

UCAIUG: AMI-SEC-ASAP

AMI System Security Requirements

V1.01

ASAP

12/17/2008

1 **Executive Summary**

2 This document provides the utility industry and vendors with a set of security requirements for
3 Advanced Metering Infrastructure (AMI). These requirements are intended to be used in the
4 procurement process, and represent a superset of requirements gathered from current cross-
5 industry accepted security standards and best practice guidance documents.
6

7 This document provides substantial supporting information for the use of these requirements
8 including scope, context, constraints, objectives, user characteristics, assumptions, and
9 dependencies. This document also introduces the concept of requirements for security states and
10 modes, with requirements delineated for security states.
11

12 These requirements are categorized into three areas: 1) Primary Security Services, 2) Supporting
13 Security Services and 3) Assurance Services. The requirements will change over time
14 corresponding with current security threats and countermeasures they represent. The AMI-SEC
15 Task Force presents the current set as a benchmark, and the authors expect utilities and vendors
16 to tailor the set to individual environments and deployments.
17

18 While these requirements are capable of standing on their own, this document is intended to be
19 used in conjunction with other 2008 deliverables from the AMI-SEC Task Force, specifically the
20 Risk Assessment, the Architectural Description, the Component Catalog (in development as of
21 this writing), and the Implementation Guide (to be developed late 2008). This document also
22 discusses the overall process for usage of this suite.
23

24 **Acknowledgements**

25 The AMI-SEC Task Force would like to acknowledge the work of the primary authors,
26 contributing authors, editors, reviewers, and supporting organizations. Specifically, the Task
27 Force would like to thank:

- 28
- 29 • The AMI Security Acceleration Project (ASAP)
 - 30 ○ The Architectural Team including resources from Consumers Energy,
 - 31 EnerNex Corporation, InGuardians, The Software Engineering Institute at
 - 32 Carnegie Mellon University, and Southern California Edison
 - 33 ○ Supporting organizations including The Electric Power Research Institute and
 - 34 The United States Department of Energy
 - 35 ○ Participating utilities, including American Electric Power, Austin Energy, BC
 - 36 Hydro, Consumers Energy, Duke Energy, Kansas City Power & Light, Oncor,
 - 37 Pacific Gas & Electric, San Diego Gas & Electric, Southern California Edison
- 38 • The utilities, vendors, consultants, national laboratories, higher education institutions,
- 39 governmental entities, and other organizations that have actively contributed to and
- 40 participated in the activities of the AMI-SEC Task Force
- 41

42 The AMI-SEC Task Force would also like to thank the Department of Homeland Security Cyber
43 Security Division, National Institute of Standards and Technology Computer Security Division,
44 North American Reliability Corporation and The Common Criteria for the works that they have
45 produced that served as reference material for the AMI Systems Security Requirements
46 document.

47

48 **Authors**

49 Bobby Brown
50 Brad Singletary
51 Bradford Willke
52 Coalton Bennett
53 Darren Highfill
54 Doug Houseman
55 Frances Cleveland
56 Howard Lipson
57 James Ivers
58 Jeff Gooding
59 Jeremy McDonald
60 Neil Greenfield
61 Sharon Li

62

63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108

Table of Contents

Executive Summary	i
Acknowledgements	ii
1. Introduction	1
1.1 Purpose	1
1.1.1 Strategic Importance	1
1.1.2 Problem Domain	1
1.1.3 Intended Audience	3
1.1. Scope	3
1.2. Document Overview	4
1.3. Definitions, acronyms, and abbreviations	6
1.4. References	6
2. General system description	7
2.1. Use Cases	7
2.1.1. Billing	8
2.1.2. Customer	10
2.1.3. Distribution System	11
2.1.4. Installation	12
2.1.5. System	13
2.2. System Context	14
2.3. System Constraints	17
2.4. Security States and Modes	18
2.4.1. System States	19
2.4.2. System Modes	20
2.5. Security Objectives	21
2.5.1. Holistic Security	23
2.6. User Characteristics	23
2.7. Assumptions and Dependencies	24
3. System Security Requirements	24
3.1. Primary Security Services	25
3.1.1. Confidentiality and Privacy (FCP)	25
3.1.2. Integrity (FIN)	26
3.1.3. Availability (FAV)	28
3.1.4. Identification (FID)	29
3.1.5. Authentication (FAT)	29
3.1.6. Authorization (FAZ)	33
3.1.7. Non-Repudiation (FNR)	34
3.1.8. Accounting (FAC)	34
3.2. Supporting Security Services	37
3.2.1. Anomaly Detection Services (FAS)	37
3.2.2. Boundary Services (FBS)	37
3.2.3. Cryptographic Services (FCS)	39
3.2.4. Notification and Signaling Services (FNS)	40
3.2.5. Resource Management Services (FRS)	41
3.2.6. Trust and Certificate Services (FTS)	43

