
3190 reduces the protection, the risk should be clear to the user.
- 3191 • Security should be reconfigured. In other words, if a policy is changed (for instance,
3192 stronger security is enabled), the systems should adapt to meet the new requirements. It
3193 should not be necessary to physically visit devices to reconfigure them. However, if
3194 policy changes, some devices might be unable to change, and end up being isolated from
3195 the new configuration. How can the user minimize the disruption?
- 3196 • Part of usability is maintainability. There needs to be ways to upgrade security without
3197 replacing equipment. Firmware upgrades are often proprietary, vendor-specific, and have

3198 uncertain security. How can a vendor best plan their migration strategy between security
3199 revisions and major policy changes?

3200 Usability of security technologies needs to improve to address these issues.

3201 **8.6.15 Cyber Security Issues for Electric Vehicles**

3202 PEVs have a similar entry point to the electric grid as the smart meters. Thus, they are associated
3203 with largely the same security and privacy issues. When PEVs connect to the grid to charge their
3204 batteries, it is necessary to communicate across a digital network to interface with a payment and
3205 settlement system. Assuming that proper standards are adopted, these charging solutions will
3206 have the same issues as payment and settlement systems for other products. Appropriate physical
3207 security measures and tamper-evident mechanisms must be developed to prevent or detect the
3208 insertion of “cloning” devices to capture customer information and electric use debit and credit
3209 information. One may expect that miscreants will develop means to clone legitimate PEV
3210 interfaces for criminal activity.

3211 It has been reported that a terminated employee from a car dealership logged into the company’s
3212 Web-based system and was able to remotely wreak havoc on more than 100 vehicles. The
3213 dealership’s system was able to disable the starter system and trigger incessant horn honking for
3214 customers that have fallen behind on car payments as an alternative to repossessing the vehicle.
3215 It is necessary to develop mechanisms that make sure car buyers are properly informed and fully
3216 protected.

3217 Like other areas that depend on a supply chain, PEVs have similar issues. Thus, it is necessary to
3218 make sure that car repair shops will not be able to install illegal devices at time of car
3219 maintenance.

3220 Utilities and private/public charging stations may also be subject to law enforcement search
3221 warrants and subpoenas in regards to PEV usage. A PEV may be stolen and used in the act of a
3222 crime. Law enforcement may issue an “alert” to control areas to determine if the suspected PEV
3223 is “connected” to the grid and would want to know where and when. Research may also be
3224 requested by law enforcement to enable a utility to be able to “disable” a PEV in order to
3225 preserve evidence and apprehend the criminals. Authentication and non-repudiation are key in
3226 this process, otherwise a thief can use the same processes to steal a car (or disable cars as in the
3227 example, above).

3228 **8.6.16 Detecting Anomalous Behavior Using Modeling**

3229 Various sensors in the power/electrical domain already collect a wide array of data from the grid.
3230 In the Smart Grid, there will also be a number of sensors in the cyber domain that will provide
3231 data about the computing elements as well as about the electrical elements. In addition to
3232 naturally occurring noise, some of the sensor data may report effects of malicious cyber activity
3233 and “misinformation” fed by an adversary.

3234 Reliable operation of the Smart Grid depends on timely and accurate detection of outliers and
3235 anomalous events. Power grid operations will need sophisticated outlier detection techniques that
3236 enable the collection of high integrity data in the presence of errors in data collection.

3237 Research in this area will explore developing normative models of steady state operation of the
3238 grid and probabilistic models of faulty operation of sensors. Smart Grid operators can be

3239 misguided by intruders who alter readings systematically, possibly with full knowledge of outlier
3240 detection strategies being used. Ways of detecting and coping with errors and faults in the power
3241 grid need to be reviewed and studied in a model that includes such systematic malicious
3242 manipulation. Research should reveal the limits of existing techniques and provide better
3243 understanding of assumptions and new strategies to complement or replace existing ones.

3244 Some example areas where modeling research could lead to development of new sensors
3245 include:

- 3246 • Connection/disconnection information reported by meters may identify an unauthorized
3247 disconnect, which in the context of appropriate domain knowledge can be used to
3248 determine root cause. This research would develop methods to determine when the
3249 number of unauthorized disconnects should be addressed by additional remediation
3250 actions to protect the overall AMI communications infrastructure, as well as other
3251 distribution operations (DR events, etc.).
- 3252 • Information about meters running backwards could generally be used for theft detection
3253 (for those customers not subscribed to net metering). This research would identify
3254 thresholds where too many unauthorized occurrences would initiate contingency
3255 operations to protect the distribution grid.

3256 Related prior work includes fraud detection algorithms and models that are being used in the
3257 credit card transactions.

3258 **CHAPTER NINE**
3259 **OVERVIEW OF THE STANDARDS REVIEW**

3260 **9.1 OBJECTIVE**

3261 The objective of the standards review is to ensure that all standards applicable to the Smart Grid
3262 adequately address the cyber security requirements included in this report. If the standards do not
3263 have adequate coverage, this review will identify those where changes may need to be made or
3264 where other standards may need to be applied to provide sufficient coverage in that area. If the
3265 standard passes the CSWG cybersecurity assessment, then it may be included in the SGIP
3266 Catalog of Standards.

3267 The CSWG works with the SGIP and the standards bodies to identify the standards for review
3268 and to gain appropriate access to the standards. This is an ongoing effort as there are many
3269 standards that apply and must be assessed. To undertake the process, the CSWG established a
3270 standards subgroup to perform the assessments. This CSWG Standards Subgroup developed a
3271 review process and an assessment template for performing the assessments.

3272 **9.2 REVIEW PROCESS**

3273 **9.2.1 Overview**

3274 The NISTIR 7628 contains a catalog of cybersecurity requirements that can be used as a
3275 checklist for determining what types of cybersecurity requirements are applicable to specific
3276 Smart Grid interactions and cybersecurity requirement families that should be considered in the
3277 review document.

3278 **9.2.2 CSWG Review Process**

3279 Before the CSWG compares the standards document against the NISTIR 7628, the CSWG
3280 reviews the scope of the standard and will document additional assumptions as to whether
3281 cybersecurity should be part of the standards document. The cybersecurity content can take the
3282 form of detailed cybersecurity technologies, specific cybersecurity requirements to meet specific
3283 cybersecurity goals, general cybersecurity best practices, or high-level policy statements. This
3284 cybersecurity content can also cover reliability/availability requirements, confidentiality
3285 requirements, data integrity requirements, and privacy issues.

3286 Some of these requirements are general, such as having policies and procedures for specific
3287 types of interactions, for example “SG.CM-1: Configuration Management Policy and
3288 Procedures”. Some are more specific, such as “SG.SC-12: Use of Validated Cryptography”. In
3289 using this catalog as a checklist, it is clear that most interactions only need or reflect a small set
3290 of these requirements, such as:

3291 "Access to the mapping database for updates must use authentication - SG.CM-3: Configuration
3292 Change Control”

3293 “Cryptographic algorithms shall be current, publicly vetted, and government approved - SG.SC-
3294 11: Cryptographic Key Establishment and Management”.

3295 **9.2.3 Step 1: Reviewing the Document Scope**

3296 When the CSWG receives a request to review a document, the CSWG reviews the scope and
3297 purpose of the requested review document, and notes any assumptions as to the domain and type
3298 of document. If the document should or does contain cybersecurity requirements, then the
3299 document is assessed for cybersecurity completeness and correctness. The CSWG Standards
3300 Subteam usually requests an expert on the document to participate and answer questions on the
3301 context or purpose of cybersecurity items.

3302 **9.2.4 Step 2: NISTIR 7628 High Level Cybersecurity Requirements**

3303 After assessing the overall scope of the document, the CSWG starts a detailed review of the
3304 cybersecurity contents of the document, assessing them against the High Level Security
3305 Requirements from the NISTIR 7628 volume 1. During this assessment, some requirements and
3306 interactions may not have direct correlations with the NISTIR 7628 high level cybersecurity
3307 requirements. This will lead to a potential recommendation of

3308 The NISTIR 7628 high level cybersecurity requirements may need to be updated to include
3309 them, or the requirement may be so specific that the requirements is not needed in the NISTIR
3310 7628.

3311 If there is a NISTIR 7628 cybersecurity family that is not referenced within the review document
3312 and the cybersecurity family can apply to the review document, then a gap is documented by the
3313 CSWG and a potential recommendation is documented for the review document.

3314 **9.2.5 Step 3: Recommendations on Standard**

3315 During the assessment, cybersecurity concerns or issues are noted and often discussed with the
3316 owners of the document. Recommendations for improvement on cybersecurity issues are
3317 provided so that the document owners may choose to update the document or underake
3318 additional documents to address these CSWG recommendations.

3319 If the standard meets all major requirements, the CSWG recommends inclusion in the SGIP
3320 Catalog of Standards. If some requirements are not met, the CSWG may recommend conditional
3321 approval pending the correction or mitigation of the cybersecurity concern.

3322 **9.3 NIST CSWG STANDARDS ASSESSMENT CONCEPTS**

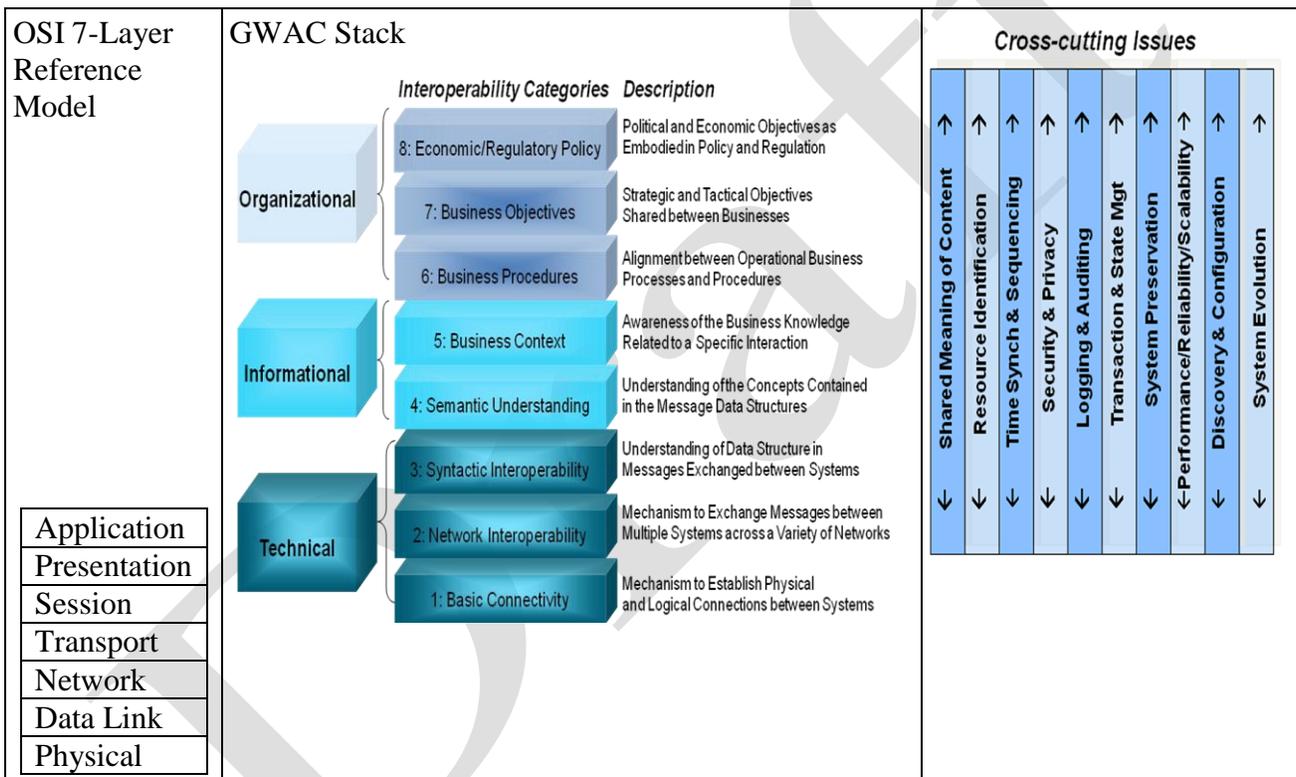
3323 The following subsections provide the background and concepts used in assessing standards:

3324 **9.3.1 Correlation of Cybersecurity with Information Exchange Standards**

3325 Correlating cybersecurity with specific information exchange standards, including functional
3326 requirements standards, object modeling standards, and communication standards, is very
3327 complex. There is rarely a one-to-one correlation, with more often a one-to-many or many-to-
3328 one correspondence.

3329 First, communication standards for the Smart Grid are designed to meet many different
3330 requirements at many different “layers” in the reference model. Two commonly used reference
3331 models are the International Organization for Standardization (ISO) / Open Systems

3332 Interconnection model (OSI) 7-layer reference model¹¹ and the GridWise Architecture Council
 3333 (GWAC) Stack¹² (see **Error! Reference source not found.**), where the OSI 7-layer model maps
 3334 to the Technical levels of the GWAC Stack. Some standards address the lower layers of the
 3335 reference models, such as wireless media, fiber optic cables, and power line carrier. Others
 3336 address the “transport” layers for getting messages from one location to another. Still others
 3337 cover the “application” layers, the semantic structures of the information as it is transmitted
 3338 between software applications. In addition, there are communication standards that are strictly
 3339 abstract models of information – the relationships of pieces of information with each other.
 3340 Cybersecurity is a cross-cutting issue and should be reflected in requirements at all levels:
 3341 cybersecurity policies and procedures mainly cover the GWAC Stack Organizational and
 3342 Informational levels, while cybersecurity technologies generally address those requirements at
 3343 the Technical level.



3344 **Figure 9-1 ISO/OSI 7-Layer Reference Model and GWAC Stack Reference Model**

3345 Second, regardless of what communications standards are used, cybersecurity must address all
 3346 layers – end-to-end – from the source of the data to the ultimate destination of the data. In
 3347 addition, cybersecurity must address those aspects outside of the communications system in the
 3348 upper GWAC Stack layers that may be functional requirements or may rely on procedures rather
 3349 than technologies, such as authenticating the users and software applications, and screening

¹¹ ISO 7498-1:1994, *Information technology-Open Systems Interconnection-Basic Reference Model: The Basic Model*.

¹² The GWAC Stack is available at <http://www.gridwiseac.org/> in the [GridWise Interoperability Context-Setting Framework](#).

3350 personnel. Cybersecurity must also address how to cope during an attack, recover from it
3351 afterwards, and create a trail of forensic information to be used in post-attack analysis.

3352 Third, the cybersecurity requirements must reflect the environment where a standard is
3353 implemented rather than the standard itself - how and where a standard is used must establish the
3354 levels and types of cybersecurity needed. Communications standards do not address the
3355 importance of specific data or how it might be used in systems; these standards only address how
3356 to exchange the data. Standards related to the upper layers of the GWAC Stack may address
3357 issues of data importance.

3358 Fourth, some standards do not mandate their provisions using “shall” statements, but rather use
3359 statements such as “should,” “may,” or “could.” Some standards also define their provisions as
3360 being “normative” or “informative.” Normative provisions often are expressed with “shall”
3361 statements. Various standards organizations use different terms (e.g., standard, guideline) to
3362 characterize their standards according to the kinds of statements used. If standards include
3363 security provisions, they need to be understood in the context of the “shall,” “should,” “may,”
3364 and/or “could” statements, “normative,” or “informative” language with which they are
3365 expressed.

3366 Therefore, cybersecurity must be viewed as a stack or “profile” of different security technologies
3367 and procedures, woven together to meet the security requirements of a particular implementation
3368 of policy, procedural, and communication standards designed to provide specific services.
3369 Ultimately cybersecurity, as applied to the information exchange standards, should be described
3370 as profiles of technologies and procedures which can include both “power system” methods (e.g.
3371 redundant equipment, analysis of power system data, and validation of power system states) and
3372 information technology (IT) methods (e.g. encryption, role-based access control, and intrusion
3373 detection).

3374 There also can be a relationship between certain communication standards and correlated
3375 cybersecurity technologies. For instance, if Transmission Control Protocol (TCP)/Internet
3376 Protocol (IP) is being used at the transport layer and if authentication, data integrity, and/or
3377 confidentiality are important, then transport layer security (TLS) should be used.

3378 In the following discussions of information exchange standard being reviewed, these caveats
3379 should be taken into account.

3380 **9.3.2 Correlation of Cybersecurity Requirements with Physical Security Requirements**

3381 Correlating cybersecurity requirements with specific physical security requirements is very
3382 complex since they generally address very different aspects of a system. Although both cyber
3383 and physical security requirements seek to prevent or deter deliberate or inadvertent attackers
3384 from accessing a protected facility, resource, or information, physical security solutions and
3385 procedures are vastly different from cybersecurity solutions and procedures, and involve very
3386 different expertise. Each may be used to help protect the other, while compromises of one can
3387 definitely compromise the other.

3388 Physical and environmental security that encompasses protection of physical assets from damage
3389 is addressed by the National Institute of Standards and Technology (NIST) Interagency Report
3390 (IR) 7628, Guidelines to Smart Grid Cyber Security, only at a high level. Therefore, assessments
3391 of standards that cover these non-cyber issues must necessarily also be at a general level.

3392 **9.3.3 Standardization Cycles of Information Exchange Standards**

3393 Information exchange standards, regardless of the standards organization, are developed over a
3394 time period of many months by experts who are trying to meet a specific need. In most cases,
3395 these experts are expected to revisit standards every five years in order to determine if updates
3396 are needed. In particular, since cybersecurity requirements were often not included in standards
3397 in the past, existing communication standards often have no references to security except in
3398 generalities, using language such as “appropriate security technologies and procedures should be
3399 implemented.”

3400 With the advent of the Smart Grid, cybersecurity has become increasingly important within the
3401 utility sector. However, since the development cycles of communication standards and
3402 cybersecurity standards are usually independent of each other, appropriate normative references
3403 between these two types of standards are often missing. Over time, these missing normative
3404 references can be added, as appropriate.

3405 Since technologies (including cybersecurity technologies) are rapidly changing to meet
3406 increasing new and more powerful threats, some cybersecurity standards can be out-of-date by
3407 the time they are released. This means that some requirements in a security standard may be
3408 inadequate (due to new technology developments), while references to other security standards
3409 may be obsolete. This rapid improving of technologies and obsolescence of older technologies is
3410 impossible to avoid, but may be ameliorated by indicating minimum requirements and urging
3411 fuller compliance to new technologies as these are proven.

3412 **9.3.4 References and Terminology**

3413 References to NISTIR 7628, security requirements refer to NISTIR 7628, Guidelines for Smart
3414 Grid Cyber Security, Chapter 3, High-Level Security Requirements.

3415 References to “government-approved cryptography” refer to the list of approved cryptography
3416 suites identified in Chapter 4, Cryptography and Key Management, of NISTIR 7628. Summary
3417 tables of the approved cryptography suites are provided in Chapter 4.3.2.1.

3418 The terms “approved”, “acceptable”, and “deprecated” are defined as the following:¹³

- 3419 • Approved is used to mean that an algorithm is specified in a FIPS or NIST
3420 Recommendation (published as a NIST Special Publication).
- 3421 • Acceptable is used to mean that the algorithm and key length is safe to use; no security
3422 risk is currently known.
- 3423 • Deprecated means that the use of the algorithm and key length is allowed, but the user
3424 must accept some risk. The term is used when discussing the key lengths or algorithms
3425 that may be used to apply cryptographic protection to data (e.g., encrypting or generating
3426 a digital signature).

3427 As noted, standards have different degrees for expressing requirements, and the security
3428 requirements must match these degrees. For these standards assessments, the following
3429 terminology is used to express these different degrees¹⁴:

¹³ The definitions are obtained from NIST Special Publication 800-131A, Transitions: *Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*.

- 3430 • Requirements are expressed by “...shall...,” which indicates mandatory requirements
- 3431 strictly to be followed in order to conform to the standard and from which no deviation is
- 3432 permitted (shall equals is required to).
- 3433 • Recommendations are expressed by “...should...,” which indicates that among several
- 3434 possibilities one is recommended as particularly suitable, without mentioning or
- 3435 excluding others; or that a certain course of action is preferred but not necessarily
- 3436 required (should equals is recommended that).
- 3437 • Permitted or allowed items are expressed by “...may...,” which is used to indicate a
- 3438 course of action permissible within the limits of the standard (may equals is permitted to).
- 3439 • Ability to carry out an action is expressed by “...can ...,” which is used for statements of
- 3440 possibility and capability, whether material, physical, or causal (can equals is able to).
- 3441 • The use of the word must is deprecated, and should not be used in these standards to
- 3442 define mandatory requirements. The word must is only used to describe unavoidable
- 3443 situations (e.g. “All traffic in this lane must turn right at the next intersection.”)

3444 **9.4 NIST CSWG STANDARDS ASSESSMENT TEMPLATE**

3445 The following subsections present the standards assessment template, including the template
 3446 structure and questions, used by the standards subgroup to report findings from their standards
 3447 review effort.

3448 **9.4.1 Description of Document**

3449 **9.4.2 Assumptions**

3450 **9.4.3 Assessment of Cybersecurity Content**

3451 **9.4.3.1 Does the standard address cybersecurity? If not, should it?**

3452 **9.4.3.2 What aspects of cybersecurity does the standard address and how well**
 3453 **(correctly) does it do so?**

3454 **Table 9-1: Correlations between Standard being Assessed and the NISTIR Security Requirements**

Reference in Standard	Applicable NISTIR 7628 High Level Security Requirements	Comments including how NISTIR HLR Requirements Are or Are Not Completely Met

3455 **9.4.3.3 What aspects of cybersecurity does the standard not address? Which of these**
 3456 **aspects should it address? Which should be handled by other means?**

3457

¹⁴ The first clause of each terminology definition comes from the International Electrotechnical Commission (IEC) Annex H of Part 2 of ISO/IEC Directives. The second clause (after “which”) comes from the Institute of Electrical and Electronics Engineers (IEEE) as a further amplification of the term.

3458 **9.4.3.4 What work, if any, is being done currently or is planned to address the gaps**
3459 **identified above? Is there a stated timeframe for completion of these planned**
3460 **modifications?**

3461 **9.4.3.5 Recommendations**

3462 The CSWG recommends {specific recommendations from the CSWG on the standard}

3463

3464 **9.4.3.6 List any references to other standards and whether they are normative or**
3465 **informative**

3466

3467 **9.5 STANDARDS REVIEW LIST**

3468 The standards reviewed by the CSWG, if so recommended, are included in the SGIP Catalog of
3469 Standards after completing the full SGIP approval process.

3470

3471

DRAFT

3472 **CHAPTER TEN**
3473 **KEY POWER SYSTEM USE CASES FOR SECURITY**
3474 **REQUIREMENTS**

3475 The focus of this chapter is to identify the key Use Cases that are “architecturally significant”
3476 with respect to security requirements for the Smart Grid. This identification is neither exhaustive
3477 nor complete. New Use Cases may be added to this appendix in future versions of this report as
3478 they become available. The Use Cases presented in this appendix will be employed in evaluating
3479 Smart Grid characteristics and associated cyber security objectives; the high-level requirements
3480 of confidentiality, integrity, and availability, (CI&A); and stakeholder concerns. The focus here
3481 is more on operational functions rather than “back office” or corporate functions, since it is the
3482 automation and control aspects of power system management that are relatively unique and
3483 certainly stretch the security risk assessment, security controls, and security management limits.

3484 Many interfaces and “environments”—with constraints and sensitive aspects—make up the
3485 information infrastructure that monitors and controls the power system infrastructure. This
3486 chapter does not directly capture those distinctions, but leaves it up to the implementers of
3487 security measures to take those factors into account.

3488 **10.1 USE CASE SOURCE MATERIAL**

3489 The Use Cases listed in this chapter were derived “as-is” from a number of sources and put into a
3490 common format for evaluation. The resulting list presented in this appendix does not constitute a
3491 catalog of recommended or mandatory Use Cases, nor are the listed Use Cases intended for
3492 architecting systems or identifying all the potential scenarios that may exist. The full set of Use
3493 Cases presented in this chapter was derived from the following sources:

- 3494 • **IntelliGrid Use Cases:** Over 700 Use Cases are provided by this source, but only the
3495 power system operations Use Cases and Demand Response (DR) or Advanced Metering
3496 Infrastructure (AMI) cases are of particular interest for security. The Electric Power
3497 Research Institute (EPRI) IntelliGrid project developed the complete list of Use Cases.
3498 *See* IntelliGrid Web site, [Complete List of Power System Functions](#).
- 3499 • **AMI Business Functions:** Use Cases were extracted from Appendix B of the Advanced
3500 Metering Infrastructure Security (AMI-SEC) System Security Requirements document
3501 (published by the AMI-SEC Task Force) by the Transmission and Distribution Domain
3502 Expert Working Group (T&D DEWG), and the Smart Grid Interoperability Panel –
3503 Cyber Security Working Group (SGIP-CSWG) has now also posted this material on the
3504 SGIP TWiki).
- 3505 • **Benefits and Challenges of Distribution Automation:** Use Case Scenarios (White
3506 Paper for Distribution on T&D DEWG), extracted from a California Energy Commission
3507 (CEC) document which has 82 Use Cases; now posted on the SGIP TWiki.
- 3508 • **EPRI Use Case Repository:** A compilation of IntelliGrid and Southern California
3509 Edison (SCE) Use Cases, plus others. *See* EPRI Web site, [Use Case Repository](#).
- 3510 • **SCE Use Cases:** Developed by Southern California Edison with the assistance of
3511 EnerNex. *See* SCE.com Web site, [Open Innovation](#).

3512 A certain amount of overlap is found in these sources, particularly in the new area of AMI.
3513 However, even the combined set (numbering over 1000 Use Cases) does not address all
3514 requirements. For example, for one operation—the connect/disconnect of meters—6 utilities
3515 developed more than 20 use case variations to meet their diverse needs, often as a means to
3516 address different state regulatory requirements.

3517 The collected Use Cases listed in this chapter were not generally copied verbatim from their
3518 sources but were oftentimes edited to focus on the security issues.

3519 **10.2 KEY SECURITY REQUIREMENTS CONSIDERATIONS**

3520 The Use Cases listed in subsection 11.3 can be considered to have key security requirements that
3521 may vary in vulnerabilities and impacts, depending upon the actual systems, but that nonetheless
3522 can be generally assessed as having security requirements in the three principal areas addressed
3523 in subsections 11.2.1 through 11.2.3.

3524 **10.2.1 CIA Security Requirements**

3525 The following points briefly outline security requirements related to confidentiality, integrity,
3526 and availability.

3527 **Confidentiality** is generally the least critical for power system reliability. However, this is
3528 important as customer information becomes more easily available in cyber form:

- 3529 • Privacy of customer information is the most important,
- 3530 • Electric market information has some confidential portions,
- 3531 • General corporate information, such as human resources, internal decision making, etc.

3532 **Integrity** is generally considered the second most critical security requirement for power system
3533 operations and includes assurance that—

- 3534 • Data has not been modified without authorization,
- 3535 • Source of data is authenticated,
- 3536 • Time -stamp associated with the data is known and authenticated,
- 3537 • Quality of data is known and authenticated.

3538 **Availability** is generally considered the most critical security requirement, although the time
3539 latency associated with availability can vary:

- 3540 • 4 milliseconds for protective relaying,
- 3541 • Subseconds for transmission wide area situational awareness monitoring,
- 3542 • Seconds for substation and feeder supervisory control and data acquisition (SCADA)
3543 data,
- 3544 • Minutes for monitoring noncritical equipment and some market pricing information,
- 3545 • Hours for meter reading and longer term market pricing information,
- 3546 • Days/weeks/months for collecting long-term data such as power quality information.

3547 **10.2.2 Critical Issues for the Security Requirements of Power Systems**

3548 The automation and control systems for power system operations have many differences from
3549 most business or corporate systems. Some particularly critical issues related to security
3550 requirements include—

- 3551 • Operation of the power system must continue 24×7 with high availability (e.g., 99.99%
3552 for SCADA and higher for protective relaying) regardless of any compromise in security
3553 or the implementation of security measures which hinder normal or emergency power
3554 system operations.
- 3555 • Power system operations must be able to continue during any security attack or
3556 compromise (as much as possible).
- 3557 • Power system operations must recover quickly after a security attack or compromised
3558 information system.
- 3559 • The complex and many-fold interfaces and interactions across this largest machine of the
3560 world—the power system—makes security particularly difficult since it is not easy to
3561 separate the automation and control systems into distinct “security domains,” and yet
3562 end-to-end security is critical.
- 3563 • There is not a one-size-fits-all set of security practices for any particular system or for
3564 any particular power system environment.
- 3565 • Testing of security measures cannot be allowed to impact power system operations.
- 3566 • Balance is needed between security measures and power system operational
3567 requirements. Absolute security is never perfectly achievable, so the costs and impacts on
3568 functionality of implementing security measures must be weighed against the possible
3569 impacts from security breaches.
- 3570 • Balance is also needed between risk and the cost of implementing the security measures.

3571 **10.2.3 Security Programs and Management**

3572 Development of security programs is critical to all Use Cases, including—

- 3573 • Risk assessment to develop security requirements based on business rational (e.g. impacts
3574 from security breaches of ICIA) and system vulnerabilities.
 - 3575 – The likelihood of particular threat agents, which are usually included in risk
3576 assessments, should only play a minor role in the overall risk assessment, since the
3577 power system is so large and interconnected that appreciating the risk of these threat
3578 agents would be very difficult.
 - 3579 – However, in detailed risk assessments of specific assets and systems, some
3580 appreciation of threat agent probabilities is necessary to ensure that an appropriate
3581 balance between security and operability is maintained.
- 3582 • Security technologies that are needed to meet the security requirements:
 - 3583 – Plan the system designs and technologies to embed the security from the start
 - 3584 – Implement the security protocols

- 3585 – Add physical security measures
- 3586 – Implement the security monitoring and alarming tools
- 3587 – Establish role-based access control (RBAC) to authorize and authenticate users, both
- 3588 human and cyber, for all activities, including password/access management,
- 3589 certificate and key management, and revocation management
- 3590 – Provide the security applications for managing the security measures
- 3591 • Security policies, training, and enforcement to focus on the human side of security,
- 3592 including:
 - 3593 – Normal operations
 - 3594 – Emergency operations when faced with a possible or actual security attack
 - 3595 – Recovery procedures after an attack
 - 3596 – Documentation of all anomalies for later analysis and re-risk assessment.
- 3597 • Conformance testing for both humans and systems to verify they are using the security
- 3598 measures and tools appropriately and not bypassing them:
 - 3599 – Care must be taken not to impact operations during such testing
 - 3600 – If certain security measures actually impact power system operations, the balance
 - 3601 between that impact and the impact of a security compromise should be evaluated
- 3602 • Periodic reassessment of security risks

3603 **10.3 USE CASE SCENARIOS**

3604 The following subsections present the key Use Cases deemed architecturally significant with
 3605 respect to security requirements for the Smart Grid, with the listing grouped according to 10
 3606 main categories: AMI, Demand Response, Customer Interfaces, Electricity Market, Distribution
 3607 Automation, Plug-in Hybrid Electric Vehicles (PHEV), Distributed Resources, Transmission
 3608 Resources, Regional Transmission Operator / Independent System Operator (RTO/ISO)
 3609 Operations, and Asset Management.

3610 **10.3.1 AMI Security Use Cases**

3611 In this chapter basic use cases are described which can be used as building blocks for more
 3612 complex use cases that users of this guideline and AMI security profile may be interested in.
 3613 Dozens of use cases can be constructed from these basic functions. A few short examples are
 3614 provided below that demonstrate a more detailed process of combining the basic building blocks
 3615 in the AMI security profile.

3616 There are other functions not specified below which can be composed from these defined
 3617 functions. The absence of a function on the list of use cases should not be taken as indication
 3618 those functions are less important, but as an indication those functions are combinations of basic
 3619 functions with the possible addition of out-of-scope and/or business process behaviors. Some
 3620 examples:

- 3621 • Revenue Protection: Revenue protection with respect to AMI consists of a number of
3622 business processes combined with AMI functions. For example, theft of service can be
3623 identified by comparing meter reads (Meter Sends Information function) of power line
3624 branch meter with the sum of meter reads of each of the subscribers on that branch (a
3625 specific non-AMI business process). A discrepancy on the total can indicate theft of
3626 service.

- 3627 • Meter Removal: Detection of meter removal can occur in a number of different ways
3628 including “Meter Sends Information” where the exception case indicates no contact with
3629 the meter or “Meter Sends Alarm” where the self-protection capability of the meter notes
3630 a tamper event. Additionally, meter not communicating (disassociated from network)
3631 where a meter that has been associated or registered on the network is no longer
3632 performing necessary activities to maintain registration.

- 3633 • Meter Bypass: Generically, detection of meter bypass is a back office business process
3634 dependent on information received from the field. One way of detecting meter bypass is
3635 historical analysis of consumption data and comparison of that data to other similar
3636 subscribers in the region.

- 3637 • Outage Detection and Restoration: This is not directly an AMI function, but information
3638 for the process can be acquired from the AMI meter field through the “Meter Sends
3639 Information” function and the “Meter Sends Alarm” function. Depending on the needs of
3640 restoration, “Utility Sends Operational Command” may also occur. The specific set of
3641 functions for detection and restoration will most likely be different with each outage
3642 event and may differ based on the Utility and its practices.

- 3643 • Pre-paid Metering: Depending on the specific mechanism for pre-paid metering (e.g.
3644 payment at the meter, payment to the utility, emergency power enable button) this can
3645 end up being the combination of any or all AMI functions. At the simplest, the setting of
3646 a consumption limit on a meter based on some business process decision by the utility
3647 would be a “Utility Sends Operational Command”. Information about consumption rates
3648 as well as warnings about credit exhaustion will flow back to the utility via “Meter Sends
3649 Information” and “Meter Sends Alarm”.

3650 The 6 basic functions listed below were chosen because they mostly represent the same level of
3651 control plane and they involve only AMI elements. These use cases have been updated and
3652 improved since the first issuance of this document to more accurately reflect reality. As utilities
3653 flesh out their set of use cases which involve (but are not necessarily limited to) AMI elements,
3654 they should use this set of functions to describe the AMI portion of the use case.
3655

Category: AMI		Overall Use Case #1
Scenario: Meter sends information		
<p><u>Category Description</u></p> <p>AMI systems consist of the hardware, software, and associated system and data management applications that create a communications network between end systems at customer premises (including meters, gateways, and other equipment) and diverse business and operational systems of utilities and third parties. AMI systems provide the technology to allow the exchange of information between customer end systems and those other utility and third-party systems. In order to protect this critical infrastructure, end-to-end security must be provided across the AMI systems, encompassing the customer end systems as well as the utility and third-party systems that are interfaced to the AMI systems.</p>		
<p><u>Scenario Description</u></p> <p>A meter sends automated energy usage information to the Utility (e.g. meter read (usage data)). The automated send of energy usage information is initiated by the meter and is sent to the Advanced metering Infrastructure (AMI) Head End System (HES). The Head End system message flows to the meter Reading and Control (MRC). The MRC evaluates the message. The MRC archives the automated energy usage information and forwards the information onto the meter Data Management Systems (MDMS).</p> <ul style="list-style-type: none"> • Meter configuration information • Periodic meter Reading • On-Demand meter Reading • Net metering for distributed energy resources (DER) and plug in electric vehicle (PEV) 		
<p><u>Smart Grid Characteristics</u></p> <ul style="list-style-type: none"> • Enables active participation by consumers • Enables new products, services and markets • Optimizes asset utilization and operate efficiently 	<p><u>Cyber Security Objectives/Requirements</u></p> <ul style="list-style-type: none"> • Confidentiality (privacy) of customer metering data over the AMI system, metering database, and billing database to avoid serious breaches of privacy and potential legal repercussions • Integrity of meter data is important, but the impact of incorrect data is not large • Availability of meter data is not critical in real-time 	<p><u>Potential Stakeholder Issues</u></p> <ul style="list-style-type: none"> • Customer data access • Customer data privacy and security • Reliable data for billing • Third party or party acting as an agent of the utility access to energy usage information for market and/or consumer services • Third party or party acting on behalf of the utility reliable data

3656
3657

Category: AMI		Overall Use Case #2
Scenario: Utility sends operational command to meter		
<p><u>Category Description</u></p> <p>AMI systems consist of the hardware, software, and associated system and data management applications that create a communications network between end systems at customer premises (including meters, gateways, and other equipment) and diverse business and operational systems of utilities and third parties. AMI systems provide the technology to allow the exchange of information between customer end systems and those other utility and third-party systems. In order to protect this critical infrastructure, end-to-end security must be provided across the AMI systems, encompassing the customer end systems as well as the utility and third-party systems that are interfaced to the AMI systems.</p>		
<p><u>Scenario Description</u></p> <p>A Utility requires an operational command be sent to the meter, such as a disconnect or reconnect of an electric smart meter. The command flows to the meter Reading and Control (MRC) that looks up the meter associated with the customer and then instructs the Advanced metering Infrastructure (AMI) Head End system (HES) to communicate the command to the meter. The HES evaluates current conditions and, if suitable (e.g. reconnects are not executed if the system is in a rolling black out state), sends the command to the meter. When the meter receives the command and parameters, the meter evaluates the command as to whether it is permitted. If the command is permitted, the meter executes the command and sends the result to the HES. If the command is not permitted, the meter sends the result to the HES. The HES evaluates the result (whether the action was successful or not and why) and relays that to the MRC. The MRC records the command result and notifies the appropriate actors.</p> <ul style="list-style-type: none"> • Configuration request • Calibration request • Connect / Disconnect request • Prepaid metering configuration/setup 		
<p><u>Smart Grid Characteristics</u></p> <ul style="list-style-type: none"> • Optimizes asset utilization and operate efficiently • Operates resiliently against attack and natural disasters 	<p><u>Cyber Security Objectives/Requirements</u></p> <ul style="list-style-type: none"> • Confidentiality requirements of the meter command is generally not very important • Integrity of control commands to the meter is critical to avoid dangerous/unsafe conditions. • Availability is not important with the exception of emergency situations such as fire or medical emergency for remote connect/disconnect. 	<p><u>Potential Stakeholder Issues</u></p> <ul style="list-style-type: none"> • Customer Safety • Third party or party acting as an agent of the utility access to energy usage information for market and/or consumer services

3661

Category: AMI		Overall Use Case #3
Scenario: Field tool sends instruction to the meter		
<p><u>Category Description</u></p> <p>AMI systems consist of the hardware, software, and associated system and data management applications that create a communications network between end systems at customer premises (including meters, gateways, and other equipment) and diverse business and operational systems of utilities and third parties. AMI systems provide the technology to allow the exchange of information between customer end systems and those other utility and third-party systems. In order to protect this critical infrastructure, end-to-end security must be provided across the AMI systems, encompassing the customer end systems as well as the utility and third-party systems that are interfaced to the AMI systems.</p>		
<p><u>Scenario Description</u></p> <p>A field tool requires onsite maintenance of an electric smart meter. The Field Tool connects directly to an electric smart meter, then the command flows to the smart meter. When the meter receives the command and parameters, the meter evaluates the command as to whether it is permitted. If the command is permitted, the meter executes the command and sends the result back to the field tool. This use case is a closed loop, as stated in the preconditions.</p> <ul style="list-style-type: none"> • Meter calibration update • Meter configuration update 		
<p><u>Smart Grid Characteristics</u></p> <ul style="list-style-type: none"> • Optimizes asset utilization and operate efficiently • Enables new products, services and markets 	<p><u>Cyber Security Objectives/Requirements</u></p> <ul style="list-style-type: none"> • Confidentiality is not important unless some maintenance activity involves personal information • Integrity of meter maintenance repairs and updates are essential to prevent malicious intrusions and integrity of billing data to prevent high utility bills • Availability is important, because field tool requires real time interaction with the meter. 	<p><u>Potential Stakeholder Issues</u></p> <ul style="list-style-type: none"> • Customer data privacy and security • Third party or party acting as an agent of the utility having access to customer & Utility information

3662

3663

Category: AMI	Overall Use Case #4	
Scenario: Utility sends non-operational instruction to meter (peer-to-peer)		
<p><u>Category Description</u></p> <p>AMI systems consist of the hardware, software, and associated system and data management applications that create a communications network between end systems at customer premises (including meters, gateways, and other equipment) and diverse business and operational systems of utilities and third parties. AMI systems provide the technology to allow the exchange of information between customer end systems and those other utility and third-party systems. In order to protect this critical infrastructure, end-to-end security must be provided across the AMI systems, encompassing the customer end systems as well as the utility and third-party systems that are interfaced to the AMI systems.</p>		
<p><u>Scenario Description</u></p> <p>This use case describes the Utility sending a non-operational instruction send to meter as a peer-to-peer transaction. A Utility requires actions from a set of meter which may or may not result in a change to the power state of the grid. These include at least meter reading, and certain configuration changes. The meter Reading and Control (MRC) determines the need to send instruction(s) to a meter. MRC looks up the meter associated with the customer and then instructs the Advanced metering Infrastructure (AMI) Head End system (HES) to queue up and execute the instruction(s). The AMI Head End can determine the instruction needs to be split into packets, schedules the sending of the packets and continues to send the packets to the meter until all instruction packets have been sent. The meter receives the instruction(s) and determines if the instruction is permitted. After execution, the meter sends the instruction result to the HES. The HES will then send the instruction result to the MRC. If the instruction result is energy usage information, the MRC will then forward the energy usage information onto the meter Data Management System (MDMS). If the MDMS receives energy usage information, then the MDMS forwards the energy usage information onto other actors for other actions.</p> <ul style="list-style-type: none"> • Meter calibration validation • Connectivity validation • Geolocation of meter • Smart meter battery management 		
<p><u>Smart Grid Characteristics</u></p> <ul style="list-style-type: none"> • Optimizes asset utilization and operate efficiently • Operates resiliently in response to natural and manmade events • Increases the timeliness, availability, and granularity of information for billing 	<p><u>Cyber Security Objectives/Requirements</u></p> <ul style="list-style-type: none"> • Confidentiality may or may not be an issue depending on whether information is public (date, time) or private (password change, Personal Identifiable Information). Some items must be confidential due to laws and regulations; confidentiality of other items may be left up to local policy, such as firmware or GPS coordinates. • Integrity of meter maintenance repairs and updates is essential to prevent malicious intrusions • Availability is important, but only in terms of hours or maybe days to provide synchronization and coherence of devices on the network, i.e. all devices acting together for entire population 	<p><u>Potential Stakeholder Issues</u></p> <ul style="list-style-type: none"> • Customer data privacy and security • Third party or party acting as an agent of the utility having access to customer & Utility information • Third party access to electrical distribution system, e.g. separation of duties & authority (regulatory impact) • Vendor product quality

Category: AMI	Overall Use Case #5	
Scenario: Utility sends batch instruction to meters (group multicast transaction)		
<p><u>Category Description</u></p> <p>AMI systems consist of the hardware, software, and associated system and data management applications that create a communications network between end systems at customer premises (including meters, gateways, and other equipment) and diverse business and operational systems of utilities and third parties. AMI systems provide the technology to allow the exchange of information between customer end systems and those other utility and third-party systems. In order to protect this critical infrastructure, end-to-end security must be provided across the AMI systems, encompassing the customer end systems as well as the utility and third-party systems that are interfaced to the AMI systems.</p>		
<p><u>Scenario Description</u></p> <p>This use case describes a batch instruction send to meters as a multicast transaction in an open loop situation. The open loop situation means that Advanced metering Infrastructure (AMI) Head End System (HES) does not expect a response for each packet sent to a meter. A Utility requires actions from a set of meters which may or may not result in a change to the power state of the grid. These include at least meter reading, and certain configuration changes. The meter Reading and Control (MRC) determines the need to send batch instructions to more than one meter. MRC looks up the meter associated with the customer and then instructs the Advanced metering Infrastructure (AMI) Head End system (HES) to queue up and execute the instructions. The AMI Head End can determine the instruction needs to be split into packets, schedules the sending of the packets and continues to send the packets to the meters until all instruction packets have been sent. The meter(s) receive the instruction(s) and determines if the instruction is permitted. After execution, the meter(s) send the instruction result to the HES. The HES will then send the instruction result to the MRC. If the instruction result is energy usage information, the MRC will then forward the energy usage information onto the meter Data Management System (MDMS). If the MDMS receives energy usage information, then the MDMS forwards the energy usage information onto other actors for other actions.</p> <ul style="list-style-type: none"> • Firmware update • Key management update 		
<p><u>Smart Grid Characteristics</u></p> <ul style="list-style-type: none"> • Optimizes asset utilization and operate efficiently • Enables new products, services and markets • Reduces cost of operations 	<p><u>Cyber Security Objectives/Requirements</u></p> <ul style="list-style-type: none"> • Confidentiality is not important unless some maintenance activity involves personal information • Integrity of meter maintenance repairs and updates are essential to prevent malicious intrusions • Availability is important, but only in terms of hours or maybe days 	<p><u>Potential Stakeholder Issues</u></p> <ul style="list-style-type: none"> • Confirmation (if required) of update status. • Customer data privacy and security • Third party or party acting as an agent of the utility access to energy usage information for market and/or consumer services

3665
3666

Category: AMI		Overall Use Case #6
Scenario: Meter sends alarm or unsolicited and unscheduled request to the utility		
<p><u>Category Description</u> AMI systems consist of the hardware, software, and associated system and data management applications that create a communications network between end systems at customer premises (including meters, gateways, and other equipment) and diverse business and operational systems of utilities and third parties. AMI systems provide the technology to allow the exchange of information between customer end systems and those other utility and third-party systems. In order to protect this critical infrastructure, end-to-end security must be provided across the AMI systems, encompassing the customer end systems as well as the utility and third-party systems that are interfaced to the AMI systems.</p>		
<p><u>Scenario Description</u> A meter sends an alarm or unsolicited and unscheduled request to the Utility (e.g. Physical tamper detection, Network join request, or HAN device / direct load control device enrollment request (proxy for customer). The message is initiated by the meter and sends the messages to the Advanced metering Infrastructure (AMI) Head End System (HES). The HES message flows to the meter Reading and Control (MRC). The MRC evaluates the message. The MRC records the command result and notifies the appropriate actors.</p>		
<p><u>Smart Grid Characteristics</u></p> <ul style="list-style-type: none"> • Optimizes asset utilization and operate efficiently • Operates resiliently against attack and natural disasters 	<p><u>Cyber Security Objectives/Requirements</u></p> <ul style="list-style-type: none"> • Confidentiality is not important unless alarm contains private information or exposes an attempt to obtain security information stored in the meter • Integrity - Protect against energy theft • Protect integrity of meter configuration • protect integrity of reporting • To protect the integrity of the network (authorized devices) • Availability is important to capture last gasp detecting, join detection, and reporting 	<p><u>Potential Stakeholder Issues</u></p> <ul style="list-style-type: none"> • Network Service Providers • Customer may receive outage notification through third party • Billing service provider • Transmission & Distribution service provider

3667

3668

3669 **10.3.2 Demand Response Security Use Cases**

Category: Demand Response (DR)		Overall Use Case #7
Scenario: Real-Time Pricing (RTP) for Customer Load and DER/PEV		
<p><u>Category Description</u></p> <p>Demand response is a general capability that could be implemented in many different ways. The primary focus is to provide the customer with pricing information for current or future time periods so they may respond by modifying their demand. This may entail just decreasing load or may involve shifting load by increasing demand during lower priced time periods so that they can decrease demand during higher priced time periods. The pricing periods may be real-time based or may be tariff based, while the prices may also be operationally based or fixed or some combination. RTP inherently requires computer-based responses, while the fixed time-of-use pricing may be manually handled once the customer is aware of the time periods and the pricing.</p>		
<p><u>Scenario Description</u></p> <p>Use of RTP for electricity is common for very large customers, affording them an ability to determine when to use power and minimize the costs of energy for their business. The extension of RTP to smaller industrial and commercial customers and even residential customers is possible with smart metering and in-home displays. Aggregators or customer energy management systems must be used for these smaller consumers due to the complexity and 24x7 nature of managing power consumption. Pricing signals may be sent via an AMI system, the Internet, or other data channels.</p>		
<p><u>Smart Grid Characteristics</u></p> <ul style="list-style-type: none"> • Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets 	<p><u>Cyber Security Objectives/Requirements</u></p> <ul style="list-style-type: none"> • Integrity, including nonrepudiation, of pricing information is critical, since there could be large financial and possibly legal implications • Availability, including nonrepudiation, for pricing signals is critical because of the large financial and possibly legal implications • Confidentiality is important mostly for the responses that any customer might make to the pricing signals 	<p><u>Potential Stakeholder Issues</u></p> <ul style="list-style-type: none"> • Customer data privacy and security • Retail Electric Supplier access • Customer data access

Category: Demand Response		Overall Use Case #8
Scenario: Time of Use (TOU) Pricing		
<p><u>Category Description</u></p> <p>Demand response is a general capability that could be implemented in many different ways. The primary focus is to provide the customer with pricing information for current or future time periods so they may respond by modifying their demand. This may entail just decreasing load or may involve shifting load by increasing demand during lower priced time periods so that they can decrease demand during higher priced time periods. The pricing periods may be real-time based or may be tariff based, while the prices may also be operationally based or fixed or some combination. Real-time pricing inherently requires computer-based responses, while the fixed TOU pricing may be manually handled once the customer is aware of the time periods and the pricing.</p>		
<p><u>Scenario Description</u></p> <p>TOU creates blocks of time and seasonal differences that allow smaller customers with less time to manage power consumption to gain some of the benefits of real-time pricing. This is the favored regulatory method in most of the world for dealing with global warming.</p> <p>Although RTP is more flexible than TOU, it is likely that TOU will still provide many customers will all of the benefits that they can profitably use or manage.</p>		
<p><u>Smart Grid Characteristics</u></p> <ul style="list-style-type: none"> • Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets 	<p><u>Cyber Security Objectives/Requirements</u></p> <ul style="list-style-type: none"> • Integrity is not critical since TOU pricing is fixed for long periods and is not generally transmitted electronically • Availability is not an issue • Confidentiality is not an issue, except with respect to meter reading 	<p><u>Potential Stakeholder Issues</u></p> <ul style="list-style-type: none"> • Customer data privacy and security • Retail Electric Supplier access • Customer data access

Category: Demand Response		Overall Use Case #9
Scenario: Net Metering for DER and PEV		
<p><u>Category Description</u></p> <p>Demand response is a general capability that could be implemented in many different ways. The primary focus is to provide the customer with pricing information for current or future time periods so they may respond by modifying their demand. This may entail just decreasing load or may involve shifting load by increasing demand during lower priced time periods so that they can decrease demand during higher priced time periods. The pricing periods may be real-time based or may be tariff based, while the prices may also be operationally based or fixed or some combination. Real-time pricing inherently requires computer-based responses, while the fixed time-of-use pricing may be manually handled once the customer is aware of the time periods and the pricing.</p>		
<p><u>Scenario Description</u></p> <p>When customers have the ability to generate or store power as well as consume power, net metering is installed to measure not only the flow of power in each direction, but also when the net power flows occurred. Often TOU tariffs are employed.</p> <p>Today larger commercial and industrial (C&I) customers and an increasing number of residential and smaller C&I customers have net metering installed for their photovoltaic systems, wind turbines, combined heat and power (CHP), and other DER devices. As PEVs become available, net metering will increasingly be implemented in homes and small businesses, even parking lots.</p>		
<p><u>Smart Grid Characteristics</u></p> <ul style="list-style-type: none"> • Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets 	<p><u>Cyber Security Objectives/Requirements</u></p> <ul style="list-style-type: none"> • Integrity is not very critical since net metering pricing is fixed for long periods and is not generally transmitted electronically • Availability is not an issue • Confidentiality is not an issue, except with respect to meter reading 	<p><u>Potential Stakeholder Issues</u></p> <ul style="list-style-type: none"> • Customer data privacy and security • Retail Electric Supplier access • Customer data access

3676

Category: Demand Response		Overall Use Case #10
Scenario: Feed-In Tariff Pricing for DER and PEV		
<p><u>Category Description</u></p> <p>Demand response is a general capability that could be implemented in many different ways. The primary focus is to provide the customer with pricing information for current or future time periods so they may respond by modifying their demand. This may entail just decreasing load or may involve shifting load by increasing demand during lower priced time periods so that they can decrease demand during higher priced time periods. The pricing periods may be real-time based or may be tariff based, while the prices may also be operationally based or fixed or some combination. Real-time pricing inherently requires computer-based responses, while the fixed time-of-use pricing may be manually handled once the customer is aware of the time periods and the pricing.</p>		
<p><u>Scenario Description</u></p> <p>Feed-in tariff pricing is similar to net metering except that generation from customer DER/PEV has a different tariff rate than the customer load tariff rate during specific time periods.</p>		
<p><u>Smart Grid Characteristics</u></p> <ul style="list-style-type: none"> • Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets 	<p><u>Cyber Security Objectives/Requirements</u></p> <ul style="list-style-type: none"> • Integrity is not critical, since feed-in tariff pricing is fixed for long periods and is generally not transmitted electronically • Availability is not an issue • Confidentiality is not an issue, except with respect to meter reading 	<p><u>Potential Stakeholder Issues</u></p> <ul style="list-style-type: none"> • Customer data privacy and security • Retail Electric Supplier access • Customer data access

3677

3678

3679

Category: Demand Response		Overall Use Case #11
Scenario: Critical Peak Pricing		
<p><u>Category Description</u></p> <p>Demand response is a general capability that could be implemented in many different ways. The primary focus is to provide the customer with pricing information for current or future time periods so they may respond by modifying their demand. This may entail just decreasing load or may involve shifting load by increasing demand during lower priced time periods so that they can decrease demand during higher priced time periods. The pricing periods may be real-time based or may be tariff based, while the prices may also be operationally based or fixed or some combination. Real-time pricing inherently requires computer-based responses, while the fixed time-of-use pricing may be manually handled once the customer is aware of the time periods and the pricing.</p>		
<p><u>Scenario Description</u></p> <p>Critical Peak Pricing builds on TOU pricing by selecting a small number of days each year where the electric delivery system will be heavily stressed and increasing the peak (and sometime shoulder peak) prices by up to 10 times the normal peak price. This is intended to reduce the stress on the system during these days.</p>		
<p><u>Smart Grid Characteristics</u></p> <ul style="list-style-type: none"> • Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets 	<p><u>Cyber Security Objectives/Requirements</u></p> <ul style="list-style-type: none"> • Integrity is not critical, since feed-in tariff pricing is fixed for long periods and is generally not transmitted electronically • Availability is not an issue • Confidentiality is not an issue, except with respect to meter reading 	<p><u>Potential Stakeholder Issues</u></p> <ul style="list-style-type: none"> • Customer data privacy and security • Retail Electric Supplier access • Customer data access

3680

3681

Category: Demand Response		Overall Use Case #12
Scenario: Mobile Plug-In Electric Vehicle Functions		
<p><u>Category Description</u></p> <p>Demand response is a general capability that could be implemented in many different ways. The primary focus is to provide the customer with pricing information for current or future time periods so they may respond by modifying their demand. This may entail just decreasing load or may involve shifting load by increasing demand during lower priced time periods so that they can decrease demand during higher priced time periods. The pricing periods may be real-time based or may be tariff based, while the prices may also be operationally based or fixed or some combination. Real-time pricing inherently requires computer-based responses, while the fixed time-of-use pricing may be manually handled once the customer is aware of the time periods and the pricing.</p>		
<p><u>Scenario Description</u></p> <p>In addition to customers with PEVs participating in their home-based Demand Response functions, they will have additional requirements for managing the charging and discharging of their mobile PEVs in other locations:</p> <p>Customer connects PEV at another home Customer connects PEV outside home territory Customer connects PEV at public location Customer charges the PEV</p>		
<p><u>Smart Grid Characteristics</u></p> <ul style="list-style-type: none"> • Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets 	<p><u>Cyber Security Objectives/Requirements</u></p> <ul style="list-style-type: none"> • Integrity is not critical, since feed-in tariff pricing is fixed for long periods and is generally not transmitted electronically • Availability is not an issue • Confidentiality is not an issue, except with respect to meter reading 	<p><u>Potential Stakeholder Issues</u></p> <ul style="list-style-type: none"> • Customer data privacy and security • Retail Electric Supplier access • Customer data access

3684 **10.3.3 Customer Interfaces Security Use Cases**

Category: Customer Interfaces		Overall Use Case #13
Scenario: Customer's In Home Device is Provisioned to Communicate With the Utility		
Category Description Customers want to understand how their energy consumption habits affect their monthly energy bills and to find ways to reduce their monthly energy costs. Customers should have the ability to receive information on their usage and the price of energy on a variety of devices (in-home displays, computers, and mobile devices). In addition to real-time and historical energy data, customers should be able to receive messages from the utility notifying them about outages.		
Scenario Description This scenario describes the process to configure a customer's device to receive and send data to utility systems. The device could be an information display, communicating thermostat, load control device, or smart appliance.		
Smart Grid Characteristics <ul style="list-style-type: none"> • Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets 	Cyber Security Objectives/Requirements <ul style="list-style-type: none"> • To protect passwords • To protect key material • To authenticate with other devices on the AMI system 	Potential Stakeholder Issues <ul style="list-style-type: none"> • Customer device standards • Customer data privacy and security