109	3.3. Assurance.....	43
110	3.3.1. Development Rigor (ADR).....	43
111	3.3.2. Organizational Rigor (AOR).....	47
112	3.3.3. Handling/Operating Rigor (AHR)	57
113	3.3.4. Accountability (AAY)	60
114	3.3.5. Access Control (AAC).....	63
115	Appendix A: Architectural Description	65
116	A.1. Scope.....	65
117	A.2. Mission.....	66
118	A.3. Stakeholders & Concerns.....	66
119	A.4. Security Analysis Approach.....	67
120	A.5. Architecture Description Approach	68
121	A.5.1. Viewpoints	68
122	A.5.2. Views	69
123	A.6 Contextual View	69
124	A.7 Top Level Model.....	70
125	A.7.1. Customer Model.....	71
126	A.7.2. Third Party Model.....	73
127	A.7.3. Utility Model.....	74
128	A.8 Security Domains View	78
129	A.8.1. Utility Edge Services Domain.....	79
130	A.8.2 Premise Edge Services Domain	79
131	A.8.3. Communication Services Domain	80
132	A.8.4. Managed Network Services Domain	80
133	A.8.5. Automated Network Services Domain	80
134	A.8.6. Utility Enterprise Services Domain	81
135		

136		
137	Appendix B – Supplemental Material: Business Functions as Stakeholders in AMI Systems	1
138	B.1 Introduction	1
139	B.1.2 Scope of AMI Systems.....	1
140	B.2 Overview of Business Functions Utilizing AMI Systems	2
141	B.3 AMI Metering Business Functions	3
142	B.3.1 Metering Services.....	3
143	B.3.2 Pre-Paid Metering	5
144	B.3.3 Revenue Protection	5
145	B.3.4 Remote Connect / Disconnect.....	6
146	B.3.5 Meter Maintenance.....	7
147	B.4 Distribution Operations Business Functions	8
148	B.4.1 Distribution Automation (DA)	8
149	B.4.2 Outage Detection and Restoration.....	9
150	B.4.3 Load Management.....	11
151	B.4.4 Power Quality Management.....	12
152	B.4.5 Distributed Energy Resource (DER) Management.....	12
153	B.4.6 Distribution Planning	15
154	B.4.7 Work Management.....	16
155	B.5 Customer Interactions Business Functions	17
156	B.5.1 Customer Services.....	17
157	B.5.2 Tariffs and Pricing Schemes	18
158	B.5.3 Demand Response	19
159	B.6 External Parties Business Functions	21
160	B.6.1 Gas and Water Metering	21
161	B.6.2 Third Party Access	21
162	B.6.3 External Party Information.....	22
163	B.6.4 Education.....	23
164	B.6.5 Third Party Access for Certain Utility Functions.....	23
165		
166		

Table of Figures

167		
168		
169	Figure 1 – Deliverables Process Flow	5
170	Figure 2 – AMI Security Domain Model	15
171	Figure 3 - Example of a System State Flow Diagram.....	19
172	Figure 4 – AMI Top Level Model.....	70
173	Figure 5 - Customer Model.....	71
174	Figure 6 - Third Party Model.....	73
175	Figure 7 - Utility Model.....	74
176	Figure 8 - AMI Service Domains.....	78
177	Figure 9 - Scope of AMI Systems	2
178	Figure 10 - Business Functions Utilizing the AMI/Enterprise Bus Interface.....	3
179		

180 **1. Introduction**

181 As a key element in the evolution of the Smart Grid, the Advanced Metering Infrastructure
182 (AMI) is the convergence of the power grid, the communications infrastructure, and the
183 supporting information infrastructure. AMI security must exist in the real world with many
184 interested parties and overlapping responsibilities. This document focuses on the security
185 services that are important to secure the power grid, communications infrastructure and
186 supporting information infrastructure.

187 **1.1 Purpose**

188 The purpose of the AMI Security Specification is to provide the utility industry along with
189 supporting vendor communities and other stakeholders a set of security requirements that should
190 be applied to AMI implementations to ensure the high level of information assurance,
191 availability and security necessary to maintain a reliable system and consumer confidence.
192 While this specification focuses on AMI, the security requirements contained in the document
193 may be extended to other network-centric, Smart Grid solutions.

194 **1.1.1 Strategic Importance**

195 Utility companies of the future will deliver energy and information to customers through a
196 “smart” energy supply chain created by the convergence of electric, communication and
197 information technologies that are highly automated for responding to the changing environment,
198 electricity demands and customer needs. The building blocks of this Smart Grid include AMI,
199 advanced transmission and distribution automation, distributed generation, electric vehicle
200 refueling infrastructure and renewable energy generation projects of today.