3685

Category: Customer Interfaces		Overall Use Case #14
Scenario: Customer Views Pricing or Energy Data on Their In-Home Device		
Category Description Customers want to understand how their energy consumption habits affect their monthly energy bills and to find ways to reduce their monthly energy costs. Customers should have the ability to receive information on their usage and the price of energy on a variety of devices (in-home displays, computers, and mobile devices). In addition to real-time and historical energy data, customers should be able to receive messages from the utility notifying them about outages.		
Scenario Description This scenario describes the information that should be available to customers on their in-home devices. Multiple communication paths and device functions will be considered.		
Smart Grid Characteristics <ul style="list-style-type: none"> • Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets 	Cyber Security Objectives/Requirements <ul style="list-style-type: none"> • To validate that information is trustworthy (integrity) 	Potential Stakeholder Issues <ul style="list-style-type: none"> • Customer device standards • Customer data privacy and security

3686

Category: Customer Interfaces		Overall Use Case #15
Scenario: In-Home Device Troubleshooting		
<u>Category Description</u> Customers want to understand how their energy consumption habits affect their monthly energy bills and to find ways to reduce their monthly energy costs. Customers should have the ability to receive information on their usage and the price of energy on a variety of devices (in-home displays, computers, and mobile devices). In addition to real-time and historical energy data, customers should be able to receive messages from the utility notifying them about outages.		
<u>Scenario Description</u> This alternate scenario describes the resolution of communication or other types of errors that could occur with in-home devices. Roles of the customer, device vendor, and utility will be discussed.		
<u>Smart Grid Characteristics</u> <ul style="list-style-type: none"> • Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets 	<u>Cyber Security Objectives/Requirements</u> <ul style="list-style-type: none"> • To avoid disclosing customer information • To avoid disclosing key material and/or passwords 	<u>Potential Stakeholder Issues</u> <ul style="list-style-type: none"> • Customer device standards • Customer data privacy and security

3687

Category: Customer Interfaces		Overall Use Case #16
Scenario: Customer Views Pricing or Energy Data via the Internet		
<u>Category Description</u> Customers want to understand how their energy consumption habits affect their monthly energy bills and to find ways to reduce their monthly energy costs. Customers should have the ability to receive information on their usage and the price of energy on a variety of devices (in -home displays, computers, and mobile devices). In addition to real-time and historical energy data, customers should be able to receive messages from the utility notifying them about outages.		
<u>Scenario Description</u> In addition to a utility operated communications network (i.e., AMI), the Internet can be used to communicate to customers and their devices. Personal computers and mobile devices may be more suitable for displaying some types of energy data than low cost specialized in-home display devices. This scenario describes the information that should be available to the customer using the Internet and some possible uses for the data.		
<u>Smart Grid Characteristics</u> <ul style="list-style-type: none"> • Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets 	<u>Cyber Security Objectives/Requirements</u> <ul style="list-style-type: none"> • To protect customer's information (privacy) • To provide accurate information 	<u>Potential Stakeholder Issues</u> <ul style="list-style-type: none"> • Customer device standards • Customer data privacy and security

3688

Category: Customer Interfaces		Overall Use Case #17
Scenario: Utility Notifies Customers of Outage		
Category Description Customers want to understand how their energy consumption habits affect their monthly energy bills and to find ways to reduce their monthly energy costs. Customers should have the ability to receive information on their usage and the price of energy on a variety of devices (in-home displays, computers, and mobile devices). In addition to real-time and historical energy data, customers should be able to receive messages from the utility notifying them about outages.		
Scenario Description When an outage occurs the utility can notify affected customers and provide estimated restoration times and report when power has been restored. Smart Grid technologies can improve the utility's accuracy for determination of affected area and restoration progress.		
Smart Grid Characteristics <ul style="list-style-type: none"> • Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets 	Cyber Security Objectives/Requirements <ul style="list-style-type: none"> • To validate that the notification is legitimate • Customer's information is kept private 	Potential Stakeholder Issues <ul style="list-style-type: none"> • Customer device standards • Customer data privacy and security

3689

Category: Customer Interfaces		Overall Use Case #18
Scenario: Customer Access to Energy-Related Information		
<u>Category Description</u> Customers with home area networks (HANs) and/or building energy management (BEM) systems will be able to interact with the electric utilities as well as third-party energy services providers to access information on their own energy profiles, usage, pricing, etc.		
<u>Scenario Description</u> Customers with HANs and/or BEM systems will be able to interact with the electric utilities as well as third-party energy services providers. Some of these interactions include: Access to real-time (or near-real-time) energy and demand usage and billing information Requesting energy services such as move-in/move-out requests, prepaying for electricity, changing energy plans (if such tariffs become available), etc. Access to energy pricing information Access to their own DER generation/storage status Access to their own PEV charging/discharging status Establishing thermostat settings for demand response pricing levels Although different types of energy related information access is involved, the security requirements are similar.		
<u>Smart Grid Characteristics</u>	<u>Cyber Security Objectives/Requirements</u>	<u>Potential Stakeholder Issues</u>
<ul style="list-style-type: none"> • Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets 	<ul style="list-style-type: none"> • Integrity, including non-repudiation, is critical since energy and pricing data will have financial impacts • Availability is important to the individual customer, but will not have wide-spread impacts • Confidentiality is critical because of customer privacy issues 	<ul style="list-style-type: none"> • Customer data privacy and security • Retail Electric Supplier access • Customer data access

3690

3691 **10.3.4 Electricity Market Security Use Cases**

Category: Electricity Market		Overall Use Case #19
Scenario: Bulk Power Electricity Market		
Category Description The electricity market varies significantly from state to state, region to region, and at local levels. The market is still evolving after some initial setbacks and is expected to expand from bulk power to retail power and eventually to individual customer power as tariffs are developed to provide incentives. Demand response, handled in subsection 10.3.2, is a part of the electricity market.		
Scenario Description The bulk power market varies from region to region, and is conducted primarily through RTOs and ISOs. The market is handled independently from actual operations, although the bids into the market obviously affect which generators are used for what time periods and which functions (base load, regulation, reserve, etc.). Therefore there are no direct operational security impacts, but there are definitely financial security impacts.		
Smart Grid Characteristics <ul style="list-style-type: none"> • Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets 	Cyber Security Objectives/Requirements <ul style="list-style-type: none"> • Integrity for pricing and generation information is critical • Availability for pricing and generation information is important within minutes to hours • Confidentiality for pricing and generation information is critical 	Potential Stakeholder Issues <ul style="list-style-type: none"> • Customer data privacy and security • Retail Electric Supplier access • Customer data access

3692

Category: Electricity Market		Overall Use Case #20
Scenario: Retail Power Electricity Market		
<p><u>Category Description</u></p> <p>The electricity market varies significantly from state to state, region to region, and at local levels. The market is still evolving after some initial setbacks and is expected to expand from bulk power to retail power and eventually to individual customer power as tariffs are developed to provide incentives. Demand response, handled in subsection 10.3.2, is a part of the electricity market.</p>		
<p><u>Scenario Description</u></p> <p>The retail power electricity market is still minor, but growing, compared to the bulk power market but typically involves aggregators and energy service providers bidding customer-owned generation or load control into both energy and ancillary services. Again it is handled independently from actual power system operations. Therefore there are no direct operational security impacts, but there are definitely financial security impacts. (The aggregator's management of the customer-owned generation and load is addressed in the Demand Response subsection (see 10.3.2).)</p>		
<p><u>Smart Grid Characteristics</u></p> <ul style="list-style-type: none"> • Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets 	<p><u>Cyber Security Objectives/Requirements</u></p> <ul style="list-style-type: none"> • Integrity for pricing and generation information is critical • Availability for pricing and generation information is important within minutes to hours • Confidentiality for pricing and generation information is critical 	<p><u>Potential Stakeholder Issues</u></p> <ul style="list-style-type: none"> • Customer data privacy and security • Retail Electric Supplier access • Customer data access

3693

Category: Electricity Market		Overall Use Case #21
Scenario: Carbon Trading Market		
<u>Category Description</u> The electricity market varies significantly from state to state, region to region, and at local levels. The market is still evolving after some initial setbacks and is expected to expand from bulk power to retail power and eventually to individual customer power as tariffs are developed to provide incentives. Demand response, handled in subsection 10.3.2, is a part of the electricity market.		
<u>Scenario Description</u> The carbon trading market does not exist yet, but the security requirements will probably be similar to the retail electricity market.		
<u>Smart Grid Characteristics</u> <ul style="list-style-type: none"> • Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets 	<u>Cyber Security Objectives/Requirements</u> <ul style="list-style-type: none"> • Integrity for pricing and generation information is critical • Availability for pricing and generation information is important within minutes to hours • Confidentiality for pricing and generation information is critical 	<u>Potential Stakeholder Issues</u> <ul style="list-style-type: none"> • Customer data privacy and security • Retail Electric Supplier access • Customer data access

3694

3695 **10.3.5 Distribution Automation Security Use Cases**

Category: Distribution Automation (DA)		Overall Use Case #22
Scenario: DA within Substations		
<p>Category Description</p> <p>A broad definition of “distribution automation” includes any automation that is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources, and automated interfaces with end-users.</p> <p>No one approach is optimal for a utility or its customers. Certain DA functions, such as optimal volt/VAR control, can be more beneficial to one utility or even a few feeders in one utility, while other DA functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.</p> <p>Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.</p>		
<p>Scenario Description</p> <p>Distribution automation within substations involves monitoring and controlling equipment in distribution substations to enhance power system reliability and efficiency. Different types of equipment are monitored and controlled:</p> <p>Distribution supervisory control and data acquisition (SCADA) system monitors distribution equipment in substations</p> <p>Supervisory control on substation distribution equipment</p> <p>Substation protection equipment performs system protection actions</p> <p>Reclosers in substations</p>		
<p>Smart Grid Characteristics</p> <ul style="list-style-type: none"> • Provides power quality for the range of needs in a digital economy • Optimizes asset utilization and operating efficiency • Anticipates and responds to system disturbances in a self-correcting manner 	<p>Cyber Security Objectives/Requirements</p> <ul style="list-style-type: none"> • Integrity of distribution control commands is critical for distribution operations, avoiding outages, and providing power to customers reliably and efficiently • Availability for control is critical, while monitoring individual equipment is less critical • Confidentiality is not very important 	<p>Potential Stakeholder Issues</p> <ul style="list-style-type: none"> • Customer safety • Device standards • Cyber Security

Category: Distribution Automation		Overall Use Case #23
Scenario: DA Using Local Automation		
<p><u>Category Description</u></p> <p>A broad definition of “distribution automation” includes any automation that is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources, and automated interfaces with end-users.</p> <p>No one approach is optimal for a utility or its customers. Certain distribution automation functions, such as optimal volt/VAR control, can be more beneficial to one utility or even a few feeders in one utility, while other distribution automation functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.</p> <p>Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.</p>		
<p><u>Scenario Description</u></p> <p>Local automation of feeder equipment consists of power equipment that is managed locally by computer-based controllers that are preset with various parameters to issue control actions. These controllers may just monitor power system measurements locally, or may include some short range communications to other controllers and/or local field crews. However, in these scenarios, no communications exist between the feeder equipment and the control center.</p> <p>Local automated switch management</p> <p>Local volt/VAR control</p> <p>Local Field crew communications to underground network equipment</p>		
<p><u>Smart Grid Characteristics</u></p> <ul style="list-style-type: none"> • Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances 	<p><u>Cyber Security Objectives/Requirements</u></p> <ul style="list-style-type: none"> • Integrity of distribution control commands is critical for distribution operations, avoiding outages, and providing power to customers reliably and efficiently • Availability for control is critical, while monitoring individual equipment is less critical • Confidentiality is not very important 	<p><u>Potential Stakeholder Issues</u></p> <ul style="list-style-type: none"> • Customer safety • Customer device standards • Demand response acceptance by customers

Category: Distribution Automation		Overall Use Case #24
Scenario: DA Monitoring and Controlling Feeder Equipment		
<p><u>Category Description</u></p> <p>A broad definition of “distribution automation” includes any automation that is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources, and automated interfaces with end-users.</p> <p>No one approach is optimal for a utility or its customers. Certain distribution automation functions, such as optimal volt/VAR control, can be more beneficial to one utility or even a few feeders in one utility, while other distribution automation functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.</p> <p>Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.</p>		
<p><u>Scenario Description</u></p> <p>Operators and distribution applications can monitor the equipment on the feeders and determine whether any actions should be taken to increase reliability, improve efficiency, or respond to emergencies. For instance, they can—</p> <ul style="list-style-type: none"> Remotely open or close automated switches Remotely switch capacitor banks in and out Remotely raise or lower voltage regulators Block local automated actions Send updated parameters to feeder equipment Interact with equipment in underground distribution vaults Retrieve power system information from smart meters Automate emergency response Provide dynamic rating of feeders 		
<p><u>Smart Grid Characteristics</u></p> <ul style="list-style-type: none"> • Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances 	<p><u>Cyber Security Objectives/Requirements</u></p> <ul style="list-style-type: none"> • Integrity of distribution control commands is critical for distribution operations, avoiding outages, and providing power to customers reliably and efficiently • Availability for control is critical, while monitoring individual equipment is less critical • Confidentiality is not very important 	<p><u>Potential Stakeholder Issues</u></p> <ul style="list-style-type: none"> • Customer safety • Customer device standards • Demand response acceptance by customers

Category: Distribution Automation		Overall Use Case #25
Scenario: Fault Detection, Isolation, and Restoration		
<p><u>Category Description</u></p> <p>A broad definition of “distribution automation” includes any automation that is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources, and automated interfaces with end-users.</p> <p>No one approach is optimal for a utility or its customers. Certain distribution automation functions, such as optimal volt/VAR control, can be more beneficial to one utility or even a few feeders in one utility, while other distribution automation functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.</p> <p>Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.</p>		
<p><u>Scenario Description</u></p> <p>AMI smart meters and distribution automated devices can detect power outages that affect individual customers and larger groups of customers. As customers rely more fundamentally on power (e.g., PEV) and become used to not having to call in outages, outage detection, and restoration will become increasingly critical.</p> <p>The automated fault location, isolation, and restoration (FLIR) function uses the combination of the power system model with the SCADA data from the field on real-time conditions to determine where a fault is probably located by undertaking the following steps:</p> <p>Determines the faults cleared by controllable protective devices:</p> <p>Determines the faulted sections based on SCADA fault indications and protection lockout signals</p> <p>Estimates the probable fault locations based on SCADA fault current measurements and real-time fault analysis</p> <p>Determines the fault-clearing non-monitored protective device</p> <p>Uses closed-loop or advisory methods to isolate the faulted segment</p> <p>Once the fault is isolated, it determines how best to restore service to unfaulted segments through feeder reconfiguration.</p>		
<p><u>Smart Grid Characteristics</u></p> <ul style="list-style-type: none"> • Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances 	<p><u>Cyber Security Objectives/Requirements</u></p> <ul style="list-style-type: none"> • Integrity of outage information is critical • Availability to detect large-scale outages usually involve multiple sources of information • Confidentiality is not very important 	<p><u>Potential Stakeholder Issues</u></p> <ul style="list-style-type: none"> • Customer safety • Customer device standards • Demand response acceptance by customers

Category: Distribution Automation		Overall Use Case #26
Scenario: Load Management		
<p><u>Category Description</u></p> <p>A broad definition of “distribution automation” includes any automation that is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources, and automated interfaces with end-users.</p> <p>No one approach is optimal for a utility or its customers. Certain distribution automation functions, such as optimal volt/VAR control, can be more beneficial to one utility or even a few feeders in one utility, while other distribution automation functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.</p> <p>Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.</p>		
<p><u>Scenario Description</u></p> <p>Load management provides active and passive control by the utility of customer appliances (e.g. cycling of air conditioner, water heaters, and pool pumps) and certain C&I customer systems (e.g., plenum precooling, heat storage management).</p> <p>Direct load control and load shedding</p> <p>Demand side management</p> <p>Load shift scheduling</p> <p>Curtailement planning</p> <p>Selective load management through HANs</p>		
<p><u>Smart Grid Characteristics</u></p> <ul style="list-style-type: none"> • Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances 	<p><u>Cyber Security Objectives/Requirements</u></p> <ul style="list-style-type: none"> • Integrity of load control commands is critical to avoid unwarranted outages • Availability for load control is important – in aggregate (e.g. > 300 MW), it can be critical • Confidentiality is not very important 	<p><u>Potential Stakeholder Issues</u></p> <ul style="list-style-type: none"> • Customer safety • Customer device standards • Demand response acceptance by customers

Category: Distribution Automation		Overall Use Case #27
Scenario: Distribution Analysis using Distribution Power Flow Models		
<p><u>Category Description</u></p> <p>A broad definition of “distribution automation” includes any automation which is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources, and automated interfaces with end-users.</p> <p>No one approach is optimal for a utility or its customers. Certain distribution automation functions, such as optimal volt/VAR control, can be more beneficial to one utility or even a few feeders in one utility, while other distribution automation functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.</p> <p>Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.</p>		
<p><u>Scenario Description</u></p> <p>The brains behind the monitoring and controlling of field devices are the DA analysis software applications. These applications generally use models of the power system to validate the raw data, assess real-time and future conditions, and issue the appropriate actions. The applications may be distributed and located in the field equipment for local assessments and control, and/or may be centralized in a distribution management system (DMS) for global assessment and control.</p> <p>Local peer-to-peer interactions between equipment</p> <p>Normal distribution operations using the Distribution System Power Flow (DSPF) model</p> <p>Emergency distribution operations using the DSPF model</p> <p>Study-Mode DSPF model</p> <p>DSPF/DER model of distribution operations with significant DER generation/storage</p>		
<p><u>Smart Grid Characteristics</u></p> <ul style="list-style-type: none"> • Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances 	<p><u>Cyber Security Objectives/Requirements</u></p> <ul style="list-style-type: none"> • Integrity is critical to operate the distribution power system reliably, efficiently, and safely • Availability is critical to operate the distribution power system reliably, efficiently, and safely • Confidentiality is not important 	<p><u>Potential Stakeholder Issues</u></p> <ul style="list-style-type: none"> • Customer safety • Customer device standards • Demand response acceptance by customers

Category: Distribution Automation		Overall Use Case #28
Scenario: Distributed Energy Resources Management		
<p><u>Category Description</u></p> <p>A broad definition of “distribution automation” includes any automation which is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected DER, and automated interfaces with end-users.</p> <p>No one approach is optimal for a utility or its customers. Certain distribution automation functions, such as optimal volt/VAR control, can be more beneficial to one utility or even a few feeders in one utility, while other distribution automation functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.</p> <p>Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.</p>		
<p><u>Scenario Description</u></p> <p>In the future, more and more of generation and storage resources will be connected to the distribution network and will significantly increase the complexity and sensitivity of distribution operations. Therefore, the management of DER generation will become increasingly important in the overall management of the distribution system, including load forecasts, real-time monitoring, feeder reconfiguration, virtual and logical microgrids, and distribution planning.</p> <p>Direct monitoring and control of DER</p> <p>Shut-down or islanding verification for DER</p> <p>PEV management as load, storage, and generation resource</p> <p>Electric storage fill/draw management</p> <p>Renewable energy DER with variable generation</p> <p>Small fossil resource management, such as backup generators to be used for peak shifting</p>		
<p><u>Smart Grid Characteristics</u></p> <ul style="list-style-type: none"> • Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances 	<p><u>Cyber Security Objectives/Requirements</u></p> <ul style="list-style-type: none"> • Integrity is critical for any management/ control of generation and storage • Availability requirements may vary depending on the size (individual or aggregate) of the DER plant • Confidentiality may involve some privacy issues with customer-owned DER 	<p><u>Potential Stakeholder Issues</u></p> <ul style="list-style-type: none"> • Customer safety • Customer device standards • Demand response acceptance by customers

Category: Distribution Automation		Overall Use Case #29
Scenario: Distributed Energy Resource Management		
<p><u>Category Description</u></p> <p>A broad definition of “distribution automation” includes any automation which is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources, and automated interfaces with end-users.</p> <p>No one approach is optimal for a utility or its customers. Certain distribution automation functions, such as optimal volt/VAR control, can be more beneficial to one utility or even a few feeders in one utility, while other distribution automation functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.</p> <p>Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.</p>		
<p><u>Scenario Description</u></p> <p>Distribution planning typically uses engineering systems with access only to processed power system data that is available from the control center. It is therefore relatively self-contained.</p> <p>Operational planning</p> <p>Assessing planned outages</p> <p>Storm condition planning</p> <p>Short-term distribution planning</p> <p>Short term load forecast</p> <p>Short term DER generation and storage impact studies</p> <p>Long term distribution planning</p> <p>Long term load forecasts by area</p> <p>Optimal placements of switches, capacitors, regulators, and DER</p> <p>Distribution system upgrades and extensions</p> <p>Distribution financial planners</p>		
<p><u>Smart Grid Characteristics</u></p> <ul style="list-style-type: none"> • Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances 	<p><u>Cyber Security Objectives/Requirements</u></p> <ul style="list-style-type: none"> • Integrity not critical due to multiple sources of data • Availability is not important • Confidentiality is not important 	<p><u>Potential Stakeholder Issues</u></p> <ul style="list-style-type: none"> • Cyber security

3712 **10.3.6 PHEV Security Use Cases**

Category: Plug In Hybrid Electric Vehicles (PHEV)		Overall Use Case #30
Scenario: Customer Connects PHEV to Energy Portal		
Category Description Plug in electric vehicles will have a significant impact on the future electric system and challenge the utility and customer to manage vehicle connection and charging. As adoption rates of electric vehicles increase, the utility will have to handle the new load imposed on the electrical system. Scenarios will consider customer payment issues regarding mobility, load shifting vehicle charging, and the use of electric vehicles as a distributed resource.		
Scenario Description This scenario discusses the simple case of a customer plugging in an electric vehicle at their premise to charge its battery. Variations of this scenario will be considered that add complexity: a customer charging their vehicle at another location and providing payment or charging at another location where the premise owner pays.		
Smart Grid Characteristics <ul style="list-style-type: none"> • Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets • Provides power quality for the digital economy • Optimizes asset utilization and operate efficiently 	Objectives/Requirements <ul style="list-style-type: none"> • The customer's information is kept private • Billing information is accurate 	Potential Stakeholder Issues <ul style="list-style-type: none"> • Vehicle standards • Customer safety • Customer device standards • Demand response acceptance by customers

3713

Category: Plug In Hybrid Electric Vehicles		Overall Use Case #31
Scenario: Customer Connects PHEV to Energy Portal and Participates in "Smart" (Optimized) Charging		
<u>Category Description</u> Plug in electric vehicles will have a significant impact on the future electric system and challenge the utility and customer to manage vehicle connection and charging. As adoption rates of electric vehicles increase, the utility will have to handle the new load imposed on the electrical system. Scenarios will consider customer payment issues regarding mobility, load shifting vehicle charging, and the use of electric vehicles as a distributed resource.		
<u>Scenario Description</u> In addition to simply plugging in an electric vehicle for charging, in this scenario the electric vehicle charging is optimized to take advantage of lower rates or help prevent excessive load peaks on the electrical system.		
<u>Smart Grid Characteristics</u>	<u>Objectives/Requirements</u>	<u>Potential Stakeholder Issues</u>
<ul style="list-style-type: none"> • Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets • Provides power quality for the digital economy • Optimizes asset utilization and operate efficiently 	<ul style="list-style-type: none"> • Customer information is kept private 	<ul style="list-style-type: none"> • Vehicle standards • Customer safety • Customer device standards • Demand response acceptance by customers

3714

Category: Plug In Hybrid Electric Vehicles		Overall Use Case #32
Scenario: PHEV or Customer Receives and Responds to Discrete Demand Response Events		
<u>Category Description</u> Plug in electric vehicles will have a significant impact on the future electric system and challenge the utility and customer to manage vehicle connection and charging. As adoption rates of electric vehicles increase, the utility will have to handle the new load imposed on the electrical system. Scenarios will consider customer payment issues regarding mobility, load shifting vehicle charging, and the use of electric vehicles as a distributed resource.		
<u>Scenario Description</u> An advanced scenario for electric vehicles is the use of the vehicle to provide energy stored in its battery back to the electrical system. Customers could participate in demand response programs where they are provided an incentive to allow the utility to request power from the vehicle at times of high system load.		
<u>Smart Grid Characteristics</u>	<u>Objectives/Requirements</u>	<u>Potential Stakeholder Issues</u>
<ul style="list-style-type: none"> • Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets • Provides power quality for the digital economy • Optimizes asset utilization and operate efficiently 	<ul style="list-style-type: none"> • Improved system stability and availability • To keep customer information private • To insure DR messages are accurate and trustworthy 	<ul style="list-style-type: none"> • Vehicle standards • Customer safety • Customer device standards • Demand response acceptance by customers

3715

Category: Plug In Hybrid Electric Vehicles		Overall Use Case #33
Scenario: PHEV or Customer Receives and Responds to Utility Price Signals		
<u>Category Description</u> Plug in electric vehicles will have a significant impact on the future electric system and challenge the utility and customer to manage vehicle connection and charging. As adoption rates of electric vehicles increase, the utility will have to handle the new load imposed on the electrical system. Scenarios will consider customer payment issues regarding mobility, load shifting vehicle charging, and the use of electric vehicles as a distributed resource.		
<u>Scenario Description</u> In this scenario, the electric vehicle is able to receive and act on electricity pricing data sent from the utility. The use of pricing data for charging is primarily covered in another scenario. The pricing data can also be used in support of a distributed resource program where the customer allows the vehicle to provide power to the electric grid based on market conditions.		
<u>Smart Grid Characteristics</u>	<u>Objectives/Requirements</u>	<u>Potential Stakeholder Issues</u>
<ul style="list-style-type: none"> • Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets • Provides power quality for the digital economy • Optimizes asset utilization and operate efficiently 	<ul style="list-style-type: none"> • Improved system stability and availability • Pricing signals are accurate and trustworthy • Customer information is kept private 	<ul style="list-style-type: none"> • Vehicle standards • Customer safety • Customer device standards • Demand response acceptance by customers

3716

3717 **10.3.7 Distributed Resources Security Use Cases**

Category: Distributed Resources		Overall Use Case #34
Scenario: Customer Provides Distributed Resource		
Category Description Traditionally, distributed resources have served as a primary or emergency backup energy source for customers that place a premium on reliability and power quality. Distributed resources include generation and storage devices that can provide power back to the electric power system. Societal, policy, and technological changes are increasing the adoption rate of distributed resources, and Smart Grid technologies can enhance the value of these systems.		
Scenario Description This scenario describes the process of connecting a distributed resource to the electric power system and the requirements of net metering.		
Smart Grid Characteristics <ul style="list-style-type: none"> • Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets • Provides power quality for the digital economy • Optimizes asset utilization and operate efficiently 	Objectives/Requirements <ul style="list-style-type: none"> • Customer information is kept private • Net metering is accurate and timely 	Potential Stakeholder Issues <ul style="list-style-type: none"> • Safety • Customer data privacy and security

3718

Category: Distributed Resources		Overall Use Case #35	
Scenario: Utility Controls Customer's Distributed Resource			
<u>Category Description</u>			
<p>Traditionally, distributed resources have served as a primary or emergency backup energy source for customers that place a premium on reliability and power quality. Distributed resources include generation and storage devices that can provide power back to the electric power system. Societal, policy, and technological changes are increasing the adoption rate of distributed resources, and Smart Grid technologies can enhance the value of these systems.</p>			
<u>Scenario Description</u>			
<p>Distributed generation and storage can be used as a demand response resource where the utility can request or control devices to provide energy back to the electrical system. Customers enroll in utility programs that allow their distributed resource to be used for load support or to assist in maintaining power quality. The utility programs can be based on direct control signals or pricing information.</p>			
<u>Smart Grid Characteristics</u>		<u>Cyber Security Objectives/Requirements</u>	<u>Potential Stakeholder Issues</u>
<ul style="list-style-type: none"> • Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets • Provides power quality for the digital economy • Optimizes asset utilization and operate efficiently 		<ul style="list-style-type: none"> • Commands are trustworthy and accurate • Customer's data is kept private • DR messages are received timely 	<ul style="list-style-type: none"> • Safety • Customer data privacy and security

3719

3720 **10.3.8 Transmission Resources Security Use Cases**

Category: Transmission Operations		Overall Use Case #36
Scenario: Real-Time Normal Transmission Operations Using Energy Management System (EMS) Applications and SCADA Data		
<p>Category Description</p> <p>Transmission operations involve monitoring and controlling the transmission system using the SCADA system to monitor and control equipment in transmission substations. The EMS assesses the state of the transmission system using applications typically based on transmission power flow models. The SCADA/EMS is located in the utility’s control center, while the key equipment is located in the transmission substations. Protective relaying equipment monitors the health of the transmission system and takes corrective action within a few milliseconds, such as tripping circuit breakers if power system anomalies are detected.</p>		
<p>Scenario Description</p> <p>Transmission normal real-time operations involve monitoring and controlling the transmission system using the SCADA and EMS. The types of information exchanged include—</p> <p>Monitored equipment states (open/close), alarms (overheat, overload, battery level, capacity), and measurements (current, voltage, frequency, energy)</p> <p>Operator command and control actions, such as supervisory control of switching operations, setup/options of EMS functions, and preparation for storm conditions</p> <p>Closed-loop actions, such as protective relaying tripping circuit breakers upon power system anomalies</p> <p>Automation system controls voltage, VAR, and power flow based on algorithms, real-time data, and network linked capacitive and reactive components</p>		
<p>Smart Grid Characteristics</p> <ul style="list-style-type: none"> • Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances 	<p>Cyber Security Objectives/Requirements</p> <ul style="list-style-type: none"> • Integrity is vital to the safety and reliability of the transmission system • Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g., 1 s) • Confidentiality is not important 	<p>Potential Stakeholder Issues</p> <ul style="list-style-type: none"> • Customer safety • Customer device standards • Demand response acceptance by customers

3721

Category: Transmission Operations		Overall Use Case #37
Scenario: EMS Network Analysis Based on Transmission Power Flow Models		
<p><u>Category Description</u></p> <p>Transmission operations involve monitoring and controlling the transmission system using the SCADA system to monitor and control equipment in transmission substations. The EMS assesses the state of the transmission system using applications typically based on transmission power flow models. The SCADA/EMS is located in the utility's control center, while the key equipment is located in the transmission substations. Protective relaying equipment monitors the health of the transmission system and takes corrective action within a few milliseconds, such as tripping circuit breakers if power system anomalies are detected.</p>		
<p><u>Scenario Description</u></p> <p>EMS assesses the state of the transmission power system using the transmission power system analysis models and the SCADA data from the transmission substations</p> <p>EMS performs model update, state estimation, bus load forecast</p> <p>EMS performs contingency analysis, recommends preventive and corrective actions</p> <p>EMS performs optimal power flow analysis, recommends optimization actions</p> <p>EMS or planners perform stability study of network</p> <p>Exchange power system model information with RTOs/ISOs and/or other utilities</p>		
<p><u>Smart Grid Characteristics</u></p> <ul style="list-style-type: none"> • Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances 	<p><u>Cyber Security Objectives/Requirements</u></p> <ul style="list-style-type: none"> • Integrity is vital to the reliability of the transmission system • Availability is critical to react to contingency situations via operator commands (e.g. one second) • Confidentiality is not important 	<p><u>Potential Stakeholder Issues</u></p> <ul style="list-style-type: none"> • Cyber Security

3722

Category: Transmission Operations		Overall Use Case #38
Scenario: Real-Time Emergency Transmission Operations		
<u>Category Description</u>		
<p>Transmission operations involve monitoring and controlling the transmission system using the SCADA system to monitor and control equipment in transmission substations. The EMS assesses the state of the transmission system using applications typically based on transmission power flow models. The SCADA/EMS is located in the utility's control center, while the key equipment is located in the transmission substations. Protective relaying equipment monitors the health of the transmission system and takes corrective action within a few milliseconds, such as tripping circuit breakers if power system anomalies are detected.</p>		
<u>Scenario Description</u>		
<p>During emergencies, the power system takes some automated actions and the operators can also take actions:</p> <p>Power System Protection: Emergency operations handles under-frequency load/generation shedding, under-voltage load shedding, load tap changer (LTC) control/blocking, shunt control, series compensation control, system separation detection, and wide area real-time instability recovery</p> <p>Operators manage emergency alarms</p> <p>SCADA system responds to emergencies by running key applications such as disturbance monitoring analysis (including fault location), dynamic limit calculations for transformers and breakers based on real-time data from equipment monitors, and pre-arming of fast acting emergency automation</p> <p>SCADA/EMS generates signals for emergency support by distribution utilities (according to the T&D contracts):</p> <p>Operators performs system restorations based on system restoration plans prepared (authorized) by operation management</p>		
<u>Smart Grid Characteristics</u>	<u>Cyber Security Objectives/Requirements</u>	<u>Potential Stakeholder Issues</u>
<ul style="list-style-type: none"> • Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances 	<ul style="list-style-type: none"> • Integrity is vital to the safety and reliability of the transmission system • Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g., 1 s) • Confidentiality is not important 	<ul style="list-style-type: none"> • Customer safety • Customer device standards • Demand response acceptance by customers

3723
3724

Category: Transmission Operations		
Scenario: Wide Area Synchro-Phasor System		
<p><u>Category Description</u></p> <p>Transmission operations involve monitoring and controlling the transmission system using the SCADA system to monitor and control equipment in transmission substations. The EMS assesses the state of the transmission system using applications typically based on transmission power flow models. The SCADA/EMS is located in the utility's control center, while the key equipment is located in the transmission substations. Protective relaying equipment monitors the health of the transmission system and takes corrective action within a few milliseconds, such as tripping circuit breakers if power system anomalies are detected.</p>		
<p><u>Scenario Description</u></p> <p>The wide area synchrophasor system provides synchronized and time-tagged voltage and current phasor measurements to any protection, control, or monitoring function that requires measurements taken from several locations, whose phase angles are measured against a common, system-wide reference. Present day implementation of many protection, control, or monitoring functions is hobbled by not having access to the phase angles between local and remote measurements. With system-wide phase angle information, they can be improved and extended. The essential concept behind this system is the system-wide synchronization of measurement sampling clocks to a common time reference.</p>		
<p><u>Smart Grid Characteristics</u></p> <ul style="list-style-type: none"> • Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances 	<p><u>Cyber Security Objectives/Requirements</u></p> <ul style="list-style-type: none"> • Integrity is vital to the safety and reliability of the transmission system • Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g., 1 s) • Confidentiality is not important 	<p><u>Potential Stakeholder Issues</u></p> <ul style="list-style-type: none"> • Cyber Security • Customer data privacy and security

3727 **10.3.9 RTO/ISO Operations Security Use Cases**

Category: RTO/ISO Operations		
Scenario: RTO/ISO Management of Central and DER Generators and Storage		
Category Description TBD		
Scenario Description RTOs and ISOs manage the scheduling and dispatch of central and distributed generation and storage. These functions include— Real-time scheduling with the RTO/ISO (for nonmarket generation/storage) Real-time commitment to RTO/ISO Real-time dispatching by RTO/ISO for energy and ancillary services Real-time plant operations in response to RTO/ISO dispatch commands Real-time contingency and emergency operations Black start (system restoration after blackout) Emissions monitoring and control		
Smart Grid Characteristics <ul style="list-style-type: none"> • Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances 	Cyber Security Objectives/Requirements <ul style="list-style-type: none"> • Integrity is vital to the safety and reliability of the transmission system • Availability is critical to operator commands (e.g. one second) • Confidentiality is not important 	Potential Stakeholder Issues <ul style="list-style-type: none"> • Cyber Security • Customer data privacy and security

3728

3729 **10.3.10 Asset Management Security Use Cases**

Category: Asset Management		
Scenario: Utility Gathers Circuit and/or Transformer Load Profiles		
<p><u>Category Description</u></p> <p>At a high level, asset management seeks a balance between asset performance, cost, and risk to achieve the utilities business objectives. A wide range of conventional functions, models, applications, devices, methodologies, and tools may be deployed to effectively plan, select, track, utilize, control, monitor, maintain, and protect utility assets.</p> <p>For our purposes we will establish the scope for the asset management category to be the use of specific applications and devices by utility staff, such as condition monitoring equipment, protection equipment, event recorders, computer-based maintenance management systems (CMMS), display applications, ratings databases, analysis applications, and data marts (historians).</p>		
<p><u>Scenario Description</u></p> <p>Load profile data is important for the utility planning staff and is also used by the asset management team that is monitoring the utilization of the assets and by the SCADA/EMS and system operations team. This scenario involves the use of field devices that measure loading, the communications network that delivers the data, the historian database, and the load profile application and display capability that is either separate or an integrated part of the SCADA/EMS.</p> <p>Load profile data may also be used by automatic switching applications that use load data to ensure new system configurations do not cause overloads.</p>		
<p><u>Smart Grid Characteristics</u></p> <p>Provides power quality for the range of needs in a digital economy</p> <p>Optimizes asset utilization and operating efficiency</p> <p>Anticipates and responds to system disturbances in a self-correcting manner</p>	<p><u>Objectives/Requirements</u></p> <p>Data is accurate (integrity)</p> <p>Data is provided timely</p> <p>Customer data is kept private</p>	<p><u>Potential Stakeholder Issues</u></p> <p>Customer data privacy and security</p> <p>Cyber Security</p>

Category: Asset Management		
Scenario: Utility Makes Decisions on Asset Replacement Based on a Range of Inputs Including Comprehensive Offline and Online Condition Data and Analysis Applications		
<p><u>Category Description</u></p> <p>At a high level, asset management seeks a balance between asset performance, cost, and risk to achieve the utilities business objectives. A wide range of conventional functions, models, applications, devices, methodologies, and tools may be deployed to effectively plan, select, track, utilize, control, monitor, maintain, and protect utility assets.</p> <p>For our purposes we will establish the scope for the asset management category to be the use of specific applications and devices by utility staff such as condition monitoring equipment, protection equipment, event recorders, CMMS, display applications, ratings databases, analysis applications and data marts (historians).</p>		
<p><u>Scenario Description</u></p> <p>When decisions on asset replacement become necessary, the system operator, asset management, apparatus engineering, and maintenance engineering staff work closely together with the objective of maximizing the life and utilization of the asset while avoiding an unplanned outage and damage to the equipment.</p> <p>This scenario involves the use of online condition monitoring devices for the range of assets monitored, offline test results, mobile work force technologies, the communications equipment used to collect the online data, data marts (historian databases) to store and trend data as well as condition analysis applications, CMMS applications, display applications, and SCADA/EMS.</p>		
<p><u>Smart Grid Characteristics</u></p> <p>Provides power quality for the range of needs in a digital economy</p> <p>Optimizes asset utilization and operating efficiency</p> <p>Anticipates and responds to system disturbances in a self-correcting manner</p>	<p><u>Objectives/Requirements</u></p> <p>Data provided is accurate and trustworthy</p> <p>Data is provided timely</p>	<p><u>Potential Stakeholder Issues</u></p> <p>Cyber Security</p> <p>Customer data privacy and security</p>

Category: Asset Management		
Scenario: Utility Performs Localized Load Reduction to Relieve Circuit and/or Transformer Overloads		
<p><u>Category Description</u></p> <p>At a high level, asset management seeks a balance between asset performance, cost, and risk to achieve the utilities business objectives. A wide range of conventional functions, models, applications, devices, methodologies, and tools may be deployed to effectively plan, select, track, utilize, control, monitor, maintain, and protect utility assets.</p> <p>For our purposes we will establish the scope for the asset management category to be the use of specific applications and devices by utility staff, such as condition monitoring equipment, protection equipment, event recorders, CMMS, display applications, ratings databases, analysis applications, and data marts (historians).</p> <p>Advanced functions that are associated with asset management include dynamic rating and end of life estimation.</p>		
<p><u>Scenario Description</u></p> <p>Transmission capacity can become constrained due to a number of system-level scenarios and result in an overload situation on lines and substation equipment. Circuit and/or transformer overloads at the distribution level can occur when higher than anticipated customer loads are placed on a circuit or when operator or automatic switching actions are implemented to change the network configuration.</p> <p>Traditional load reduction systems are used to address generation shortfalls and other system-wide issues. Localized load reduction can be a key tool enabling the operator to temporarily curtail the load in a specific area to reduce the impact on specific equipment. This scenario describes the integrated use of the AMI system, the demand response system, other load reduction systems, and the SCADA/EMS to achieve this goal.</p>		
<p><u>Smart Grid Characteristics</u></p> <p>Provides power quality for the range of needs in a digital economy</p> <p>Optimizes asset utilization and operating efficiency</p> <p>Anticipates and responds to system disturbances in a self-correcting manner</p>	<p><u>Objectives/Requirements</u></p> <p>Load reduction messages are accurate and trustworthy</p> <p>Customer's data is kept private</p> <p>DR messages are received and processed timely</p>	<p><u>Potential Stakeholder Issues</u></p> <p>Demand response acceptance by customers</p> <p>Customer data privacy and security</p> <p>Retail Electric Supplier access</p> <p>Customer data access</p>

Category: Asset Management		
Scenario: Utility System Operator Determines Level of Severity for an Impending Asset Failure and Takes Corrective Action		
<p><u>Category Description</u></p> <p>At a high level, asset management seeks a balance between asset performance, cost, and risk to achieve the utilities business objectives. A wide range of conventional functions, models, applications, devices, methodologies, and tools may be deployed to effectively plan, select, track, utilize, control, monitor, maintain, and protect utility assets.</p> <p>For our purposes we will establish the scope for the asset management category to be the use of specific applications and devices by utility staff, such as condition monitoring equipment, protection equipment, event recorders, CMMS, display applications, ratings databases, analysis applications, and data marts (historians).</p>		
<p><u>Scenario Description</u></p> <p>When pending asset failure can be anticipated, the system operator, asset management, apparatus engineering, and maintenance engineering staff work closely together with the objective of avoiding an unplanned outage while avoiding further damage to the equipment.</p> <p>This scenario involves the use of online condition monitoring devices for the range of assets monitored, offline test results, mobile workforce technologies, the communications equipment used to collect the online data, data marts (historian databases) to store, and trend data, as well as condition analysis applications, CMMS applications, display applications, and SCADA/EMS.</p>		
<p><u>Smart Grid Characteristics</u></p> <p>Provides power quality for the range of needs in a digital economy</p> <p>Optimizes asset utilization and operating efficiency</p> <p>Anticipates and responds to system disturbances in a self-correcting manner</p>	<p><u>Objectives/Requirements</u></p> <p>Asset information provided is accurate and trustworthy</p> <p>Asset information is provided timely</p>	<p><u>Potential Stakeholder Issues</u></p> <p>Cyber security</p> <p>Customer data privacy and security</p>

3732
3733
3734

3735 **APPENDIX H:**
3736 **LOGICAL ARCHITECTURE AND INTERFACES OF**
3737 **THE SMART GRID**

3738
3739 The following subsection refers to detailed logical interfaces including both diagrams and tables
3740 that allocate the logical interfaces to one of the logical interface categories.¹⁵

3741 **H.1 ADVANCED METERING INFRASTRUCTURE**

3742 The advanced metering infrastructure (AMI) consists of the communications hardware and
3743 software, together with the associated system and data management software, that creates a bi-
3744 directional network between advanced metering equipment and utility business systems,
3745 enabling collection and distribution of information to customers and other parties, such as
3746 competitive retail suppliers or the utility itself. AMI provides customers with real-time (or near-
3747 real-time) pricing of electricity and may help utilities achieve necessary load reductions. **Error!**
3748 **Reference source not found.** diagrams the AMI, and Table H-1 lists the AMI logical interfaces
3749 by category.

¹⁵ Please note that during development, logical interface 23 was deleted. Subsequent interfaces were not renumbered due to the amount of development already done at that time. It is expected that this will be resolved in the next version of this document.

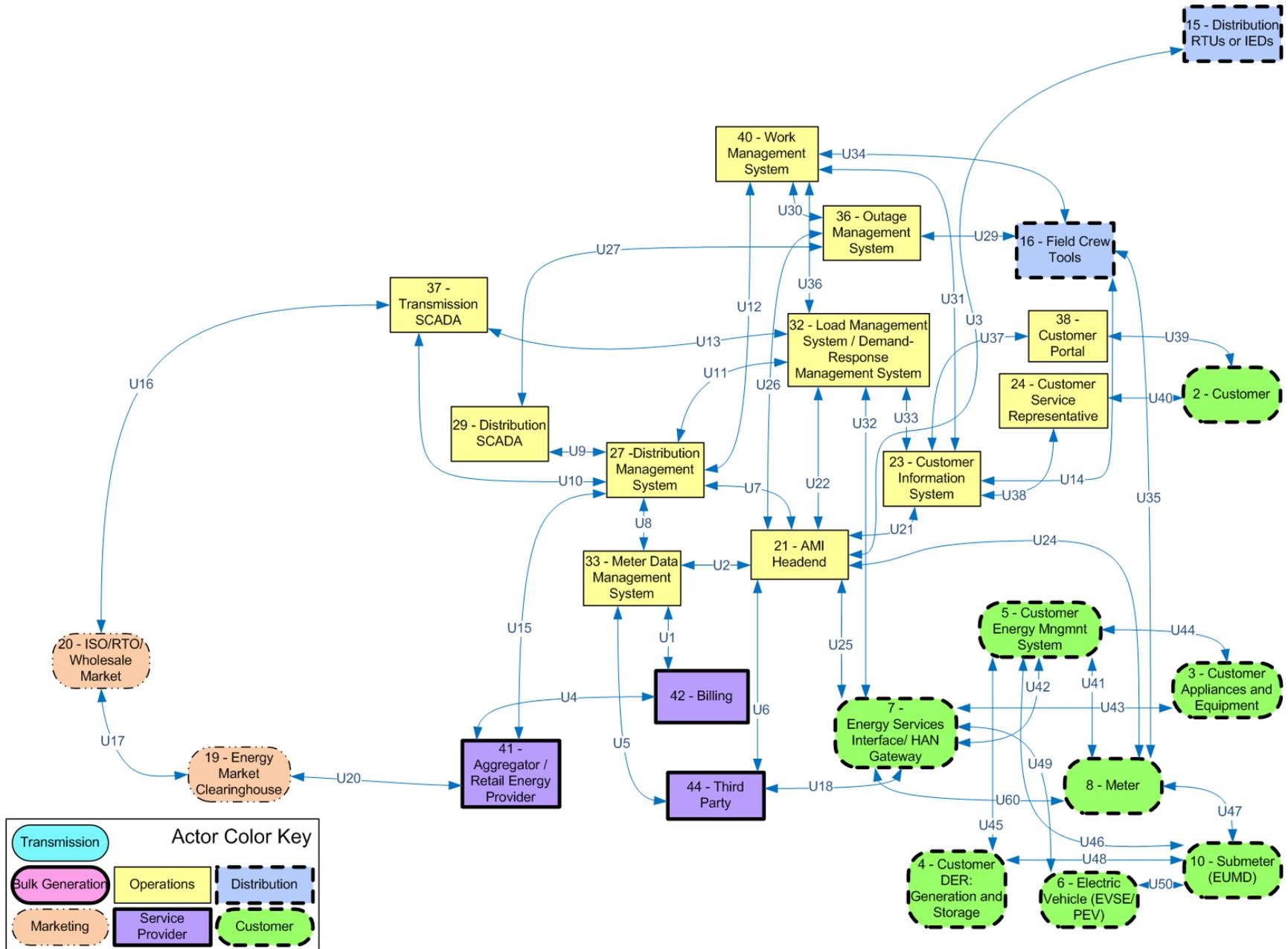


Figure H-1 Advanced Metering Infrastructure

Table H-1 AMI Logical Interfaces by Logical Interface Category

Logical Interface Category	Logical Interfaces
1. Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints, for example: <ul style="list-style-type: none"> • Between transmission SCADA and substation equipment • Between distribution SCADA and high priority substation and pole-top equipment • Between SCADA and DCS within a power plant 	U3, U28
2. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints, for example: <ul style="list-style-type: none"> • Between distribution SCADA and lower priority pole-top equipment • Between pole-top IEDs and other pole-top IEDs 	
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: <ul style="list-style-type: none"> • Between transmission SCADA and substation automation systems 	
4. Interface between control systems and equipment without high availability, without compute nor bandwidth constraints, for example: <ul style="list-style-type: none"> • Between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs 	
5. Interface between control systems within the same organization, for example: <ul style="list-style-type: none"> • Multiple DMS systems belonging to the same utility • Between subsystems within DCS and ancillary control systems within a power plant 	U9, U27
6. Interface between control systems in different organizations, for example: <ul style="list-style-type: none"> • Between an RTO/ISO EMS and a utility energy management system 	U7, U10, U13, U16
7. Interface between back office systems under common management authority, for example: <ul style="list-style-type: none"> • Between a Customer Information System and a Meter Data Management System 	U2, U22, U26, U31
8. Interface between back office systems not under common management authority, for example: <ul style="list-style-type: none"> • Between a third-party billing system and a utility meter data management system 	U1, U6, U15
9. Interface with B2B ¹⁶ connections between systems usually involving financial or market transactions, for example: <ul style="list-style-type: none"> • Between a Retail aggregator and an Energy Clearinghouse 	U17, U20
10. Interface between control systems and non-control/corporate systems, for example: <ul style="list-style-type: none"> • Between a Work Management System and a Geographic Information System 	U12, U30, U33, U36

¹⁶ B2B – Business To Business

Logical Interface Category	Logical Interfaces
11. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements, for example: <ul style="list-style-type: none"> • Between a temperature sensor on a transformer and its receiver 	None
12. Interface between sensor networks and control systems, for example: <ul style="list-style-type: none"> • Between a sensor receiver and the substation master 	None
13. Interface between systems that use the AMI network, for example: <ul style="list-style-type: none"> • Between MDMS and meters • Between LMS/DRMS and Customer EMS 	U8, U21, U25, U32
14. Interface between systems that use the AMI network with high availability, for example: <ul style="list-style-type: none"> • Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment 	
15. Interface between systems that use customer (residential, commercial, and industrial) site networks which include: <ul style="list-style-type: none"> • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV¹⁷ 	U43, U44, U45, U49
16. Interface between external systems and the customer site, for example: <ul style="list-style-type: none"> • Between Third Party and HAN Gateway • Between ESP and DER • Between Customer and CIS Web site 	U18, U19, U37, U38, U39, U40
17. Interface between systems and mobile field crew laptops/equipment, for example: <ul style="list-style-type: none"> • Between field crews and GIS • Between field crews and substation equipment 	U14, U29, U34, U35
18. Interface between metering equipment, for example: <ul style="list-style-type: none"> • Between sub-meter to meter • Between PEV meter and Energy Service Provider 	U24, U41, U46, U47, U50
19. Interface between operations decision support systems, for example: <ul style="list-style-type: none"> • Between WAMS and ISO/RTO 	None
20. Interface between engineering/maintenance systems and control equipment, for example: <ul style="list-style-type: none"> • Between engineering and substation relaying equipment for relay settings • Between engineering and pole-top equipment for maintenance • Within power plants 	U11
21. Interface between control systems and their vendors for standard maintenance and service, for example: <ul style="list-style-type: none"> • Between SCADA system and its vendor 	U5, U132

¹⁷ PEV-Plug in Electric Vehicle

Logical Interface Category	Logical Interfaces
22. Interface between security/network/system management consoles and all networks and systems, for example: <ul style="list-style-type: none"> • Between a security console and network routers, firewalls, computer systems, and network nodes 	None

3752 **H.2 DISTRIBUTION GRID MANAGEMENT**

3753 Distribution grid management (DGM) focuses on maximizing the performance of feeders,
 3754 transformers, and other components of networked distribution systems and integrating with
 3755 transmission systems and customer operations. As Smart Grid capabilities such as AMI and
 3756 demand response are developed, and as large numbers of distributed energy resources and plug-
 3757 in electric vehicles (PEVs) are deployed, the automation of distribution systems becomes
 3758 increasingly more important to the efficient and reliable operation of the overall power system.
 3759 The anticipated benefits of DGM include increased reliability, reductions in peak loads and
 3760 improved capabilities for managing distributed sources of renewable energy. Figure H-2
 3761 diagrams the DGM, and Table H-2 lists the DGM logical interfaces by category.

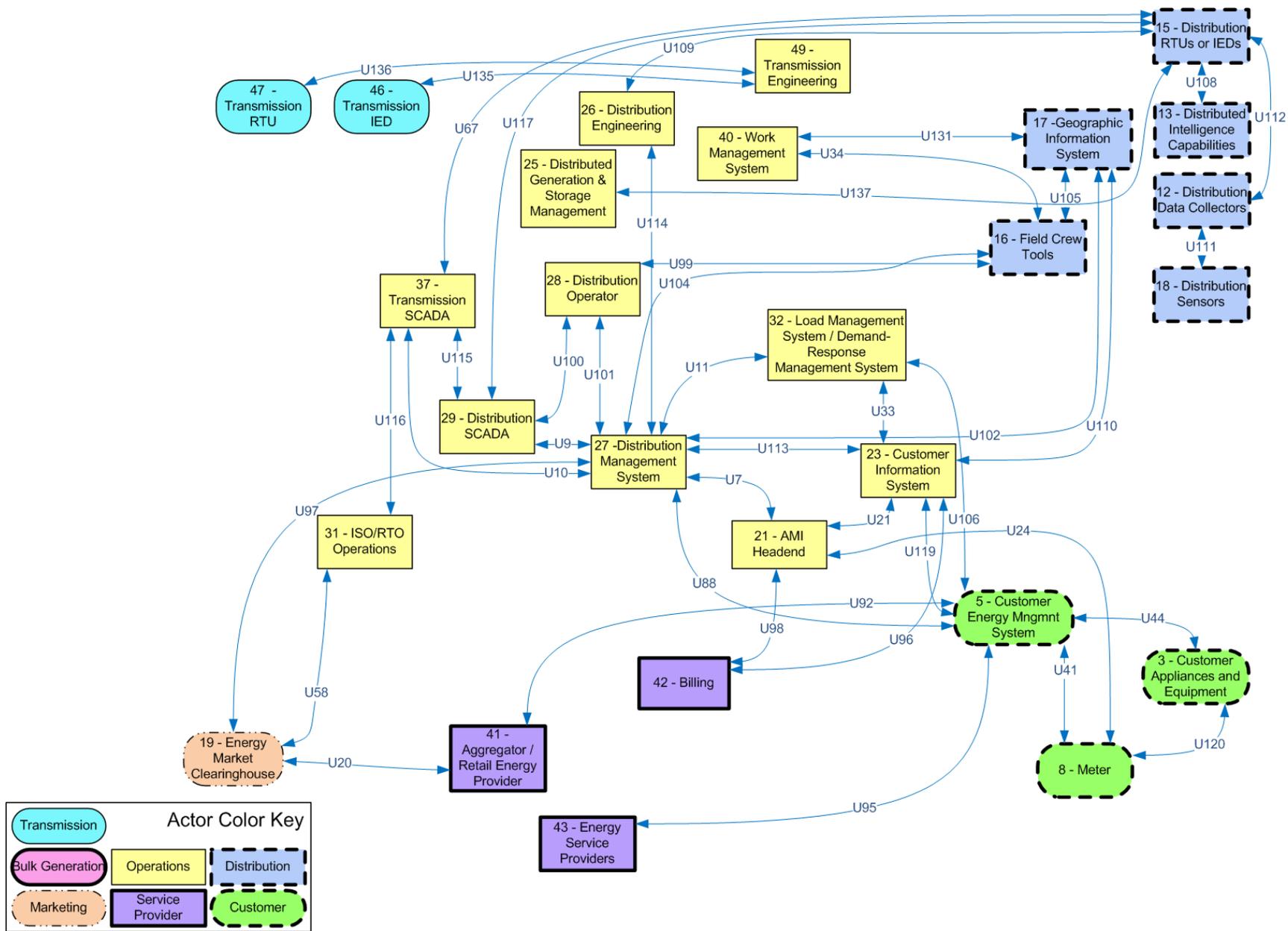


Figure H-2 Distribution Grid Management

Table H-2 DGM Logical Interfaces by Logical Interface Category

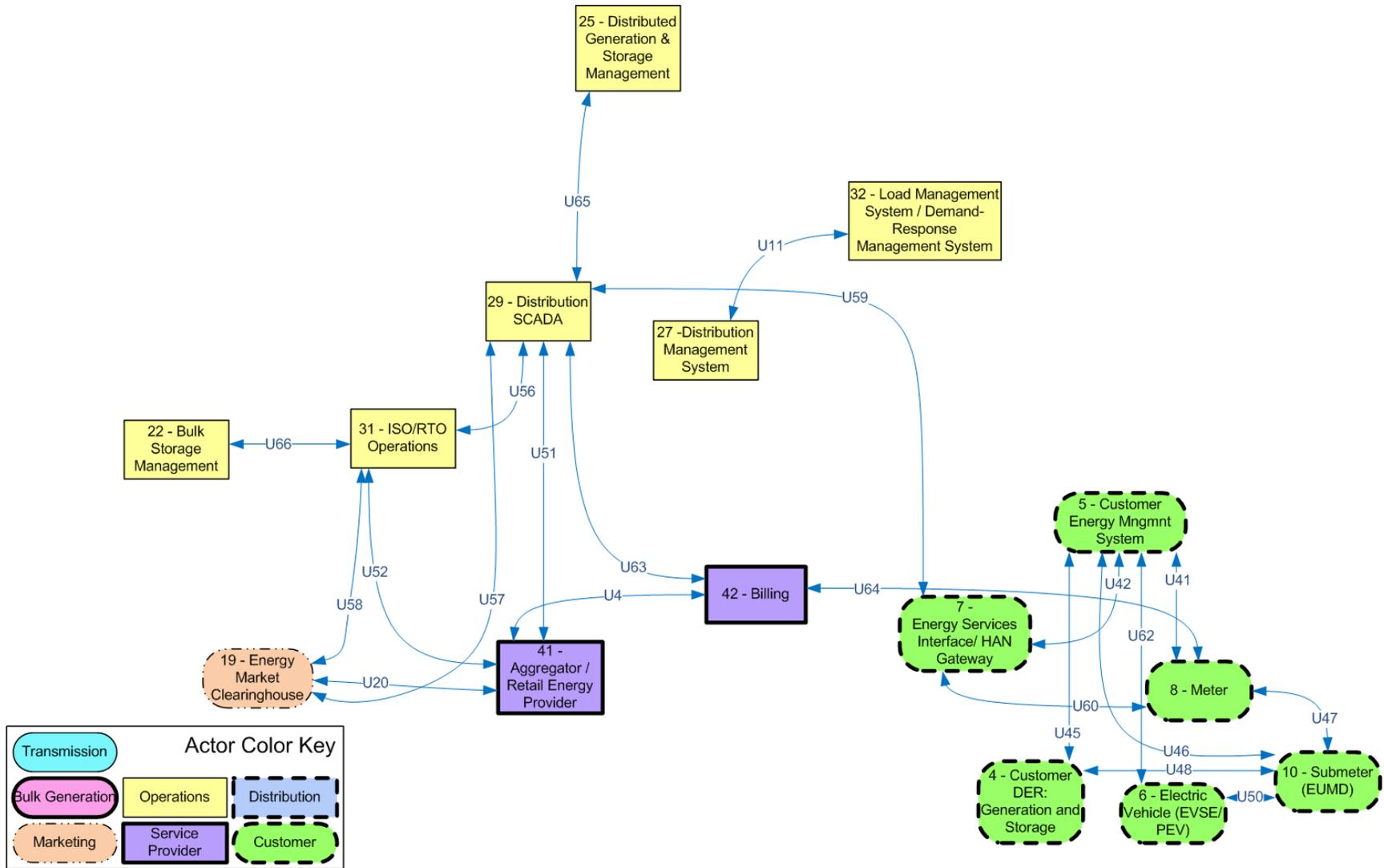
Logical Interface Category	Logical Interfaces
1. Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints, for example: <ul style="list-style-type: none"> • Between transmission SCADA and substation equipment • Between distribution SCADA and high priority substation and pole-top equipment • Between SCADA and DCS within a power plant 	U102, U117, U135, U136
2. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints, for example: <ul style="list-style-type: none"> • Between distribution SCADA and lower priority pole-top equipment • Between pole-top IEDs and other pole-top IEDs 	
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: <ul style="list-style-type: none"> • Between transmission SCADA and substation automation systems 	
4. Interface between control systems and equipment without high availability, without compute nor bandwidth constraints, for example: <ul style="list-style-type: none"> • Between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs 	
5. Interface between control systems within the same organization, for example: <ul style="list-style-type: none"> • Multiple DMS systems belonging to the same utility • Between subsystems within DCS and ancillary control systems within a power plant 	U9, U11
6. Interface between control systems in different organizations, for example: <ul style="list-style-type: none"> • Between an RTO/ISO EMS and a utility energy management system 	U7, U10, U115, U116
7. Interface between back office systems under common management authority, for example: <ul style="list-style-type: none"> • Between a Customer Information System and a Meter Data Management System 	U96, U98, U110
8. Interface between back office systems not under common management authority, for example: <ul style="list-style-type: none"> • Between a third-party billing system and a utility meter data management system 	None
9. Interface with B2B connections between systems usually involving financial or market transactions, for example: <ul style="list-style-type: none"> • Between a Retail aggregator and an Energy Clearinghouse 	U20, U58, U97
10. Interface between control systems and non-control/corporate systems, for example: <ul style="list-style-type: none"> • Between a Work Management System and a Geographic Information System 	U33, U106, U113, U114, U131
11. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements, for example: <ul style="list-style-type: none"> • Between a temperature sensor on a transformer and its receiver 	U111
12. Interface between sensor networks and control systems, for example: <ul style="list-style-type: none"> • Between a sensor receiver and the substation master 	U108, U112

Logical Interface Category	Logical Interfaces
13. Interface between systems that use the AMI network, for example: <ul style="list-style-type: none"> • Between MDMS and meters • Between LMS/DRMS and Customer EMS 	U95, U119
14. Interface between systems that use the AMI network with high availability, for example: <ul style="list-style-type: none"> • Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment 	
15. Interface between systems that use customer (residential, commercial, and industrial) site networks which include: <ul style="list-style-type: none"> • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV 	U44, U120
16. Interface between external systems and the customer site, for example: <ul style="list-style-type: none"> • Between Third Party and HAN Gateway • Between ESP and DER • Between Customer and CIS Web site 	U88, U92, U100, U101
17. Interface between systems and mobile field crew laptops/equipment, for example: <ul style="list-style-type: none"> • Between field crews and GIS • Between field crews and substation equipment 	U99, U104, U105
18. Interface between metering equipment, for example: <ul style="list-style-type: none"> • Between sub-meter to meter • Between PEV meter and Energy Service Provider 	U24, U41
19. Interface between operations decision support systems, for example: <ul style="list-style-type: none"> • Between WAMS and ISO/RTO 	None
20. Interface between engineering/maintenance systems and control equipment, for example: <ul style="list-style-type: none"> • Between engineering and substation relaying equipment for relay settings • Between engineering and pole-top equipment for maintenance • Within power plants 	U109
21. Interface between control systems and their vendors for standard maintenance and service, for example: <ul style="list-style-type: none"> • Between SCADA system and its vendor 	None
22. Interface between security/network/system management consoles and all networks and systems, for example: <ul style="list-style-type: none"> • Between a security console and network routers, firewalls, computer systems, and network nodes 	None

3765 **H.3ELECTRIC STORAGE**

3766 Electric storage (ES) is the means of storing energy either directly or indirectly. The significant
3767 bulk of energy storage technology available today is pumped hydro-electric storage hydroelectric
3768 technology. New storage capabilities, especially in the area of distributed storage, would benefit
3769 the entire grid in many aspects. Figure H-3 shows the ES diagram, and Table H-3 lists the
3770 associated ES logical interfaces by category.

Draft



3771
3772

Figure H-3 Electric Storage

Table H-3 ES Logical Interfaces by Logical Interface Category

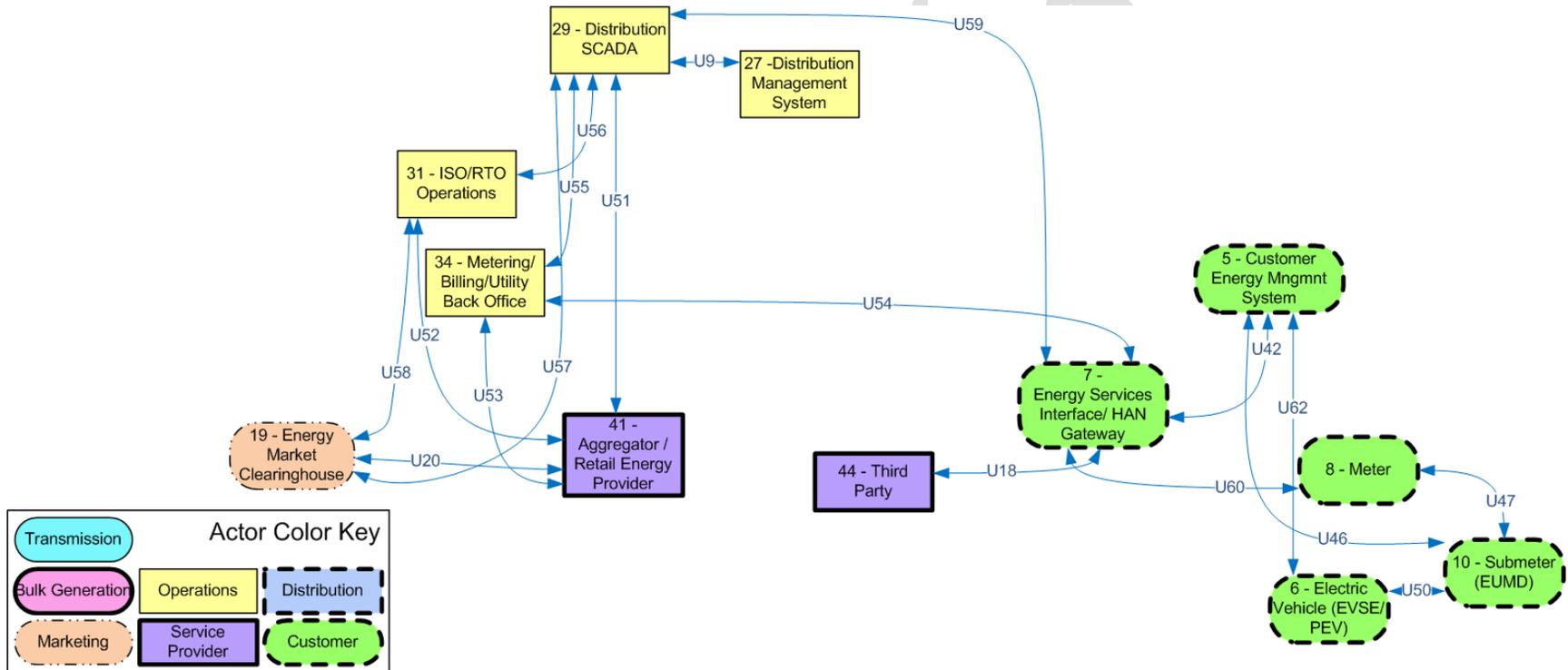
Logical Interface Category	Logical Interfaces
1. Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints, for example: <ul style="list-style-type: none"> • Between transmission SCADA and substation equipment • Between distribution SCADA and high priority substation and pole-top equipment • Between SCADA and DCS within a power plant 	None
2. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints, for example: <ul style="list-style-type: none"> • Between distribution SCADA and lower priority pole-top equipment • Between pole-top IEDs and other pole-top IEDs 	
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: <ul style="list-style-type: none"> • Between transmission SCADA and substation automation systems 	
4. Interface between control systems and equipment without high availability, without compute nor bandwidth constraints, for example: <ul style="list-style-type: none"> • Between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs 	
5. Interface between control systems within the same organization, for example: <ul style="list-style-type: none"> • Multiple DMS systems belonging to the same utility • Between subsystems within DCS and ancillary control systems within a power plant 	U65, U66
6. Interface between control systems in different organizations, for example: <ul style="list-style-type: none"> • Between an RTO/ISO EMS and a utility energy management system 	U56
7. Interface between back office systems under common management authority, for example: <ul style="list-style-type: none"> • Between a Customer Information System and a Meter Data Management System 	U63
8. Interface between back office systems not under common management authority, for example: <ul style="list-style-type: none"> • Between a third-party billing system and a utility meter data management system 	None
9. Interface with B2B connections between systems usually involving financial or market transactions, for example: <ul style="list-style-type: none"> • Between a Retail aggregator and an Energy Clearinghouse 	U4, U20, U51, U57, U58
10. Interface between control systems and non-control/corporate systems, for example: <ul style="list-style-type: none"> • Between a Work Management System and a Geographic Information System 	U59
11. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements, for example: <ul style="list-style-type: none"> • Between a temperature sensor on a transformer and its receiver 	None
12. Interface between sensor networks and control systems, for example: <ul style="list-style-type: none"> • Between a sensor receiver and the substation master 	None

Logical Interface Category	Logical Interfaces
13. Interface between systems that use the AMI network, for example: <ul style="list-style-type: none"> • Between MDMS and meters • Between LMS/DRMS and Customer EMS 	None
14. Interface between systems that use the AMI network with high availability, for example: <ul style="list-style-type: none"> • Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment 	
15. Interface between systems that use customer (residential, commercial, and industrial) site networks which include: <ul style="list-style-type: none"> • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV 	U42, U45, U62
16. Interface between external systems and the customer site, for example: <ul style="list-style-type: none"> • Between Third Party and HAN Gateway • Between ESP and DER • Between Customer and CIS Web site 	U19
17. Interface between systems and mobile field crew laptops/equipment, for example: <ul style="list-style-type: none"> • Between field crews and GIS • Between field crews and substation equipment 	None
18. Interface between metering equipment, for example: <ul style="list-style-type: none"> • Between sub-meter to meter • Between PEV meter and Energy Service Provider 	U41, U46, U47, U48, U50, U64
19. Interface between operations decision support systems, for example: <ul style="list-style-type: none"> • Between WAMS and ISO/RTO 	None
20. Interface between engineering/maintenance systems and control equipment, for example: <ul style="list-style-type: none"> • Between engineering and substation relaying equipment for relay settings • Between engineering and pole-top equipment for maintenance • Within power plants 	None
21. Interface between control systems and their vendors for standard maintenance and service, for example: <ul style="list-style-type: none"> • Between SCADA system and its vendor 	None
22. Interface between security/network/system management consoles and all networks and systems, for example: <ul style="list-style-type: none"> • Between a security console and network routers, firewalls, computer systems, and network nodes 	None

3774 **H.4ELECTRIC TRANSPORTATION**

3775 Electric transportation (ET) refers primarily to enabling large-scale integration of PEVs. Electric
 3776 transportation will significantly reduce U.S. dependence on foreign oil, increase the use of
 3777 renewable sources of energy, and dramatically reduce the nation’s carbon footprint. Figure H-4
 3778 and Table H-4 address the ET logical interfaces.

3779
3780
3781
3782
3783
3784



3785

Figure H-4 Electric Transportation

Table H-4 ET Logical Interfaces by Logical Interface Category

Logical Interface Category	Logical Interfaces
1. Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints, for example: <ul style="list-style-type: none"> • Between transmission SCADA and substation equipment • Between distribution SCADA and high priority substation and pole-top equipment • Between SCADA and DCS within a power plant 	None
2. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints, for example: <ul style="list-style-type: none"> • Between distribution SCADA and lower priority pole-top equipment • Between pole-top IEDs and other pole-top IEDs 	
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: <ul style="list-style-type: none"> • Between transmission SCADA and substation automation systems 	
4. Interface between control systems and equipment without high availability, without compute nor bandwidth constraints, for example: <ul style="list-style-type: none"> • Between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs 	
5. Interface between control systems within the same organization, for example: <ul style="list-style-type: none"> • Multiple DMS systems belonging to the same utility • Between subsystems within DCS and ancillary control systems within a power plant 	None
6. Interface between control systems in different organizations, for example: <ul style="list-style-type: none"> • Between an RTO/ISO EMS and a utility energy management system 	U56
7. Interface between back office systems under common management authority, for example: <ul style="list-style-type: none"> • Between a Customer Information System and a Meter Data Management System 	None
8. Interface between back office systems not under common management authority, for example: <ul style="list-style-type: none"> • Between a third-party billing system and a utility meter data management system 	U55
9. Interface with B2B connections between systems usually involving financial or market transactions, for example: <ul style="list-style-type: none"> • Between a Retail aggregator and an Energy Clearinghouse 	U20, U51, U52, U53, U57, U58
10. Interface between control systems and non-control/corporate systems, for example: <ul style="list-style-type: none"> • Between a Work Management System and a Geographic Information System 	U59
11. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements, for example: <ul style="list-style-type: none"> • Between a temperature sensor on a transformer and its receiver 	None

Logical Interface Category	Logical Interfaces
12. Interface between sensor networks and control systems, for example: <ul style="list-style-type: none"> • Between a sensor receiver and the substation master 	None
13. Interface between systems that use the AMI network, for example: <ul style="list-style-type: none"> • Between MDMS and meters • Between LMS/DRMS and Customer EMS 	None
14. Interface between systems that use the AMI network with high availability, for example: <ul style="list-style-type: none"> • Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment 	
15. Interface between systems that use customer (residential, commercial, and industrial) site networks which include: <ul style="list-style-type: none"> • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV 	U62
16. Interface between external systems and the customer site, for example: <ul style="list-style-type: none"> • Between Third Party and HAN Gateway • Between ESP and DER • Between Customer and CIS Web site 	U18, U19
17. Interface between systems and mobile field crew laptops/equipment, for example: <ul style="list-style-type: none"> • Between field crews and GIS • Between field crews and substation equipment 	None
18. Interface between metering equipment, for example: <ul style="list-style-type: none"> • Between sub-meter to meter • Between PEV meter and Energy Service Provider 	U46, U47, U50, U54, U60
19. Interface between operations decision support systems, for example: <ul style="list-style-type: none"> • Between WAMS and ISO/RTO 	None
20. Interface between engineering/maintenance systems and control equipment, for example: <ul style="list-style-type: none"> • Between engineering and substation relaying equipment for relay settings • Between engineering and pole-top equipment for maintenance • Within power plants 	None
21. Interface between control systems and their vendors for standard maintenance and service, for example: <ul style="list-style-type: none"> • Between SCADA system and its vendor 	None
22. Interface between security/network/system management consoles and all networks and systems, for example: <ul style="list-style-type: none"> • Between a security console and network routers, firewalls, computer systems, and network nodes 	None

3787

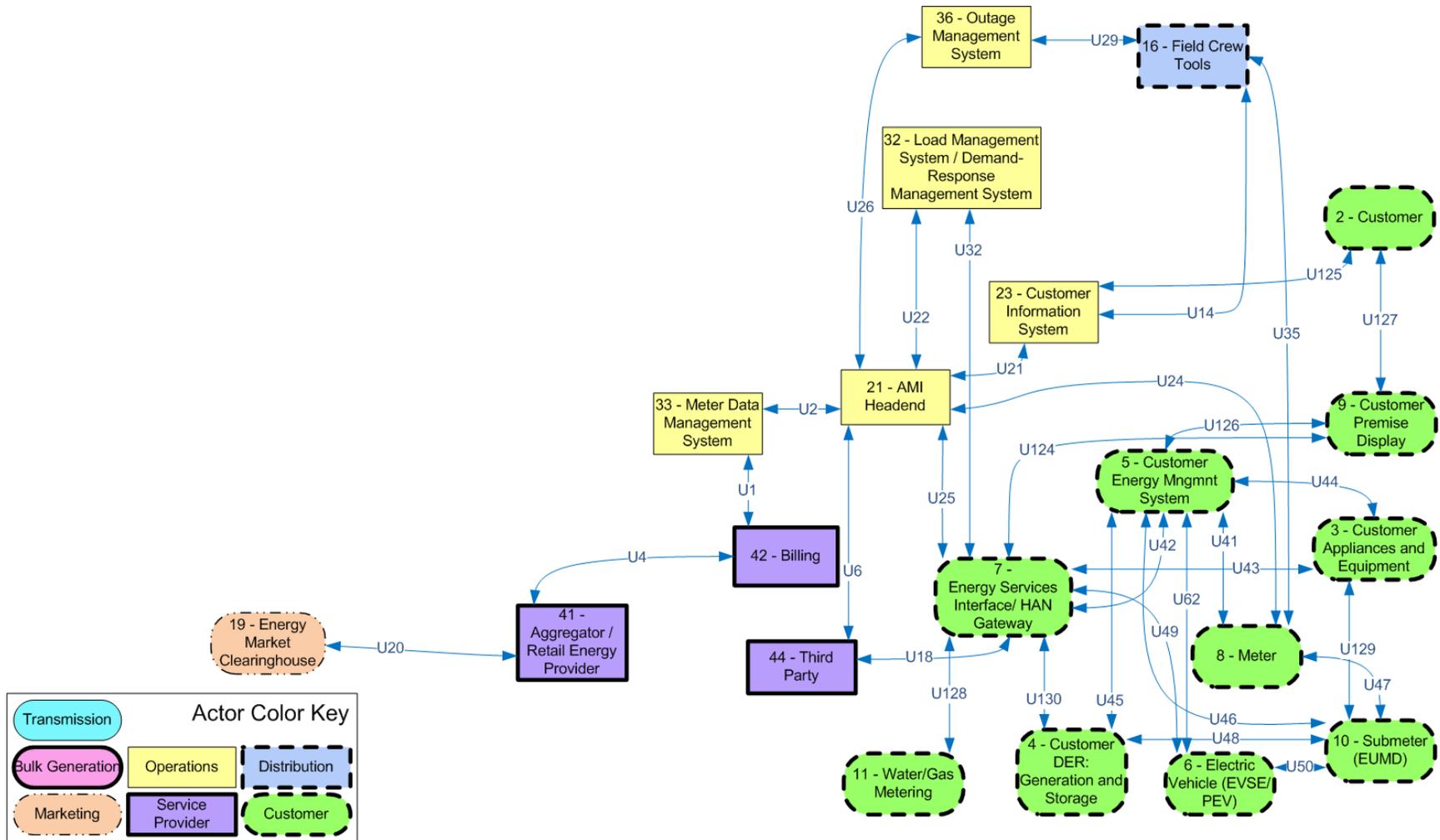
3788

3789 **H.5CUSTOMER PREMISES**

3790 The customer premises address demand response (DR) and consumer energy efficiency. This
3791 includes mechanisms and incentives for utilities, business, industrial, and residential customers
3792 to cut energy use during times of peak demand or when power reliability is at risk. Demand
3793 response is necessary for optimizing the balance of power supply and demand. Figure H-5
3794 diagrams the customer premises and Table H-5 provides the companion list of customer
3795 premises.

3796

Draft



3797

Figure H-5 Customer Premises

Table H-5 Customer Premises by Logical Interface Category

Logical Interface Category	Logical Interfaces
1. Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints, for example: <ul style="list-style-type: none"> • Between transmission SCADA and substation equipment • Between distribution SCADA and high priority substation and pole-top equipment • Between SCADA and DCS within a power plant 	None
2. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints, for example: <ul style="list-style-type: none"> • Between distribution SCADA and lower priority pole-top equipment • Between pole-top IEDs and other pole-top IEDs 	
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: <ul style="list-style-type: none"> • Between transmission SCADA and substation automation systems 	
4. Interface between control systems and equipment without high availability, without compute nor bandwidth constraints, for example: <ul style="list-style-type: none"> • Between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs 	
5. Interface between control systems within the same organization, for example: <ul style="list-style-type: none"> • Multiple DMS systems belonging to the same utility • Between subsystems within DCS and ancillary control systems within a power plant 	None
6. Interface between control systems in different organizations, for example: <ul style="list-style-type: none"> • Between an RTO/ISO EMS and a utility energy management system 	none
7. Interface between back office systems under common management authority, for example: <ul style="list-style-type: none"> • Between a Customer Information System and a Meter Data Management System 	U2, U22, U26
8. Interface between back office systems not under common management authority, for example: <ul style="list-style-type: none"> • Between a third-party billing system and a utility meter data management system 	U1
9. Interface with B2B connections between systems usually involving financial or market transactions, for example: <ul style="list-style-type: none"> • Between a Retail aggregator and an Energy Clearinghouse 	U4, U20
10. Interface between control systems and non-control/corporate systems, for example: <ul style="list-style-type: none"> • Between a Work Management System and a Geographic Information System 	None
11. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements, for example: <ul style="list-style-type: none"> • Between a temperature sensor on a transformer and its receiver 	None
12. Interface between sensor networks and control systems, for example: <ul style="list-style-type: none"> • Between a sensor receiver and the substation master 	None

Logical Interface Category	Logical Interfaces
13. Interface between systems that use the AMI network, for example: <ul style="list-style-type: none"> • Between MDMS and meters • Between LMS/DRMS and Customer EMS 	U25, U32, U130
14. Interface between systems that use the AMI network with high availability, for example: <ul style="list-style-type: none"> • Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment 	
15. Interface between systems that use customer (residential, commercial, and industrial) site networks which include: <ul style="list-style-type: none"> • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV 	U42, U43, U44, U45, U49, U62, U124, U126, U127
16. Interface between external systems and the customer site, for example: <ul style="list-style-type: none"> • Between Third Party and HAN Gateway • Between ESP and DER • Between Customer and CIS Web site 	U18, U19, U125
17. Interface between systems and mobile field crew laptops/equipment, for example: <ul style="list-style-type: none"> • Between field crews and GIS • Between field crews and substation equipment 	U14, U29, U35
18. Interface between metering equipment, for example: <ul style="list-style-type: none"> • Between sub-meter to meter • Between PEV meter and Energy Service Provider 	U24, U41, U46, U47, U48, U50, U128, U129
19. Interface between operations decision support systems, for example: <ul style="list-style-type: none"> • Between WAMS and ISO/RTO 	None
20. Interface between engineering/maintenance systems and control equipment, for example: <ul style="list-style-type: none"> • Between engineering and substation relaying equipment for relay settings • Between engineering and pole-top equipment for maintenance • Within power plants 	None
21. Interface between control systems and their vendors for standard maintenance and service, for example: <ul style="list-style-type: none"> • Between SCADA system and its vendor 	None
22. Interface between security/network/system management consoles and all networks and systems, for example: <ul style="list-style-type: none"> • Between a security console and network routers, firewalls, computer systems, and network nodes 	None

3799
3800

3801 **H.6 WIDE AREA SITUATIONAL AWARENESS**

3802 Wide area situational awareness (WASA) includes the monitoring and display of power system
3803 components and performance across interconnections and over large geographic areas in near
3804 real time. The goals of situational awareness are to understand and ultimately optimize the
3805 management of power-network components, behavior, and performance, as well as to anticipate,
3806 prevent, or respond to problems before disruptions can arise. Figure H-6 shows the diagram for
3807 the WASA logical interfaces and associated Table H-6 lists the logical interfaces by category.

Draft

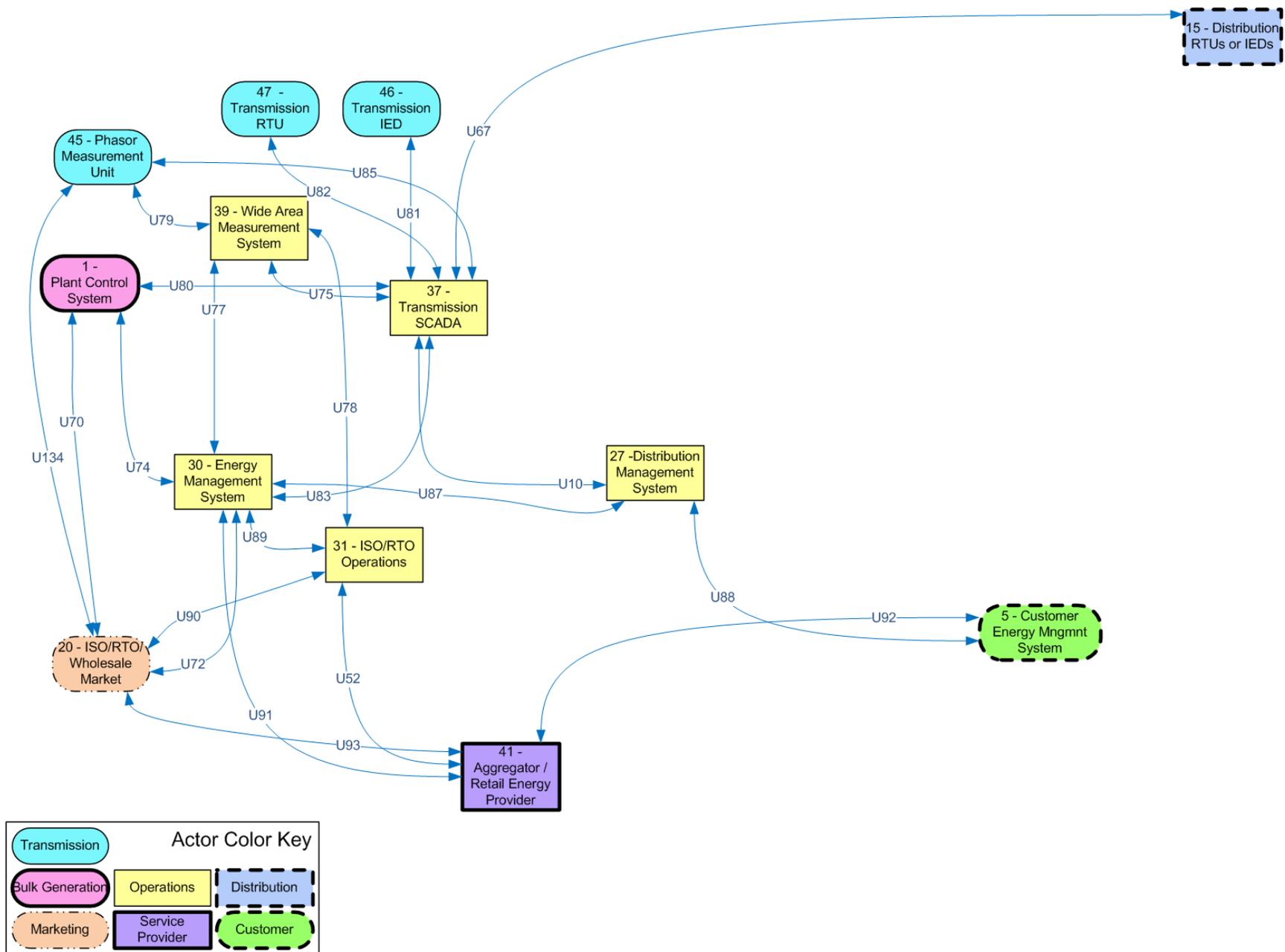


Figure H-6 Wide Area Situational Awareness

Table H-6 WASA Logical Interfaces by Logical Interface Category

Logical Interface Category	Logical Interfaces
1. Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints, for example: <ul style="list-style-type: none"> • Between transmission SCADA and substation equipment • Between distribution SCADA and high priority substation and pole-top equipment • Between SCADA and DCS within a power plant 	U67, U79, U81, U82, U85
2. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints, for example: <ul style="list-style-type: none"> • Between distribution SCADA and lower priority pole-top equipment • Between pole-top IEDs and other pole-top IEDs 	
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: <ul style="list-style-type: none"> • Between transmission SCADA and substation automation systems 	
4. Interface between control systems and equipment without high availability, without compute nor bandwidth constraints, for example: <ul style="list-style-type: none"> • Between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs 	
5. Interface between control systems within the same organization, for example: <ul style="list-style-type: none"> • Multiple DMS systems belonging to the same utility • Between subsystems within DCS and ancillary control systems within a power plant 	None
6. Interface between control systems in different organizations, for example: <ul style="list-style-type: none"> • Between an RTO/ISO EMS and a utility energy management system 	U10, U74, U80, U83, U87
7. Interface between back office systems under common management authority, for example: <ul style="list-style-type: none"> • Between a Customer Information System and a Meter Data Management System 	None
8. Interface between back office systems not under common management authority, for example: <ul style="list-style-type: none"> • Between a third-party billing system and a utility meter data management system 	None
9. Interface with B2B connections between systems usually involving financial or market transactions, for example: <ul style="list-style-type: none"> • Between a Retail aggregator and an Energy Clearinghouse 	U72, U93
10. Interface between control systems and non-control/corporate systems, for example: <ul style="list-style-type: none"> • Between a Work Management System and a Geographic Information System 	U75, U91
11. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements, for example: <ul style="list-style-type: none"> • Between a temperature sensor on a transformer and its receiver 	None

Logical Interface Category	Logical Interfaces
12. Interface between sensor networks and control systems, for example: <ul style="list-style-type: none"> • Between a sensor receiver and the substation master 	None
13. Interface between systems that use the AMI network, for example: <ul style="list-style-type: none"> • Between MDMS and meters • Between LMS/DRMS and Customer EMS 	None
14. Interface between systems that use the AMI network with high availability, for example: <ul style="list-style-type: none"> • Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment 	
15. Interface between systems that use customer (residential, commercial, and industrial) site networks which include: <ul style="list-style-type: none"> • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV 	None
16. Interface between external systems and the customer site, for example: <ul style="list-style-type: none"> • Between Third Party and HAN Gateway • Between ESP and DER • Between Customer and CIS Web site 	U88, U92
17. Interface between systems and mobile field crew laptops/equipment, for example: <ul style="list-style-type: none"> • Between field crews and GIS • Between field crews and substation equipment 	None
18. Interface between metering equipment, for example: <ul style="list-style-type: none"> • Between sub-meter to meter • Between PEV meter and Energy Service Provider 	None
19. Interface between operations decision support systems, for example: <ul style="list-style-type: none"> • Between WAMS and ISO/RTO 	U77, U78
20. Interface between engineering/maintenance systems and control equipment, for example: <ul style="list-style-type: none"> • Between engineering and substation relaying equipment for relay settings • Between engineering and pole-top equipment for maintenance • Within power plants 	None
21. Interface between control systems and their vendors for standard maintenance and service, for example: <ul style="list-style-type: none"> • Between SCADA system and its vendor 	None
22. Interface between security/network/system management consoles and all networks and systems, for example: <ul style="list-style-type: none"> • Between a security console and network routers, firewalls, computer systems, and network nodes 	None

3811 **APPENDIX I:**
 3812 **ANALYSIS MATRIX OF LOGICAL INTERFACE CATEGORIES**

3813 A set of Smart Grid key attributes was defined and allocated to each logical interface category.
 3814 These key attributes included requirements and constraints that were used in the selection of
 3815 security requirements for the logical interface category.

3816 This analysis was one of the tools that was used in the determination of the CI&A impact levels
 3817 for each logical interface category and in the selection of security requirements. The attribute
 3818 table was used as a guide for selecting unique technical requirements and determining the impact
 3819 level for confidentiality, integrity, and availability. The set of attributes allocated to each logical
 3820 interface category is not intended to be a comprehensive set, or to exclude interfaces that do not
 3821 include that attribute. For example, a Smart Grid information system may include logical
 3822 interface category 1, but not ATR-11, legacy information protocols. The goal was to define
 3823 typical attributes for each logical interface category.

3824 Table I-1 provides additional descriptions of each attribute.

3825 **Table I-1 Interface Attributes and Descriptions**

Interface Attributes	Descriptions
ATR-1a: Confidentiality requirements	Strong requirement that information should not be viewed by unauthorized entities
ATR-1b: Privacy concerns	Strong requirement that information should not be viewed by unauthorized entities
ATR-2: Integrity requirements	Strong requirement that information should not be modified by unauthorized entities, and should be validated for accuracy and errors. Higher level integrity may require additional technical controls.
ATR-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.
ATR-4: 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.
ATR-5: Microprocessor constraints on memory and compute capabilities	Severely-limited memory and/or compute capabilities of a microprocessor-based platform may constrain the types of security technologies, such as cryptography, that may be used while still allowing the platform to meet its performance requirements.
ATR-6: Wireless media	Wireless media may necessitate specific types of security technologies to address wireless vulnerabilities across the wireless path.
ATR-7: Immature or proprietary protocols	Immature or proprietary protocols may not be adequately tested either against inadvertent compromises or deliberate attacks. This may leave the interface with more vulnerabilities than if a more mature protocol were used.

Interface Attributes	Descriptions
ATR-8: Inter-organizational interactions	Interactions which cross organizational domains, including the use of out-sourced services and leased networks, can limit trust and compatibility of security policies and technologies. Therefore, these vulnerabilities should be taken into account.
ATR-9: Real-time operational requirements with low tolerance for latency problems	Real-time interactions may entail short acceptable time latencies, and may limit the security technology choices for mitigating on-going attacks.
ATR-11: Legacy communication	Older communication technologies may limit the types, thoroughness, or effectiveness of different security technologies which may be employed. This sensitivity to security technologies should be taken into account.
ATR-10: Legacy end-devices and systems protocols	Older end-devices and protocols may constrain the types, thoroughness, or effectiveness of different security technologies which may be employed.
ATR-12: Insecure, untrusted locations	Devices or systems in locations which cannot be made more secure due to their physical environment or ownership, pose additional security challenges. For instance, hardware-based cryptography may be necessary.
ATR-13: Key management for large numbers of devices	Key management for large numbers of devices without direct access to certificate management may limit the methods for deploying, updating, and revoking cryptographic keys.
ATR-14: Patch and update management constraints for devices including scalability and communications	Patch management constraints may limit the frequency and processes used for updating security patches.
ATR-15: Unpredictability, variability, or diversity of interactions	Unpredictable interactions may complicate the decisions on the types and severity of security threats and their potential impacts
ATR-16: Environmental and physical access constraints	Access constraints may limit the types of security technologies that could be deployed. For instance, if appliances are in a customer's house, access could be very limited.
ATR-17 Limited power source for primary power	Devices with limited power, such as battery-run appliances which "go to sleep" between activities, may constrain the types of security technologies to those that do not require continuous power.
ATR-18: Autonomous control	Autonomous control of devices that may not be centrally monitored could lead to undetected security threats.

3826
3827
3828
3829

Table I-2 provides the analysis matrix of the security-related logical interface categories (rows) against the attributes (ATR) that reflect the interface categories (columns).

Table I-2 Analysis Matrix of Security-Related Logical Interface Categories, Defined by Attributes

Attributes Logical Interface Categories	ATR-1a: Confidentiality requirements	ATR-1b: Privacy concerns	ATR-2: Integrity requirements	ATR-3: Availability requirements	ATR-4: Low bandwidth of communications channels	ATR-5: Microprocessor constraints on memory and compute capabilities	ATR-6: Wireless media	ATR-7: Immature or proprietary protocols	ATR-8: Inter-organizational interactions	ATR-9: Real-time operational requirements with low tolerance for latency problems	ATR-10: Legacy end-devices and systems	ATR-11: Legacy communication protocols	ATR-12: Insecure, untrusted locations	ATR-13: Key management for large numbers of devices	ATR-14: Patch and update management constraints for devices including scalability and communications	ATR-15: Unpredictability, variability, or diversity of interactions	ATR-16: Environmental and physical access constraints	ATR-17: Limited power source for primary power	ATR-18: Autonomous control
1. Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints			X	X	X	X	X	X		X	X	X	X	X	X		X		X
2. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints			X		X	X	X	X		X	X	X	X	X	X		X	X	X

Attributes Logical Interface Categories	ATR-1a: Confidentiality requirements	ATR-1b: Privacy concerns	ATR-2: Integrity requirements	ATR-3: Availability requirements	ATR-4: Low bandwidth of communications channels	ATR-5: Microprocessor constraints on memory and compute capabilities	ATR-6: Wireless media	ATR-7: Immature or proprietary protocols	ATR-8: Inter-organizational interactions	ATR-9: Real-time operational requirements with low tolerance for latency problems	ATR-10: Legacy end-devices and systems	ATR-11: Legacy communication protocols	ATR-12: Insecure, untrusted locations	ATR-13: Key management for large numbers of devices	ATR-14: Patch and update management constraints for devices including scalability and communications	ATR-15: Unpredictability, variability, or diversity of interactions	ATR-16: Environmental and physical access constraints	ATR-17: Limited power source for primary power	ATR-18: Autonomous control
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints			X	X			X	X		X	X	X	X	X			X		X
4. Interface between control systems and equipment without high availability, without compute nor bandwidth constraints			X				X	X		X	X	X	X	X	X	X	X		X
5. Interface between control systems within the same organization			X	X						X		X			X				X
6. Interface between control systems in different organizations			X	X					X	X		X			X				

Attributes Logical Interface Categories	ATR-1a: Confidentiality requirements	ATR-1b: Privacy concerns	ATR-2: Integrity requirements	ATR-3: Availability requirements	ATR-4: Low bandwidth of communications channels	ATR-5: Microprocessor constraints on memory and compute capabilities	ATR-6: Wireless media	ATR-7: Immature or proprietary protocols	ATR-8: Inter-organizational interactions	ATR-9: Real-time operational requirements with low tolerance for latency problems	ATR-10: Legacy end-devices and systems	ATR-11: Legacy communication protocols	ATR-12: Insecure, untrusted locations	ATR-13: Key management for large numbers of devices	ATR-14: Patch and update management constraints for devices including scalability and communications	ATR-15: Unpredictability, variability, or diversity of interactions	ATR-16: Environmental and physical access constraints	ATR-17: Limited power source for primary power	ATR-18: Autonomous control
7. Interface between back office systems under common management authority	x	x	x												x				
8. Interface between back office systems not under common management authority	x	x	x					x							x				
9. Interface with B2B connections between systems usually involving financial or market transactions	x	x	x	x					x	x						x			
10. Interface between control systems and non-control/ corporate systems	x	x	x	x				x	x						x	x			

Attributes Logical Interface Categories	ATR-1a: Confidentiality requirements	ATR-1b: Privacy concerns	ATR-2: Integrity requirements	ATR-3: Availability requirements	ATR-4: Low bandwidth of communications channels	ATR-5: Microprocessor constraints on memory and compute capabilities	ATR-6: Wireless media	ATR-7: Immature or proprietary protocols	ATR-8: Inter-organizational interactions	ATR-9: Real-time operational requirements with low tolerance for latency problems	ATR-10: Legacy end-devices and systems	ATR-11: Legacy communication protocols	ATR-12: Insecure, untrusted locations	ATR-13: Key management for large numbers of devices	ATR-14: Patch and update management constraints for devices including scalability and communications	ATR-15: Unpredictability, variability, or diversity of interactions	ATR-16: Environmental and physical access constraints	ATR-17: Limited power source for primary power	ATR-18: Autonomous control
11. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements					X	X	X	X		X	X	X	X				X	X	
12. Interface between sensor networks and control systems			X		X	X	X	X		X	X		X				X	X	X
13. Interface between systems that use the AMI network	X	X	X		X	X	X	X					X	X	X	X	X		
14. Interface between systems that use the AMI network for functions that require high availability	X	X	X	X	X	X	X	X					X	X	X	X	X		

Attributes Logical Interface Categories	ATR-1a: Confidentiality requirements	ATR-1b: Privacy concerns	ATR-2: Integrity requirements	ATR-3: Availability requirements	ATR-4: Low bandwidth of communications channels	ATR-5: Microprocessor constraints on memory and compute capabilities	ATR-6: Wireless media	ATR-7: Immature or proprietary protocols	ATR-8: Inter-organizational interactions	ATR-9: Real-time operational requirements with low tolerance for latency problems	ATR-10: Legacy end-devices and systems	ATR-11: Legacy communication protocols	ATR-12: Insecure, untrusted locations	ATR-13: Key management for large numbers of devices	ATR-14: Patch and update management constraints for devices including scalability and communications	ATR-15: Unpredictability, variability, or diversity of interactions	ATR-16: Environmental and physical access constraints	ATR-17: Limited power source for primary power	ATR-18: Autonomous control
15. Interface between systems that use customer (residential, commercial, and industrial) site networks such as HANs and BANs	X	X	X	X		X	X	X	X	X			X	X		X	X		X
16. Interface between external systems and the customer site	X	X	X			X		X	X				X	X		X			
17. Interface between systems and mobile field crew laptops/equipment			X	X	X		X	X					X	X	X		X		
18. Interface between metering equipment	X	X	X		X	X	X	X	X		X	X	X	X	X		X		

Attributes Logical Interface Categories	ATR-1a: Confidentiality requirements	ATR-1b: Privacy concerns	ATR-2: Integrity requirements	ATR-3: Availability requirements	ATR-4: Low bandwidth of communications channels	ATR-5: Microprocessor constraints on memory and compute capabilities	ATR-6: Wireless media	ATR-7: Immature or proprietary protocols	ATR-8: Inter-organizational interactions	ATR-9: Real-time operational requirements with low tolerance for latency problems	ATR-10: Legacy end-devices and systems	ATR-11: Legacy communication protocols	ATR-12: Insecure, untrusted locations	ATR-13: Key management for large numbers of devices	ATR-14: Patch and update management constraints for devices including scalability and communications	ATR-15: Unpredictability, variability, or diversity of interactions	ATR-16: Environmental and physical access constraints	ATR-17: Limited power source for primary power	ATR-18: Autonomous control
19. Interface between operations decision support systems			X	X					X	X									
20. Interface between engineering/maintenance systems and control equipment			X		X	X					X	X	X	X	X		X		
21. Interface between control systems and their vendors for standard maintenance and service			X						X				X	X	X		X		
22. Interface between security/network/system management consoles and all networks and systems	X	X	X	X						X	X	X		X	X	X	X		

3831 **APPENDIX J:**
 3832 **MAPPINGS TO THE HIGH-LEVEL SECURITY REQUIREMENTS**

3833 **J.1 R&D TOPICS**

3834 The following table is a mapping of research and development topics [See §8] to the High-Level Security Requirements Families.

		Smart Grid Security Requirements Families																			
		Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)	
Novel Mechanisms	Improve Cost - Effective Higher Tamper Resistant & Survivable Device Architectures					X		X													
	Intrusion Detection with Embedded Processors			X				X				X				X					
	Topics in Cryptographic Key Management		X				X			X							X	X			

		Smart Grid Security Requirements Families																		
		Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
	Detecting Anomalous Behavior Using Modeling											X			X	X				
System Level	Architecting for bounded recovery and reaction					X		X				X				X				X
	Architecting Real-time security	X					X								X		X			
	Calibrating assurance and timeliness trade-offs		X									X			X	X				
	Legacy system integration				X												X		X	X
	Resiliency Management and Decision Support		X	X		X		X				X				X				
	Efficient Composition of Mechanisms																X			

		Smart Grid Security Requirements Families																		
		Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
	Detection, Analysis, and Response																			
	Network Covert Channels in the Smart Grid: Creation, Characterization, Detection and Elimination					X		X									X			
	DoS/DDoS Resiliency	X				X	X	X									X	X		
	Cloud Security	X				X			X	X							X			
	Security Design & Verification Tools (SD&VT)				X															X
	Distributed versus Centralized security	X			X	X	X	X							X		X	X	X	

3837 **J.2 VULNERABILITY CLASSES**

3838 The following is a mapping of vulnerability classes [See §6] to the High-Level Security Requirements Families.
 3839

		Smart Grid Security Requirements Families																			
		Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)	
People, Policy and Procedure	Training	Insufficient Trained Personnel		X			X	X							X						
		Inadequate Security Training and Awareness Program		X			X	X							X						
	Policy and Procedure	Insufficient Identity Validation, Background Checks	X					X			X	X			X						X
		Inadequate Security Policy	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			X
		Inadequate Privacy Policy												X	X						
		Inadequate Patch Management Process	X			X	X	X	X							X			X	X	
		Inadequate Change and Configuration Management				X										X			X		

		Smart Grid Security Requirements Families																			
		Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)	
People, Policy and Procedure	Risk Management	Unnecessary System Access	X			X	X			X	X	X			X						
		Inadequate Periodic Security Audits			X										X						
		Inadequate Security Oversight by Management		X	X						X	X		X	X						
		Inadequate Continuity of Operations or Disaster Recovery Plan					X						X	X	X	X					
		Inadequate Risk Assessment Process													X						
		Inadequate Risk Management Process														X					
		Inadequate Incident Response Process				X		X					X	X		X	X				
	Code Quality Vulnerability		X							X					X		X	X	X	X	
	Authentication		X	X			X								X		X	X	X	X	

Platform Software/ Firmware Vulnerabilities

Software Development

		Smart Grid Security Requirements Families																			
		Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)	
Vulnerability																					
Authorization Vulnerability			X	X			X								X			X	X	X	
Cryptographic Vulnerability			X												X				X	X	
Environmental Vulnerability	X	X					X				X				X		X		X	X	
Error Handling Vulnerability			X												X			X	X	X	
General Logic Error			X												X				X	X	
Input and Output Validation			X												X			X	X	X	
Logging and Auditing Vulnerability			X				X								X				X	X	
Password Management Vulnerability	X	X					X								X				X	X	
Path Vulnerability			X												X				X	X	
Protocol Errors			X												X				X	X	

		Smart Grid Security Requirements Families																		
		Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Platform Software/ Firmware Vulnerabilities	Software Development																			
	Range and Type Error Vulnerability		X												X				X	X
	Sensitive Data Protection Vulnerability		X					X							X				X	X
	Session Management Vulnerability		X												X				X	X
	Concurrency, Synchronization and Timing Vulnerability		X												X				X	X
	Insufficient Safeguards for Mobile Code		X												X				X	X
	Buffer Overflow		X												X				X	X
	Mishandling of Undefined, Poorly Defined, or "Illegal" Conditions		X												X				X	X
	Use of Insecure Protocols		X												X		X		X	X
	Weakness that Affect Files and		X												X				X	X

		Smart Grid Security Requirements Families																			
		Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)	
Platform Vulnerabilities	Operational	Lack of Prompt Security Patches		X		X		X								X	X	X			
		Implementation	Absent of Deficient Equipment Implementation Guidelines	X	X	X	X		X				X		X	X	X			X	
			Installed Security Capabilities Not Enables by Default	X	X	X	X		X					X			X	X	X	X	
	Design	Inadequate Security Architecture and Design	X	X	X		X	X	X		X		X		X	X	X	X	X	X	X
		API Usage & Implementation	Use of Dangerous API		X											X				X	X
	API Abuse			X											X				X	X	
		Directories																			

Smart Grid Security Requirements Families

		Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
	from Software Vendors																			
	Unneeded Services Running		X	X	X								X			X	X	X	X	
	Insufficient Log Management	X	X	X	X	X	X	X		X			X			X	X	X	X	
	Inadequate Anomaly Tracking	X	X	X		X	X	X			X	X	X			X	X	X	X	
Network	Inadequate Integrity Checking				X									X			X	X	X	X
	Inadequate Network Segregation				X									X	X			X	X	X
	Inappropriate Protocol Selection				X									X			X	X	X	X
	Weakness in Authentication Process or Authentication Keys				X									X	X		X	X	X	X
	Insufficient Redundancy				X														X	X
	Physical Access to the Device	X			X		X				X	X		X	X					X

3841 **BOTTOM-UP TOPICS**

3842 The following is a mapping of topics identified in the Bottom-up chapter [See §7] to the High-Level Security Requirements Families.

	Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Openness and Accessibility of Smart Grid Standards														X					
Authenticating and Authorizing Users to Substation IEDs						X													
Authenticating and Authorizing Users to Outdoor Field Equipment						X													
Authenticating and Authorizing Maintenance Personnel to Meters						X													
Authenticating and Authorizing Consumers to Meters						X													
Authenticating Meters to/from AMI Head Ends						X													
Authenticating HAN Devices to/from HAN Gateways						X													

	Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Authenticating Meters to/from AMI Networks						X													
Securing Serial SCADA Communications																X			
Securing Engineering Dial-up Access																X			
Secure End-to-End Meter to Head End Communication																X			
Access Logs for IEDs			X																
Remote Attestation of Meters																X	X		X
Protection of Routing Protocols in AMI Layer 2/3 Networks																X	X		
Key Management for Meters																X			
Protection of Dial-up Meters																X			
Outsourced WAN Links																X			
Insecure Firmware Updates																	X	X	
Side Channel Attacks on Smart Grid Field Equipment						X										X			
Securing and Validating Field Device Settings	X					X										X			

	Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Absolute & Accurate Time Information			X			X										X			
Security Protocols																			
Synchrophasors																			
Certificates																			
Event Logs and Forensics																			
Personnel Issues In Field Service Of Security Technology																			
Weak Authentication of Devices In Substations						X					X								
Weak Security for Radio-Controlled Distribution Devices						X										X			
Weak Protocol Stack Implementations																X			
Insecure Protocols																			
License Enforcement Functions																			
IT vs. Smart Grid Security																			
Patch Management																	X		

	Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Authentication	X			X		X													
System Trust Model																X			
User Trust Model																X			
Security Levels																			
Distributed vs. Centralized Model of Management																			
Local Autonomy of Operation																			
Intrusion Detection for Power Equipment				X		X											X		
Network and System and Management for Power Equipment	X			X		X											X		
Security Event Management					X		X										X		X
Cross-Utility / Cross-Corporate Security																			
Trust Management																			
Management of Decentralized Security Controls																			
Password Management	X					X													
Cipher Suite																X			

	Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Authenticating Users to Control Center Devices and Services						X													
Authentication of Devices to Users						X													
Entropy																			
Tamper Evidence	X										X					X			
Challenges with Securing Serial Communications																			
Legacy Equipment with Limited Resources																X		X	X
Costs of Patch and Applying Firmware Updates	X	X		X		X					X						X		
Forensics and Related Investigations			X		X		X										X		
Roles and Role Based Access Control	X					X													
Limited Sharing of Vulnerability and/or Incident Information														X					
Data Flow Control Vulnerability Issues																			

	Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Use of Shared/Dedicated and Public/Private Cyber Resources																			
Traffic Analysis						X										X	X		
Poor Software Engineering Practices																	X		
Attribution of Faults to the Security System																			
Need for Unified Requirements Model																			
Broad Definition of Availability																			
Utility Purchasing Practices																		X	
Cyber Security Governance																			
Key Management Issues																			
Summarized Issues with PKI																			
Key Management Systems for Smart Grid															X				
Computational Constraints																			

	Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Channel Bandwidth																			
Connectivity																			
Certificate Life Cycles																X			
Local Autonomy of Operation																			
Availability																			
Trust Roots																			
Algorithms and Key Lengths																			
Selection and Use of Cryptographic Techniques																X			
Elliptic Curve Cryptography (ECC)														X					
Break Glass Authentication																			
Cryptographic Module Upgradeability																			
Password Complexity Rules	X					X													
Authentication						X													
Network Access Authentication and Access Control	X					X													

3847

APPENDIX K:

3848

GLOSSARY AND ACRONYMS

3DES	Triple Data Encryption Standard (168 Bit)
AAA	Authentication, Authorization, and Accounting
Active Directory	A technology created by Microsoft that provides a variety of network services and is a central component of the Windows Server platform. The directory service provides the means to manage the identities and relationships that make up network environments.
ADA	Americans with Disabilities Act
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
AGA	American Gas Association
AGC	Automatic Generation Control. A standalone subsystem that regulates the power output of electric generators within a prescribed area in response to changes in system frequency, tie-line loading, and the relation of these to each other. This maintains the scheduled system frequency and established interchange with other areas within predetermined limits.
Aggregation	Practice of summarizing certain data and presenting it as a total without any PII identifiers
AICPA	American Institute of Certified Public Accountants. The national, professional organization for all Certified Public Accountants.
AMI	Advanced Metering Infrastructure
AMI-SEC	AMI Security [Task Force]
Anonymize	<ul style="list-style-type: none"> • To organize data in such a way as to preserve the anonymity or hide the personal identity of the individual(s) to whom the data pertains • A process of transformation or elimination of PII for purposes of sharing data
ANSI	American National Standards Institute
API	Application Programming Interface
ASAP-SG	Advanced Security Acceleration Project – Smart Grid
ASTM	American Society for Testing and Materials
Asymmetric cipher	Cryptography solution in which separate keys are used for encryption and decryption, where one key is public and the other is private.
ATR	Attribute
B2B	Business to Business
BAN	Building Area Network
BEM	Building Energy Management

Block cipher	A symmetric key cipher operating on fixed-length groups of bits, called blocks, with an unvarying transformation—in contrast to a stream cipher, which operates on individual digits one at a time and whose transformation varies during the encryption. A block cipher, however, can effectively act as a stream cipher when used in certain modes of operation.
Botnet	Robot Network. A large number of compromised computers also called a “zombie army,” that can be used to flood a network with messages as a denial of service attack. A thriving botnet business consists in selling lists of compromised computers to hackers and spammers.
C&I	Commercial and Industrial
CA	Certificate Authority
CALEA	Communications Assistance for Law Enforcement Act
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing
CBC	Cipher Block Chaining
CEC	California Energy Commission
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CHP	Combined Heat and Power
CI&A	Confidentiality, Integrity, and Availability
CIM	Common Information Model. A structured set of definitions that allow different Smart Grid domain representatives to communicate important concepts and exchange information easily and effectively.
CIMA	Chartered Institute of Management Accountants
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPA	Children’s Internet Protection Act
CIS	Cryptographic Interoperability Strategy
CIS	Customer Information System
CISO	Chief Information Security Officer
CMMS	Computer-based Maintenance Management Systems
COTS	Commercial Off-the-Shelf
CPU	Central Processing Unit
CRL	Certificate Revocation List
CSCTG	Cyber Security Coordination Task Group
CSO	Chief Security Officer
CSP	Critical Security Parameters
CSR	Certificate Signing Request

CSR	Customer Service Representative
CSSWG	Control Systems Security Working Group
CSWG	Cyber Security Working Group
CRT	Cathode Ray Tube
CTR mode	Counter mode. A block cipher mode of operation also known as Integer Counter Mode (ICM) and Segmented Integer Counter (SIC) mode.
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DA	Distribution Automation
DARPA	Defense Advanced Research Projects Agency
DCS	Distributed Control System. A computer-based control system where several sections within the plants have their own processors, linked together to provide both information dissemination and manufacturing coordination.
DDoS	Distributed Denial of Service
De-identify	A form of anonymization that does not attempt to control the data once it has had PII identifiers removed, so it is at risk of re-identification.
DER	Distributed Energy Resources
DES	Data Encryption Standard
DEWG	Domain Expert Working Group
DFR	Digital Fault Recorder
DGM	Distribution Grid Management
DHS	Department of Homeland Security
Diffie-Hellman	A cryptographic key exchange protocol first published by Whitfield Diffie and Martin Hellman in 1976. It allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.
Distinguished names	String representations that uniquely identify users, systems, and organizations.
DMS	Distribution Management System
DN	Distinguished Name
DNP	Distributed Network Protocol
DNS	Domain Name Service
DoD	Department of Defense
DOE	Department of Energy
DoS	Denial of Service
DR	Demand Response
DRBG	Deterministic Random Bit Generators

DRM	Digital Rights Management. A generic term for access control technologies used by standards providers, publishers, copyright holders, manufacturers, etc. to impose limitations on the usage of digital content and devices. The term is used to describe any technology that inhibits the use of digital content in a manner not desired or intended by the content provider.
DRMS	Distribution Resource Management System
DSL	Digital Subscriber Line
DSPF	Distribution System Power Flow
DSS	Digital Signature Standard
EAP	Extensible Authentication Protocol
EAX mode	<ul style="list-style-type: none"> • A mode of operation for cryptographic block ciphers. It is an AEAD algorithm designed to simultaneously provide both authentication and privacy of the message with a two-pass scheme, one pass for achieving privacy and one for authenticity for each block. • A mixed authenticated encryption mode of operation of a block cipher in order to reduce the area overhead required by traditional authentication schemes.
EAX'	A modification of the EAX mode used in the ANSI C12.22 standard for transport of meter-based data over a network.
ECC	Elliptic Curve Cryptography (encryption)
ECDH	Elliptic Curve Diffie-Hellman. A key agreement protocol that allows two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel.
ECDSA	Elliptic Curve Digital Signature Algorithm
ECPA	Electronic Communications Privacy Act
EEO	Equal Employment Opportunity
EEPROM	Electrically Erasable Programmable Read-Only Memory
EISA	Energy Independence and Security Act
EKU	Extended Key Usage
EMS	Energy Management System
EMSK	Extended Master Session Key
Entropy	In the case of transmitted messages, a measure of the amount of information that is missing before reception.
Ephemeral Unified Model	A ECDH scheme where each party generates an ephemeral key pair to be used in the computation of the shared secret.
EPIC	Electronic Privacy Information Center
EPRI	Electric Power Research Institute
EPSA	Electric Power Supply Association
ES	Electric Storage
ESI	Energy Services Interface

ESP	Energy Service Provider
ET	Electric Transportation
EUMD	End Use Measurement Device
EV	Electric Vehicle
EV/PHEV	Electric Vehicle/Plug-in Hybrid Electric Vehicles. Cars or other vehicles that draw electricity from batteries to power an electric motor. PHEVs also contain an internal combustion engine.
EvDO	Evolution Data Optimized
EVSE	Electric Vehicle Service Element
FACTA	Fair and Accurate Credit Transactions Act
FAQ	Frequently Asked Questions
FERC	Federal Energy Regulatory Commission
FERPA	Family Educational Rights and Privacy Act
FIPS	Federal Information Processing Standards
FIPS 140-2	Publication 140-2 is a U.S. government computer security standard used to accredit cryptographic modules. NIST issued the FIPS 140 Publication Series to coordinate the requirements and standards for cryptography modules that include both hardware and software components.
FLIR	Fault Location, Isolation, Restoration
FTP	File Transfer Protocol
G&T	Generations and Transmission
GAPP	Generally Accepted Privacy Principles. Privacy principles and criteria developed and updated by the AICPA and Canadian Institute of Chartered Accountants to assist organizations in the design and implementation of sound privacy practices and policies.
GIC	Group Insurance Commission
GIS	Geographic Information System
GLBA	Gramm-Leach Bliley Act
GPRS	General Packet Radio Service
GPSK	Generalized Pre-Shared Key
Granularity	The extent to which a system contains separate components, e.g., the fineness or coarseness with which data fields are subdivided in data collection, transmission, and storage systems. The more components in a system, the more flexible it is. In more general terms, the degree to which a volume of information is finely detailed.
GRC	Governance, Risk, and Compliance
GWAC	GridWise Architecture Council

Hacker	In common usage, a hacker is a person who breaks into computers and/or computer networks, usually by gaining access to administrative controls. Proponents may be motivated by diverse objectives from the sheer entertainment value they find in the challenge of circumventing computer/network security to political or other ends. Hackers are often unconcerned about the use of illegal means to achieve their ends. Out-and-out cyber-criminal hackers are often referred to as "crackers."
HAN	Home Area Network. A network of energy management devices, digital consumer electronics, signal-controlled or -enabled appliances, and applications within a home environment that is on the home side of the electric meter.
Hash	Any well-defined procedure or mathematical function that converts a large, possibly variable-sized amount of data into a small datum, usually a single integer that may serve as an index to an array. The values returned by a hash function are called hash values, hash codes, hash sums, checksums, or simply hashes.
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health
HMAC	Hash Message Authentication Code
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
Hz	hertz
IBE	Identity-Based Encryption
ICS	Industrial Control Systems
ID	Identification
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFAC	International Federation of Accountants
IKE	Internet Key Exchange. Protocol used to set up a security association in the IPsec protocol suite.
INL	Idaho National Laboratory
IP	Internet Protocol
IPP	Independent Power Producer
IPR	Intellectual Property Rights
IPS	Intrusion Prevention System

IPSec	Internet Protocol Security
IS	Information Security
ISA	International Society of Automation
ISAKMP	Internet Security Association and Key Management Protocol
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISO	Independent System Operator
ISO/IEC27001	International Organization for Standardization/International Electrotechnical Commission Standard 27001. A auditable international standard that specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It uses a process approach for protection of critical information.
IT	Information Technology
ITGI	IT Governance Institute
ITL	Information Technology Laboratory
IVR	Interactive Voice Response
JNI	Java Native Interface
JTC	Joint Technical Committee
KDC	Key Distribution Center
KEK	Key Encryption Key
Kerberos	A computer network authentication protocol, developed by the Massachusetts Institute of Technology, which allows nodes communicating over a nonsecure network to prove their identity to one another in a secure manner. It is also a suite of free software published by MIT that implements this protocol.
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LMS	Load Management System
LTC	Load Tap Changer
MAC	Message Authentication Code
MAC address	Media Access Control address. The unique serial number burned into Ethernet and Token Ring adapters that identifies that network card from all others.
MAC protection	Message Authentication Code protection. In cryptography, a short piece of information used to authenticate a message. The MAC value protects data integrity and authenticity of the tagged message by allowing verifiers (who also possess the secret key used to generate the value) to detect any changes to the message content.
MDMS	Meter Data Management System

min	minute
MIT	Massachusetts Institute of Technology
MITM	Man in the Middle
ms	millisecond (10^{-3} second)
MTBF	Mean Time Before Failure
MW	megawatt (10^6 watts)
NAN	Neighborhood Area Network
NERC	North American Electric Reliability Corporation
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
NMAP	Networked Messaging Application Protocol
NRECA	National Rural Electric Cooperative Association
NSA	National Security Agency
NSA Suite B	A set of cryptographic algorithms promulgated by the National Security Agency to serve as an interoperable cryptographic base for both unclassified information and most classified information.
NSF	National Science Foundation
NVD	National Vulnerability Database
OCSP	Online Certificate Status Protocol
OE	Office of Electricity Delivery and Energy Reliability
OECD	Organisation for Economic Cooperation and Development. A global governmental forum of 30+ market democracies for comparison of policy experiences, good practices, and coordination of domestic and international policies. It is one of the world's largest and most reliable sources of comparable statistical, economic and social data.
OID	Object Identifier
OMS	Outage Management System
One-Pass Diffie-Hellman	A key-agreement scheme in which an ephemeral key pair generated by one party is used together with the other party's static key pair in the computation of the shared secret.
OWASP	Open Web Application Security Project
PANA	Protocol for carrying Authentication for Network Access
PAP	Priority Action Plan
PC	Personal Computer
PDA	Personal Digital Assistant
PDC	Phasor Data Concentrator

PE	Protocol Encryption
PE mode	<ul style="list-style-type: none"> • An encryption mode combining CTR mode and ECB mode developed for streaming SCADA messages. It relies on the SCADA protocol's ability to detect incorrect SCADA messages. • Position Embedding mode. A cryptographic mode designed specifically for low latency integrity protection on low-speed serial links.
Personal Information	Information that reveals details, either explicitly or implicitly, about a specific individual's household dwelling or other type of premises. This is expanded beyond the normal "individual" component because there are serious privacy impacts for all individuals living in one dwelling or premise. This can include items such as energy use patterns or other types of activities. The pattern can become unique to a household or premises just as a fingerprint or DNA is unique to an individual.
PEV	Plug-In Electric Vehicle
PFS	Perfect Forward Secrecy
PHEV	Plug In Hybrid Electric Vehicle
PIA	Privacy Impact Assessment. A process used to evaluate the possible privacy risks to personal information, in all forms, collected, transmitted, shared, stored, disposed of, and accessed in any other way, along with the mitigation of those risks at the beginning of and throughout the life cycle of the associated process, program or system.
PII	Personally Identifiable Information
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PKMv2	Privacy Key Management version 2
PLC	Programmable Logic Controller
PMU	Phasor Measurement Unit
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PQ	Power Quality
Public-key cryptography	A cryptographic approach that involves the use of asymmetric key algorithms instead of or in addition to symmetric key algorithms. Unlike symmetric key algorithms, it does not require a secure initial exchange of one or more secret keys to both sender and receiver.
PUC	Public Utilities Commission
QoS	Quality of Service
R&D	Research and Development
RA	Registration Authority
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RBAC	Role-Based Access Control

Retail Access	Competitive retail or market-based pricing offered by energy services companies or utilities to some or all of their customers under the approval/regulation of state public utilities departments.
RF	Radio Frequency
RFC	Request for Comments
RNG	Random Number Generator
RP	Relying Party
RSA	Widely used in electronic commerce protocols, this algorithm for public-key cryptography is named for Rivest, Shamir, and Adleman who were first to publicly described it. This was the first algorithm known to be suitable for signing as well as encryption and represents a great advance in public key cryptography.
RSA algorithm	RSA is public key cryptography algorithm named for its co-inventors: Ron Rivest, Adi Shamir, and Len Adleman.
RTO	Regional Transmission Operator
RTP	Real-Time Pricing
RTU	Remote Terminal Unit
s	second
S/MIME	Secure/Multipurpose Internet Mail Extensions
SA	Security Association
SAM	Security Authentication Module
SCADA	Supervisory Control and Data Acquisition
SCE	Southern California Edison
SDLC	Software Development Life Cycle
SDO	Standard Developing Organization
SEL	Schweitzer Engineering Laboratories
SEM	Security Event Management
SEP	Smart Energy Profile
SGIP	Smart Grid Interoperability Panel
SGIP TWiki	An open collaboration site for the Smart Grid community to work with NIST in developing a framework that includes protocols and model standards for information management to achieve interoperability of Smart Grid devices and systems and is part of a robust process for continued development and implementation of standards as needs and opportunities arise and as technology advances.
SGIP-CSWG	SGIP – Cyber Security Working Group
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard

Single sign-on	A property of access control of multiple, related, but independent software systems. With this property a user/device logs in once and gains access to all related systems without being prompted to log in again at each of them.
SNMP	Simple Network Management Protocol
Social Engineering	The act of manipulating people into performing actions or divulging confidential information. The term typically applies to trickery or deception being used for purposes of information gathering, fraud, or computer system access.
SP	Special Publication
SPOF	Signal Point of Failure
SSH	Secure Shell. A protocol for secure remote login and other secure network services over an insecure network.
SSID	Service Set Identifier
SSL	Secure Socket Layer
SSL/TLS	Secure Socket Layer / Transport Layer Security
SSN	Social Security Number
SSO	Single Sign-On
SSP	Sector-specific Plans
Symmetric cipher	Cryptography solution in which both parties use the same key for encryption and decryption, hence the encryption key must be shared between the two parties before any messages can be decrypted.
T&D	Transmission and Distribution
T&D DEWG	T&D Domain Expert Working Group
TA	Trust Anchor
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TCPA	Telephone Consumer Protection Act
TCS	Trouble Call System
Telnet	Teletype network. A network protocol used on the Internet or local area networks to provide a bidirectional interactive communications facility. The term telnet may also refer to the software that implements the client part of the protocol.
TEMPEST	A codename referring to investigations and studies of conducted emissions. Compromising emanations are defined as unintentional intelligence-bearing signals which, if intercepted and analyzed, may disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment.
TLS	Transport Layer Security
TNC	Trusted Network Connect
TOCTOU	Time of Check, Time of Use

TPI	Two-Person Integrity
TRSM	Tamper Resistant Security Modules
Trust anchor	In cryptography, an authoritative entity represented via a public key and associated data. When there is a chain of trust, usually the top entity to be trusted becomes the trust anchor. The public key (of the trust anchor) is used to verify digital signatures and the associated data.
TWiki	A flexible, open source collaboration and Web application platform (i.e., a structured Wiki) typically used to run a project development space, a document management system, a knowledge base, or any other groupware tool on an intranet, extranet, or the Internet to foster information flow between members of a distributed work group.
UCAIug	UtiliSec Working Group
UDP/IP	User Datagram Protocol/Internet Protocol
Upsell	Marketing term for the practice of suggesting higher priced products or services to a customer who is considering a purchase.
URL	Universal Resource Locator
USRK	Usage-Specific Root Key
Van Eck phreaking	Named after Dutch computer researcher Wim van Eck, phreaking is the process of eavesdropping on the contents of a CRT and LCD display by detecting its electromagnetic emissions. Because of its connection to eavesdropping, the term is also applied to exploiting telephone networks.
VAR	Volts-Amps-Reactive
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAMS	Wide Area Measurement System
WAN	Wide Area Network
WASA	Wide Area Situational Awareness
WG	Working Group
Wi-Fi	Term often used as a synonym for IEEE 802.11 technology. Wi-Fi is a trademark of the Wi-Fi Alliance that may be used with certified products that belong to a class of WLAN devices based on the IEEE 802.11 standards.
WiMAX	<ul style="list-style-type: none"> Worldwide Interoperability for Microwave Access. A telecommunications protocol that provides fixed and fully mobile Internet access. Wireless digital communications system, also known as IEEE 802.16, which is intended for wireless "metropolitan area networks."
WLAN	Wireless Local Area Network
WMS	Work Management System
XML	Extensible Markup Language

3849

3850

3851

APPENDIX L:

3852

SGIP-CSWG AND SGIP 2.0-SGCC MEMBERSHIP

3853

This list is a combination of all participants in the Smart Grid Interoperability Panel–Cyber

3854

Security Working Group (SGIP–CSWG) and the SGIP 2.0 Smart Grid Cybersecurity

3855

Committee, and all of the subgroups.

3856

	Name	Organization
1.	Aber, Lee	OPOWER
2.	Ackerman, Eric	Edison Electric Institute
3.	Ahmad, Wadji	General Electric
4.	Ahmadi, Mike	GraniteKey
5.	Ahsan, Naeem	DNV KEMA Energy and Sustainability
6.	Aikman, Megan	FERC
7.	Akyol, Bora	Pacific Northwest National Laboratory
8.	Alcaraz, Cristina	NIST
9.	Alexander, Michael	Underwriters Laboratories Inc.
10.	Alexander, Rob	Ember Corporation
11.	Alexander, Roger	Cooper Power Systems
12.	Allitt, Ed	IPKeys
13.	Al-Mukdad, Wendy	California PUC
14.	Alrich, Tom	ENCARI
15.	Ambady, Balu	Sensus
16.	Anderson, Casey	Tendril, Inc.
17.	Anderson, Dwight	Schweitzer Engineering Labs
18.	Anderson, Ken	Information and Privacy Commissioner's Office of Ontario
19.	Andreou, Demos	Cooper Industries
20.	Andrews, Joseph	Western Electricity Coordinating Council
21.	Antonacopoulos, Glenn	Northrop Grumman Corp.
22.	Arensman, Will	SouthWest Research Institute
23.	Arneja, Vince	Arxan Technologies, Inc.
24.	Artz, Sharla	Schweitzer Engineering Laboratories
25.	Arunachalam, Arun	Southern California Edison
26.	Ascough, Jessica	Harris Corporation
27.	Ashton, Skip	Ember Corporation
28.	Bacik, Sandy	Enernex
29.	Baiba Grazdina	Duke Energy
30.	Baker, Fred	Cisco Systems, Inc.
31.	Balsam, John	Georgia Tech Research Institute
32.	Banerjee, Aditi	Texas Instruments
33.	Barber, Mitch	Industrial Defender, Inc.
34.	Barclay, Steve	ATIS

	Name	Organization
35.	Barnes, Frank	University of Colorado at Boulder
36.	Barnett, Bruce	GE Global Research
37.	Barr, Michael	L-3 Communications Nova Engineering
38.	Bartol, Nadya	Utilities Telecom Council
39.	Barton, Michael	SunPower Corporation
40.	Bass, Len	Software Engineering Institute Carnegie Mellon University
41.	Basu, Sourjo	General Electric Energy
42.	Bates, Shirley	Siemens
43.	Batz, David	Edison Electric Institute
44.	Beale, Steven	Future of Privacy Forum
45.	Behrens, Stephen	KEMA, Inc.
46.	Beinert, Rolf	OpenADR
47.	Belanger, Phil	Oak Tree Consulting
48.	Belgi, Subodh	MIEL e-Security Private Limited
49.	Bell, Ray	Grid Net
50.	Bell, Will	Grid Net
51.	Bemmel, Vincent	Trilliant
52.	Bender, Klaus	Utilities Telecom Council
53.	Benn, Jason	Hawaiian Electric Company
54.	Benoit, Jacques	Cooper Power Systems
55.	Berkowitz, Don	S&C Electric Company
56.	Beroset, Ed	Elster Group
57.	Berrett, Dan E.	DHS Standards Awareness Team (SAT)
58.	Berrey, Adam	General Catalyst Partners
59.	Bertholet, Pierre-Yves	Ashlawn Energy, LLC
60.	Besko, Geoff	Securis, Inc.
61.	Beyene, Tsegereda	Cisco Systems, Inc.
62.	Bezecny, Steve	CenterPoint Energy
63.	Bhaskar, Mithun M.	National Institute of Technology, Warangal
64.	Biggs, Doug	Infogard
65.	Biggs, Les	Infogard
66.	Bilow, Steve	The Bilow Group
67.	Bitter, David	SMUD
68.	Blomgren, Paul	SafeNet Inc.
69.	Blossom, Michael	SmartSynch
70.	Bobba, Rakesh	University of Illinois, Urbana-Champaign
71.	Bochman, Andy	IBM
72.	Bockenek, Richard	Verizon
73.	Boivie, Rick	IBM T. J. Watson Research Center
74.	Boulez, Kris	Aszure
75.	Brackney, Dick	Microsoft
76.	Bradley, Steven	Virginia State Corporation Commission

	Name	Organization
77.	Braendle, Markus	ABB
78.	Branco, Carlos	Northeast Utilities
79.	Brennan, Jim	New Hampshire PUC
80.	Brent, Richard	FriiPwrLtd
81.	Brenton, Jim	Ercot
82.	Brewer, Tanya	NIST
83.	Brigati, David	NitroSecurity
84.	Brinskele, Ed	Vir2us Inc.
85.	Brooks, Thurston	3e Technologies International, Inc.
86.	Brown, Bobby	Booz Allen Hamilton
87.	Brown, Peter	Progress Energy
88.	Brozek, Mike	Westar Energy, Inc.
89.	Brunnetto, Michael	
90.	Bryan, Clifford	Examiner.com
91.	Brydl, Jerry	Steffes Corporation
92.	Bucciero, Joe	Buccerio Consulting
93.	Buffo, Lydia	Dominion
94.	Bump, William	Booz, Allen, Hamilton
95.	Burnham, Laurie	Dartmouth College
96.	Butler, Greg	
97.	Butterworth, Jim	Guidance Software
98.	Byrum, Drake	Cigital, Inc.
99.	Camilleri, John	Green Energy Corp
100.	Camm, Larry	Schweitzer Engineering Laboratories, Inc.
101.	Campagna, Matt	Certicom Corp.
102.	Cam-Winget, Nancy	Cisco Systems, Inc.
103.	Caprio, Daniel	McKenna Long & Aldridge LLP
104.	Cardenas, Alvaro A.	Fujitsu
105.	Carlson, Chris	Puget Sound Energy
106.	Carpenter, Matthew	
107.	Cavoukian, Ann	Office of the Information and Privacy Commissioner of Ontario
108.	Chan, Rida	Deloitte & Touche, LLP
109.	Chaney, Mike	Securicon
110.	Charbonneau, Sylvain	Hydro-Quebec
111.	Chasko, Stephen	Landis+Gyr
112.	Chason, Glen	EPRI
113.	Chaudhry, Hina	Argonne National Labs
114.	Chhabra, Rahul	Burns & McDonnell Engineering
115.	Chibba, Michelle	Office of the Information and Privacy Commissioner of Ontario
116.	Choubey, TN	Southern California Edison
117.	Chow, Edward	U of Colorado at Colorado Springs

	Name	Organization
118.	Chow, Richard	PARC
119.	Chris Starr	General Dynamics
120.	Christopher, Jason	FERC
121.	Chudgar, Raj	Sungard
122.	Chung, Raymond	National Technical Systems, Inc.
123.	Churchill, Alex	Duke Energy
124.	Cioni, Mark V.	MV Cioni Associates, Inc.
125.	Clark, Jamie	OASIS
126.	Claypoole, Ted	Womble Carlyle Sandridge & Rice, PLLC
127.	Clements, Abraham	Sandia National Laboratories
128.	Clements, Sam	Pacific Northwest National Laboratory
129.	Cleveland, Frances	Xanthus Consulting International
130.	Cohen, Michael	Mitre
131.	Cohen, Yossi	
132.	Collier, Albert	Alterium, LLC
133.	Coney, Lillie	Electronic Privacy Information Center
134.	Coomer, Mark	ITT Defense and Information Solutions
135.	Coop, Mike	ThinkSmartGrid
136.	Cornish, Kevin	Enspira
137.	Cortes, Sarah	Inman Technology IT
138.	Cosio, George	Florida Power and Light
139.	Cox, William	Cox Software Architects
140.	Cragie, Robert	Jennic LTD
141.	Crane, Melissa	Tennessee Valley Authority
142.	Crljenica, Igor	State of Michigan
143.	Cuen, Lita	LC RISQ & Associates
144.	Cui, Stephen	Microchip Technology
145.	Czaplewski, John	Northrup Grumman Corp.
146.	Dagle, Jeff	Pacific Northwest National Laboratory
147.	Dalva, Dave	Stroz Friedberg
148.	Danahy, Jack	Bochman & Danahy Research
149.	Danezis, George	Microsoft
150.	Dangler, Jack	Cigital, Inc.
151.	Dangler, Jack	SAIC
152.	Das, Subir	Applied Communication Sciences
153.	Davis, Scott	Sensus
154.	Davison, Brian	Public Utility Commission of Texas
155.	De Petrillo, Nick	Industrial Defender
156.	Delenela, Ann	Ercot
157.	DeLoach, Tim	IBM Global Business Services
158.	DePeppe, Doug	i2IS Cyberspace Solutions
159.	di Sabato, Mark	
160.	Dieffenbach, Dillon	Ernst & Young

	Name	Organization
161.	Dienhart, Mary	Xcel Energy
162.	Dierking, Tim	Aclara Power-Line Systems, Inc.
163.	Dillon, Terry	APS
164.	Dinges, Sharon	Trane
165.	Dion, Thomas	Dept of Homeland Security
166.	Do, Tam	Southwest Research Institute
167.	Dodd, David	pbnetworks
168.	Dodson, Greg	Dominion Resources Services, Inc.
169.	Don-Arthur, George	Alterium LLC
170.	Doreswamy, Rangan	Verisign, Inc.
171.	Doring, Ernest	Pacific Gas & Electric
172.	Dorn, John	Accenture
173.	Dougherty, Steven	IBM
174.	Downum, Wesley	Telcordia
175.	Dransfield, Michael	National Security Agency
176.	Drgon, Michele	DataProbit
177.	Drozinski, Timothy	Florida Power & Light Company
178.	Drummond, Rik	Drummond Group
179.	Dubrawsky, Ido	Itron
180.	Duffy, Paul	Cisco Systems
181.	Duggan, Pat	ConEd
182.	Dulaney, Mike	Arxan Technologies, Inc.
183.	Dunfee, Rhonda	Department of Energy
184.	Dunphy, Mary	
185.	Dunton, Benjamin	NYS Department of Public Service
186.	Dupper, Jeff	Ball Aerospace & Technologies
187.	Duren, Michael	Protected Computing
188.	Dutta, Prosenjit	Utilities AMI Practice
189.	Earl, Frank	Earl Consulting
190.	Eastham, Bryant	Panasonic Electric Works Laboratory of America (PEWLA)
191.	Edgar, Tom	Pacific Northwest National Laboratory
192.	Eggers, Matthew	U.S. Chamber of Commerce
193.	Eigenhuis, Scott M	
194.	Ellison, Mark	DTE Energy
195.	Emelko, Glenn	ESCO
196.	Engels, Mark	Dominion Resources Services, Inc.
197.	Ennis, Greg	Wi-Fi Alliance
198.	Enstrom, Mark	NeuStar
199.	Eraker, Liz	Samuelson Clinic at UC Berkeley
200.	Erickson, Dave	California Public Utility Commission
201.	Ersue, Mehmet	Nokia Siemens Networks
202.	Estefania, Maria	ATIS

	Name	Organization
203.	Eswarahally, Shrinath	Infineon Technologies NA
204.	Evans, Bob	Idaho National Laboratory
205.	Ewing, Chris	Schweitzer Engineering Labs
206.	Fabela, Ronnie	Lockheed Martin
207.	Fabian, Michael	Wurldtech Security Technologies
208.	Faith, Doug	MW Consulting
209.	Faith, Nathan	American Electric Power
210.	Famolari, David	Telcordia Technologies
211.	Faure, Jean-Philippe	Progilon Co.
212.	Fennell, Kevin	Landis+Gyr
213.	Fenner, Philip	American Electric Power, Inc.
214.	Fischer, Ted	Norwich University Applied Research Institutes (NUARI)
215.	Fisher, Jim	Noblis
216.	Fishman, Aryah	Edison Electric Institute
217.	Fitzpatrick, Gerald	NIST
218.	Flickinger, Derek	ThinkSmartGrid, LLC
219.	Flowers, Tom	Control Center Solutions, LLC
220.	Foglesong, Anna	Pacific Gas & Electric
221.	Ford, Guy	New Hampshire Electric Cooperative
222.	Foster, William	Lumi Wireless Technologies
223.	Francis, Daniel	AEP
224.	Franklin, Troy	FriiPwrLtd
225.	Franz, Matthew	SAIC
226.	Fraser, Barbara	Cisco
227.	Fredebeil, Karlton	Tennessee Valley Authority
228.	Frederick, Jennifer	Direct Energy
229.	Fredrickson, Dan	Tendrill Inc.
230.	Freund, Mark	Pacific Gas and Electric Company
231.	Friedman, Dan	
232.	Frogner, Bjorn	
233.	Fulford, Ed	
234.	Fuloria, Shailendra	Cambridge University
235.	Fulton, Joel	
236.	Futch, Matt	IBM Energy and Utilities
237.	Gailey, Mike	CSC
238.	Galli, Stefano	ASSIA, Inc.
239.	Garrard, Ken	Aunigma Network Solutions Corp.
240.	Gassko, Irene	Florida Power & Light
241.	Gaulding, Win	Northrop Grumman Information Systems
242.	Gerber, Josh	San Diego Gas and Electric
243.	Gerbino, Nick	Dominion Resources Services, Inc.
244.	Gering, Kip	Itron
245.	Gerney, Arkadi	OPOWER

	Name	Organization
246.	Gerra, Arun	University of Colorado, Boulder
247.	Ghansah, Isaac	California State University Sacramento
248.	Gibbs, Derek	SmartSynch
249.	Gilchrist, Grant	EnerNex
250.	Gill, Jeff	RuggedCom Inc.
251.	Gillmore, Matt	CMS Energy
252.	Givens, Beth	Privacy Rights Clearinghouse
253.	Glasse, Todd	Certichron Inc.
254.	Glavin, Kevin	Cigital
255.	Glenn, Bill	Westar Energy, Inc.
256.	Goff, Ed	Progress Energy
257.	Gokul, Jay	Technology Crest Corp.
258.	Golla, Ramprasad	Grid Net
259.	Gomez, Aaron	Drummond Group
260.	Gonzalez, Efrain	Southern California Edison
261.	Gooding, Jeff	Southern California Edison
262.	Goodson, Paul	ISA
263.	Gorog, Christopher	Atmel Corporation
264.	Grainger, Steven	General Dynamics
265.	Grazdina, Baiba	Duke Energy
266.	Greenberg, Alan M.	Boeing
267.	Greenfield, Neil	American Electric Power, Inc.
268.	Greer, David	University of Tulsa
269.	Griffin, Slade	Enernex
270.	Grochow, Jerrold	MIT
271.	Gulick, Jessica	SAIC
272.	Gunter, Carl	U. of Illinois
273.	Gupta, Rajesh	UC San Diego
274.	Gupta, Sarbari	Electrosoft
275.	Gutierrez, Julio	Florida Power & Light
276.	Habre, Alex	PJM
277.	Hague, David	
278.	Halasz, Dave	Aclara
279.	Halbgewachs, Ronald D.	Sandia National Laboratories
280.	Hall, Tim	Mocana
281.	Hallman, Georgia	Guidance Software
282.	Hambrick, Gene	Carnegie Mellon University
283.	Hanley, James	General Electric
284.	Hardjono, Thomas	MIT
285.	Harkins, Dan	Aruba Networks
286.	Harper, John	American Electric Power, Inc.
287.	Harris, Greg	Harris Corporation
288.	Harris, Therese	Public Utility Commission of Texas

	Name	Organization
289.	Harrison, Becky	GridWise Alliance
290.	Hartman, Darren	ICSA Labs
291.	Hartmann, Chad	Xcel Energy
292.	Hashimoto, Mikio	Toshiba
293.	Hastings, Nelson	NIST
294.	Hawk, Carol	Department of Energy
295.	Hayden, Ernest	Verizon
296.	He, Donya	BAE Systems
297.	Heger, Mary	Ameren Services
298.	Heiden, Rick	Pitney Bowes
299.	Heidner, Dennis	
300.	Helm, Donny	Oncor
301.	Henderson, Lynn	Northrop Grumman Information Systems
302.	Hensel, Hank	CSC
303.	Herold, Rebecca	Rebecca Herold & Associates, LLC
304.	Heron, George L.	BlueFin Security
305.	Herrell, Jonas	University of California, Berkeley
306.	Hertzler, Megan	Xcel Energy
307.	Hertzog, Christine	Smart Grid Library
308.	Hieta, Karin	California Public Utility Commission
309.	Higgins, Moira	TSRI
310.	Highfill, Darren	SCE
311.	Hilber, Del	Constellation Energy
312.	Histed, Jonathan	Novar Honeywell
313.	Hoag, John C.	Ohio University
314.	Holland, Clayton	DHS / Missing Link Security
315.	Hollenbaugh, Greg	Electrosoft Inc.
316.	Holstein, Dennis	OPUS Consulting Group
317.	Hoofnagle, Chris	University of California, Berkeley
318.	Hooper, Emmanuel	Harvard University
319.	Hornung, Lynette	
320.	House, Joshua	Future of Privacy
321.	Houseman, Doug	Capgemini Consulting
322.	Howie, Sarah	NextEnergy Center
323.	Huber, Robert	Critical Intelligence
324.	Hudson, John	CenterPoint Energy
325.	Hughes, Joe	EPRI
326.	Humphrey, Robert	Duke Energy
327.	Humphries, Scott	SmartSynch
328.	Hunt, Chuck	
329.	Hunteman, William	Department of Energy
330.	Hurley, Jesse	Shift Research, LLC
331.	Hussey, Laura	Schweitzer Engineering Laboratories, Inc.

	Name	Organization
332.	Hutson, Jeff	Accenture
333.	Huzmezan, Mihai	General Electric
334.	Ibrahim, Erfan	EPRI
335.	Iga, Yoichi	Renesas Electronics Corp.
336.	Ilic, Jovan	
337.	Ilic, Marija	Carnegie-Mellon University
338.	Inaba, Atsushi	GlobalSign
339.	Iorga, Michaela	NIST
340.	Ivers, James	SEI
341.	Jacobs, Leonard	Xcel Energy
342.	Jaffray, Travis	
343.	Jaokar, Ajit	Futuretext
344.	Jarrett, Terry	Missouri Public Service Commission
345.	Jeirath, Nakul	Southwest Research Institute
346.	Jepson, Robert	Lockheed Martin Energy Solutions
347.	Jin, Chunlian	Pacific Northwest National Laboratory
348.	Joffe, Rodney	NeuStar
349.	Johnson, Freeman	NIST
350.	Johnson, Oliver	Tendril
351.	Jones, Barry	Sempra
352.	Jones, Derrick	Enteredge Technology, LLC
353.	Joshi, Makarand	
354.	Kahl, Steve	North Dakota
355.	Kahn, Ely	FriiPwrLtd
356.	Kaiser, Lisa	Department of Homeland Security
357.	Kalbfleisch, Roderick	Northeast Utilities
358.	Kanda, Mitsuru	Toshiba
359.	Kashatus, Jennifer	Womble Carlyle Sandridge & Rice, PLLC
360.	Kassakhian, Ken	Colorado Dept. of Regulatory Authorities
361.	Kastner, Ryan	University of California at San Diego
362.	Katz, Martha Lessman	Gordon, Feinblatt, Rothman, Hoffberger & Hollander, LLC
363.	Kaufman, David R.	Honeywell International
364.	Kavanagh, Mike	Constellation Energy
365.	Kellogg, Shannon	EMC
366.	Kelly, Lee	
367.	Kenchington, Henry	U.S. Department of Energy
368.	Kenney, Charlie	IBM
369.	Kerber, Jennifer	Tech America
370.	Khera, Rohit	S & C Electric Company
371.	Khurana, Himanshu	Honeywell
372.	Kiely, Sarah	NRECA
373.	Kilbourne, Brett	Utilities Telecom Council

	Name	Organization
374.	Kim, Jin	Risk Management Consulting, CRA International
375.	Kim, Tae-Wan	NIST
376.	Kimura, Randy	General Electric
377.	King, Charlie	BAE Systems
378.	Kirby, Bill	Aunigma Network Solutions Corp.
379.	Kiss, Gabor	Telcordia
380.	Kladko, Stan	Aspect Labs
381.	Klein, Stanley A.	Open Secure Energy Control Systems, LLC
382.	Klerer, Mark	
383.	Kobayashi, Nobuhiro	Mitsubishi Electric
384.	Kobes, Jason	Northrop Grumman Corp.
385.	Koliwad, Ajay	General Electric
386.	Kotting, Chris	ThinkSmartGrid, LLC
387.	Koyuncu, Osman	Texas Instruments, Inc.
388.	Kravitz, David	
389.	Krishna, Karthik	Michigan Technological University
390.	Krishnamurthy, Hema	ITT Information Assurance
391.	Kube, Nate	Wurldtech
392.	Kulkarni, Manoj	Mocana
393.	Kursawe, Klaus	European Network for Cyber Security (ENCS)
394.	Kuruganti, Phani Teja	EMC2
395.	Kyle, Martin	Sierra Systems
396.	Lackey, Kevin	Electric Reliability Council of Texas (ERCOT)
397.	Lakshminarayanan, Sitaraman	General Electric
398.	LaMarre, Mike	Austin Energy ITT
399.	Lane, Anne	American Electric Power, Inc.
400.	LaPorte, TJ	Landis+Gyr
401.	Larsen, Harmony	Infogard
402.	Lauriat, Nicholas A.	Network and Security Technologies
403.	LaVoy, Lanse	DTE Energy
404.	Lawrence, Bill	Lockheed Martin Corporation
405.	Lawson, Barry	NRECA
406.	Lebanidze, Evgeny	Cigital
407.	Leduc, Jean	Hydro-Quebec
408.	Lee, Annabelle	EPRI
409.	Lee, Cheolwon	Electronics and Telecommunications Research Institute
410.	Lee, Gunhee	Electronics and Telecommunications Research Institute
411.	Lee, JJ	LS Industrial Systems
412.	Lee, Travis	SMUD
413.	Lee, Virginia	eComp Consultants
414.	Legary, Michael	Seccuris, Inc.
415.	Leggin, Nick	West Monroe

	Name	Organization
416.	Lenane, Brian	SRA International
417.	Leuck, Jason	Lockheed Martin Corporation
418.	Levinson, Alex	Lockheed Martin Information Systems and Global Solutions
419.	Levy, Roger	Lawrence Berkeley National Laboratory
420.	Lewis, David	Hydro One
421.	Lewis, Rob	Trustifiers Inc.
422.	Li, Tony	CLP Power Hong Kong Lmtd
423.	Liang, Charles Cheong	CLP Power Hong Kong Lmtd
424.	Libous, Jim	Lockheed Martin Systems Integration – Owego
425.	Light, Matthew	NERC
426.	Lilley, John	Sempra
427.	Lima, Claudio	Sonoma Innovation
428.	Lin, Yow-Jian	Telcordia Technologies
429.	Lintzen, Johannes	Utimaco Safeware AG
430.	Lipson, Howard	CERT, Software Engineering Institute
431.	Locke, David	Verizon
432.	Loomis, Joe	Southwest Research Institute
433.	Lowe, Justin	PA Consulting Group
434.	Lynch, Jennifer	University of California, Berkeley
435.	Machado, Raphael	Inmetro – Instituto Nacional de Metrologia, Brazil
436.	Maciel, Greg	Uniloc USA
437.	Madden, Jason	MRIGlobal
438.	Magda, Wally	Industrial Defender
439.	Magnuson, Gail	
440.	Mahmud, Shamun	DLT Solutions, Incorporated
441.	Malashenko, Liza	California PUC
442.	Malina, Alfred	SG-CG Smart Grid Information Security WG
443.	Manjrekar, Madhav	Siemens
444.	Manucharyan, Hovanes	LinkGard Systems
445.	Maria, Art	AT&T
446.	Markham, Tom	Honeywell
447.	Marks, Larry	
448.	Martin, Gordon	Alabama Power
449.	Martinez, Catherine	DTE Energy
450.	Martinez, Ralph	BAE Systems
451.	Marty, David	University of California, Berkeley
452.	Masch, Brian	Ernest & Young
453.	Mashima, Daisuke	Fujitsu Lab of America
454.	McBride, Sean	Critical Intelligence
455.	McCaffree, Matt	OPOWER
456.	McComber, Robert	Telvent
457.	McCullough, Jeff	Elster Group

	Name	Organization
458.	McDonald, Jeremy	Southern California Edison
459.	McGinnis, Douglas	Exelon
460.	McGrew, David	Cisco
461.	McGuire, John	American Electric Power, Inc.
462.	McGurk, Sean	Dept of Homeland Security
463.	McKay, Brian	Booz Allen Hamilton
464.	McKenna, Erin	
465.	McKinnon, David	Pacific Northwest National Laboratory
466.	McMahon, Liam	Bridge Energy Group
467.	McMillin, Bruce	Missouri University of Science and Technology
468.	McNay, Heather	Landis+Gyr
469.	McQuade, Rae	NAESB
470.	Medlar, Arthur	LocalPower
471.	Melton, Ron	Pacific Northwest National Laboratory
472.	Mennella, Jean-Pierre	SG-CG Smart Grid Information Security WG
473.	Mertz, Michael	Southern California Edison
474.	Metke, Tony	Motorola
475.	Michail, David	Zuber & Taillieu LLP
476.	Milbrand, Doug	Concurrent Technologies Corporation
477.	Millard, David	Georgia Tech Research Institute
478.	Miller, Joel	Merrion Group
479.	Miller, Melvin	Nulink Wireless
480.	Mirza, Wasi	Motorola
481.	Mitsuru, Kanda	Toshiba
482.	Mitton, David	Ambient Corp.
483.	Modeste, Ken	Underwriters Laboratories, Inc.
484.	Mohan, Apurva	Honeywell
485.	Moise, Avy	Future DOS R&D Inc.
486.	Molina, Jesus	Fujitsu Ltd.
487.	Molitor, Paul	NEMA
488.	Mollenkopf, Jim	CURRENT Group
489.	Moniz, Paulo	EDP - Energias de Portugal, S.A.
490.	Monkman, Brian	ICSA Labs
491.	Montgomery, Jason	American Electric Power, Inc.
492.	Moody, Diane	American Public Power Association
493.	Morese, Alex	State of Michigan
494.	Morris, Tommy	Mississippi State University
495.	Mosely, Donald	FriiPwrLtd
496.	Moskowitz, Robert	ICSA Labs
497.	Mulberry, Karen	Neustar
498.	Munoz, Tony	Colorado Department of Regulatory Agencies
499.	Nahas, John	ICF International
500.	Nakamura, Masafumi	Mitsubishi Research Institute, Inc.

	Name	Organization
501.	Navid, Nivad	Midwest ISO
502.	Neergaard, Dude	Oak Ridge National Laboratory
503.	Newhouse, Bill	NIST
504.	Nguyen, Nhut	Samsung
505.	Nidetz, Lee	TSRI
506.	Nissim, Sharon Goott	Electronic Privacy Information Center
507.	Noel, Paul	ASI
508.	Norton, Dave	Entergy
509.	Nutaro, James J.	Southern California Edison
510.	O'Neill, Ivan	Southern California Edison
511.	O'Sullivan, Mairtin	
512.	Obregon, Eduardo	University of Texas at El Paso
513.	Oduyemi, Felix	Southern California Edison
514.	Ohba, Yoshihiro	Toshiba
515.	Okunami, Peter M.	Hawaiian Electric Company, Inc.
516.	Old, Robert	Siemens Building Technologies, Inc.
517.	Oldak, Mike	Utilities Telecom Council
518.	Olive, Kay	Olive Strategies
519.	Ornelas, Efrain	PG&E
520.	Overman, Thomas M.	Boeing
521.	Owens, Andy	Plexus Research
522.	Owens, Leslie	American Systems
523.	Pabian, Michael	Exelon Legal Services
524.	Pace, James	Silver Spring Networks
525.	Pahl, Chris	Southern California Edison Company
526.	Paine, Tony	Keppure Technologies
527.	Pal, Partha	Raytheon BBN Technologies
528.	Pales, Wayne	CLP Power Hong Kong Lmtd
529.	Palmquist, Scott	Itron
530.	Papa, Mauricio	University of Tulsa
531.	Parthasarathy, Jagan	Business Integra
532.	Patel, Chris	EMC Technology Alliances
533.	Pearce, Thomas C. II	Public Utilities Commission of Ohio
534.	Pederson, Perry	U.S. Nuclear Regulatory Commission
535.	Peralta, Rene	NIST
536.	Peters, Mike	FERC
537.	Peterson, Thomas	Boeing
538.	Phillips, Matthew	Electronic Privacy Information Center
539.	Phillips, Michael	Centerpoint Energy
540.	Phinney, Tom	
541.	Phiri, Lindani	Elster Group
542.	Pillitteri, Victoria Yan	NIST
543.	Pittman, James	Idaho Power

	Name	Organization
544.	Pittman, Jason	DTE Energy
545.	Planter-Pascal, Claudine	FERC
546.	Polonetsky, Jules	The Future of Privacy Forum
547.	Polulyakh, Diana	Aspect Labs
548.	Pope, John	NeuStar
549.	Porterfield, Keith	Georgia System Operations Corporation
550.	Potter, Rick	Alliant Energy
551.	Powell, Terry	L-3 Communications
552.	Proctor, Brian	Sempra Energy Utilities
553.	Prowell, Stacy	Oak Ridge National Laboratory
554.	Puri, Anuj	IEEE
555.	Pyle, Mike	Schneider Electric
556.	Pyles, Ward	Southern Company
557.	Qin, Andy	Cisco
558.	Qin, Jason	Skywise Systems
559.	Qiu, Bin	E:SO Global
560.	Quinn, Steve	Sophos
561.	Rader, Bodhi	FERC
562.	Radgowski, John	Dominion Resources Services, Inc
563.	Ragsdale, Gary L.	Southwest Research Institute
564.	Raines, Tim	Black Hills, Corp.
565.	Rakaczky, Ernest A.	Invensys Global Development
566.	Rao, Josyula R	IBM
567.	Ray, Indrakshi	Colorado State University
568.	Reddi, Ramesh	Intell Energy
569.	Reed, Rebecca	Texas PUC
570.	Revill, David	Georgia Transmission Corp.
571.	Rhéaume, Réjean	Hydro-Quebec
572.	Richtsmeier, Dorann	Northrup Grumman Corp.
573.	Riepenkroger, Karen	Sprint
574.	Ristaino, Andre	
575.	Rivaldo, Alan	Public Utility Commission of Texas
576.	Rivero, Al	Telvent
577.	Roberts, Don	Southern Company Transmission
578.	Roberts, Jeremy	LonMark International
579.	Robinson, Brandon	Balch & Bingham LLP
580.	Robinson, Charley	International Society of Automation
581.	Robinson, Eric	ITRON
582.	Robinson, Louis	Constellation Energy
583.	Rodriguez, Gene	IBM
584.	Rothke, Ben	National Grid
585.	Ruano, Julio	IBM
586.	Rueangvivatanakij, Birdie	Missing Link Security

	Name	Organization
587.	Rumery, Brad	Sempra
588.	Rush, Bill	
589.	Russell, Dave	Noveda Technologies
590.	Rutfield, Craig	NTRU Cryptosystems, Inc.
591.	Rutkowska, Joanna	Invisible Things
592.	Rutkowski, Tony	Yaana Technologies
593.	Sachs, Marcus	Verizon Communications
594.	Sacre, Spiro	National Technical Systems, Inc.
595.	Saint, Bob	National Rural Electric Cooperative Association
596.	Sakane, Hiro	NIST
597.	Sakr, Osman	National Technical Systems, Inc.
598.	Salons, Deborah	
599.	Sambasivan, Sam	AT&T
600.	Sanders, William	University of Illinois
601.	Saperia, Jon	
602.	Sargent, Robert	Cisco Systems, Inc.
603.	Saunders, Scott	SMUD
604.	Scace, Caroline	NIST
605.	Schaefer, Krystina	Ohio PUC
606.	Schantz, Rick	Raytheon BBN Technologies
607.	Scheff, Andrew	Scheff Associates
608.	Schmitt, Laurent	SG-CG Smart Grid Information Security WG
609.	Schneider, Brandon	SRA International
610.	Schneider, Don	Duke Energy
611.	Schoechle, Timothy	
612.	Schomburg, Paul	Panasonic Corp. of North America
613.	Schooler, Eve	Intel Labs
614.	Schroeder, Joel	Inmarsat Inc.
615.	Schulman, Ross	Center for Democracy and Technology
616.	Schultz, Bill	Vanderbilt University
617.	Schwarz, David	Department of Homeland Security
618.	Sciacca, Sam	SCS Consulting, LLC
619.	Sconzo, Mike	Electric Reliability Council of Texas
620.	Scott, David	Accenture
621.	Scott, Kat	EPIC
622.	Scott, Richard	
623.	Scott, Tom	Progress Energy
624.	Searforce, Daniel	Pennsylvania Public Utility Commission
625.	Searle, Justin	UtiliSec
626.	Seewald, Mike	Cisco
627.	Seo, Jeongtaek	Electronics and Telecommunications Research Institute
628.	Sequino, David	Green Hills Software
629.	Shah, Nihar	Information Law Group

	Name	Organization
630.	Shakespeare, Jared	Western Electricity Coordinating Council
631.	Shastri, Viji	MCAP Systems
632.	Shavit, Juliet	SmartMark Communications, LLC
633.	Shaw, Vishant	Enernex
634.	Shein, Robert	EDS
635.	Sheldon, Rick	Oakridge National Laboratory
636.	Sherman, Sean	Triton
637.	Shetty, Ram	General Electric
638.	Shin, Mark	Infogard
639.	Shiple, AJ	Wind River
640.	Shorter, Scott	Electrosoft
641.	Shpantzer, Gal	
642.	Silverstone, Ariel	
643.	Sinai, Nick	Office of Science & Technology Policy, the White House
644.	Singer, Bryan	Kenexis
645.	Sisley, Elizabeth	University of Minnesota
646.	Sitbon, Pascal	EDF Inc.
647.	Skare, Paul	Pacific Northwest National Laboratory
648.	Skidmore, Charlotte	Association of Home Appliance Manufacturers
649.	Slack, Phil	Florida Power & Light Company
650.	Smith, Brian	EnerNex
651.	Smith, Charles	General Electric
652.	Smith, Rhett	Schweitzer Engineering Laboratories, Inc.
653.	Smith, Ron	ESCO Technologies Inc.
654.	Smith, Zane	FriiPwrLtd
655.	Sokker, Anan	Florida Power & Light Company
656.	Sood, Kapil	Intel Labs
657.	Sorebo, Gilbert	SAIC
658.	Soriano, Erick	Garvey Schubert Barer
659.	Souza, Bill	
660.	Spirakis, Charles	Google
661.	St Johns, Michael	Nth Permutation
662.	Staggs, Kevin	Honeywell
663.	Stallings, Amanda	Public Utility Commission of Ohio
664.	Stammberger, Kurt	Mocana
665.	Standifur, Thomas	KEMA Inc.
666.	Starr, Christopher	General Dynamics Advanced Information Systems
667.	Steiner, Michael	IBM Thomas J. Watson Research Center
668.	Stepanovich, Amie	EPIC
669.	Sterling, Joyce	NitroSecurity
670.	Stevens, James	Software Engineering Institute
671.	Stewart, Clinton	
672.	Stitzel, Jon	Burns & McDonnell Engineering Company, Inc.

	Name	Organization
673.	StJohns, Michael	Nth Permutation
674.	Storey, Clay	Avista Corp.
675.	Stouffer, Keith	NIST
676.	Strickland, Tom	General Electric
677.	Struik, Rene	Struik Security Consultancy
678.	Struthers, Brent	NeuStar
679.	Stuber, Micheal	ltron
680.	Sturek, Don	Grid2Home
681.	Sturm, John	Indiana State University
682.	Stycos, Dave	Zocalo Data Systems, Ltd.
683.	Suarez, Luis Tony	Tennessee Valley Authority
684.	Suchman, Bonnie	Troutman Sanders LLP
685.	Sullivan, Kevin	Microsoft
686.	Sung, Lee	Fujitsu
687.	Sushilendra, Madhava	EPRI
688.	Swanson, Marianne	NIST
689.	Sweet, Jeffrey	American Electric Power, Inc.
690.	Tallent, Michael	Tennessee Valley Authority
691.	Taylor, Dave	Siemens
692.	Taylor, Malcolm	Carnegie Mellon University
693.	Tengdin, John	OPUS Consulting
694.	Thanos, Daniel	General Electric
695.	Thaw, David	Hogan & Hartson
696.	Thomas, Sarah	California Public Utility Commission
697.	Thomassen, Tom	Symantec
698.	Thompson, Catherine	Information and Privacy Commissioner's Office of Ontario
699.	Thompson, Daryl L.	Thompson Network Consulting
700.	Thompson, Mark	Aclara RF Systems, Inc.
701.	Thomson, Matt	General Electric
702.	Thrasher, Shelly	Office of the Information & Privacy Commissioner of Ontario
703.	Tien, Lee	Electronic Freedom Foundation
704.	Tiffany, Eric	Liberty Alliance
705.	Tillman, Leonard	Balch & Bingham LLP
706.	Tobin, Tim	Hogan Lovells US LLP
707.	Toecker, Michael	Burns & McDonnell
708.	Tolway, Rich	APS
709.	Tom, Steve	Idaho National Laboratory
710.	Tran, Lan	Tangible
711.	Trapp, Bob	Booz Allen Hamilton
712.	Trayer, Mark	Samsung
713.	Trimble, Curtis D.	

	Name	Organization
714.	Truskowski, Mike	Cisco System, Inc.
715.	Tull, Laurie	Anakam, an Equifax Company
716.	Tunney, Carrin	DTE Energy
717.	Turgeon, Anyck	
718.	Turke, Andy	Siemens Energy, Inc.
719.	Turner, Patrick	Secure Works
720.	Turner, Steve	International Broadband Electric Communications, Inc.
721.	Uhrig, Rick	Electrosoft
722.	Urban, Jennifer	Samuelson Clinic at UC Berkeley
723.	Uzhunnan, Abdul	DTE Energy
724.	Vader, Rob	DTE Energy
725.	van Loon, Marcel	AuthenTec
726.	Vankayala, Vidya	BC Hydro
727.	Vayos, Daphne	Northeast Utilities
728.	Veillette, Michel	Trilliant Inc.
729.	Veltsos, Christophe	Minnesota State University
730.	Venkatachalam, R. S.	Mansai Corporation
731.	Vettoretti, Paul	SBC Global
732.	Villarreal, Christopher	California Public Utilities Commission
733.	Voje, Joe	Snohomish County PUD
734.	Vollebregt, Paul	MobiComm Communications
735.	Wacks, Kenneth P.	GridWise Architecture Council
736.	Waddell, Dan	Tantus Tech
737.	Waheed, Aamir	Cisco Systems
738.	Walia, Harpreet	Wave Strong Inc.
739.	Wall, Perrin	CenterPoint Energy
740.	Wallace, Donald	Itron
741.	Walsh, Jack	ICSA Labs
742.	Walters, Keith	Edison Electric Institute
743.	Walters, Ryan	COO TerraWi Communications
744.	Wang, Alex	Cisco Systems, Inc.
745.	Wang, Longhao	Samuelson Clinic at UC Berkeley
746.	Wang, Yongge	University of North Carolina-Charlotte
747.	Ward, Mark	Pacific Gas & Electric Company
748.	Warner, Christopher	Pacific Gas & Electric Company
749.	Watson, Brett	NeuStar
750.	Webb, Kyle	Deloitte & Touche LLP
751.	Weber, Don	InGuardians
752.	Wei, Dong	SIEMENS Corporation
753.	Weimerskirch, Andre	Escrypt
754.	Wepman, Joshua	SAIC Commercial Business Services
755.	West, Andrew C	Invensys Process Systems
756.	West, Troy	Cleco Corpo.

	Name	Organization
757.	Weyer, John A.	John A. Weyer and Associates
758.	Whitaker, Kari	LockDown, Inc.
759.	White, Jim	Uniloc USA, Inc.
760.	Whitney, Tobias	The Structure Group
761.	Whitsitt, Jack	
762.	Whyte, William	Ntru Cryptosystems, Inc.
763.	Wiese, Sean	National Information Solutions Cooperative
764.	Williams, Jeffrey	
765.	Williams, Terron	Elster Electricity
766.	Wilson, Chris	TechAmerica
767.	Wilson, Jason	Duke Energy
768.	Wingo, Harry	Google
769.	Witnov, Shane	University of California, Berkeley
770.	Wohnig, Ernest	Booz-Allen Hamilton
771.	Wolf, Dana	RSA
772.	Wollman, David	NIST
773.	Worden, Michael	New York State Public Service Commission
774.	Worthington, Charles	Federal Communications Commission
775.	Wright, Andrew	N-Dimension Solutions
776.	Wright, Christine	Texas PUC
777.	Wright, Josh	Inguardians
778.	Wu, Lei	Clarkson University
779.	Wu, Richard	Nokia Siemens Networks, USA
780.	Wyatt, Michael	ITT Advanced Technologies
781.	Xia, Sharon	ALSTOM Grid Inc.
782.	Yakobitis, John J.	Federal Energy Regulatory Commission
783.	Yao, Taketsugu	Oki Electric Industry, Co., Ltd
784.	Yap, Xiang Ling	MIT
785.	Yardley, Tim	University of Illinois
786.	Yodaiken, Ruth	Federal Trade Commission
787.	Yoo, Kevin	Wurldtech
788.	Zausner, Alan	
789.	Zummo, Paul	American Public Power Association
790.	Zurcher, John	SRA