201
202 The emergence of this new class of Smart Grid systems holds tremendous promise and requires
203 innovation and deployment of new technologies, processes and policies. Composed of many
204 independent systems, the Smart Grid will evolve by integrating existing islands of automation to
205 achieve value through the delivery of information to customers, grid operators, utility companies
206 and other stakeholders. A reliable and secure Smart Grid holds the promise of enabling
207 automated demand response, providing customers a myriad of options to manage their energy
208 costs through technology enabled programs along with limiting outages with a self-healing
209 resilient transmission and distribution network and other strategically important functions.

210
211 The challenge of providing both a reliable and secure AMI solution lies in the diversity of
212 technologies, processes and approaches used to realize this vision. Managing change rising from
213 the complexity of diverse solutions with an effective and efficient systems integration process
214 will enable the AMI system. This requires a commitment to standards, best practices and a high
215 degree of architectural discipline. This document specifies platform independent security
216 requirements, services and guidance required to implement secure, resilient AMI solutions.

217 **1.1.2 Problem Domain**

218 As the utility industry’s capabilities increase to serve the needs of a rapidly growing information
219 society, the breadth and sophistication of the threat environment these Smart Grid solutions
220 operate in also increases. By bridging heterogeneous networks capable of exchanging

221 information seamlessly across the AMI older proprietary and often manual methods of securing
222 utility services will disappear as each is replaced by more open, automated and networked
223 solutions. The benefits of this increased connectivity depends upon robust security services and
224 implementations that are necessary to minimize disruption of vital services and provide increased
225 reliability, manageability and survivability of the electric grid.
226

227 Recognizing the unique challenges of AMI enabled Smart Grid solutions is imperative to
228 deploying a secure and reliable solution. Unique characteristics of AMI implementations that set
229 them apart from other utility project include the following:

- 230 • AMI touches every consumer
- 231 • AMI is a command and control system
- 232 • AMI has millions of nodes
- 233 • AMI touches almost every enterprise system
- 234 • Many current AMI solutions are narrowband solutions
235

236 These network-centric characteristics, coupled with a lack of a composite set of cross industry
237 AMI security requirements and implementation guidance, is the primary motivation for the
238 development of this document. The problem domains needing to be addressed within AMI
239 implementations are relatively new to the utility industry, however there is precedence for
240 implementing large scale, network-centric solutions with high information assurance
241 requirements. The defense, cable and telecommunication industries offer a number of examples
242 of requirements, standards and best practices directly applicable to AMI implementations.
243

244 The challenge is to secure AMI in a holistic manner, noting that such an approach requires the
245 buy-in of many stakeholders. Stakeholders can be viewed in three groups:

- 246 • Stakeholders within the enterprise who have an interest in generating value from technology
247 investments:
 - 248 – Those who make investment decisions
 - 249 – Those who decide about requirements
 - 250 – Those who use technology services
- 251 • Internal and external stakeholders who provide technology services:
 - 252 – Those who manage the technology organization and processes
 - 253 – Those who develop capabilities
 - 254 – Those who operate the services
- 255 • Internal and external stakeholders who have a control/risk responsibility:
 - 256 – Those with security, privacy and/or risk responsibilities
 - 257 – Those performing compliance functions
 - 258 – Those requiring or providing assurance services
259

260 To meet the requirements of the stakeholder community, a security framework for AMI
261 technology governance and control should:

- 262 • Provide a business focus to enable alignment between business and technology objectives
- 263 • Establish a process orientation to define the scope and extent of coverage, with a defined
264 structure enabling easy navigation of content
- 265 • Be generally acceptable by being consistent with accepted technology good practices and
266 standards and independent of specific technologies

- 267 • Supply a common language with a set of terms and definitions that are generally
268 understandable by all stakeholders
- 269 • Help meet regulatory requirements by being consistent with generally accepted corporate
270 governance standards (e.g., Committee of Sponsoring Organizations of the Treadway
271 Commission) and technology controls expected by regulators and external auditors.
272

273 As such, this document provides security requirements for the purposes of procurement, design
274 input, validation and certification. It is not the intent of this document to describe AMI
275 architecture. The satisfaction of requirements identified in this document implies a need for
276 coherent architecture, policies, procedures, etc... none of which is prescribed in this document.
277

278 AMI security involves a system of systems approach in design and operations, and therefore
279 security responsibility must extend to stakeholders and parties outside and in addition to the
280 electric utility. While security requirements for the broader AMI may or may not be within the
281 scope of a single utility's responsibility, imposing the requirements upon cooperating
282 interconnecting systems and the corresponding capabilities will meet or support some aspects of
283 AMI security objectives. Moreover, interdependencies among the power grid, the
284 communications infrastructure, and the information infrastructure pose a particularly serious
285 challenge to the design of a secure and survivable AMI.

286 **1.1.3 Intended Audience**

287 The intended audience for this document includes utility companies seeking AMI
288 implementation and policy guidance; vendors seeking product design requirements and input;
289 policy makers seeking to understand the requirements of reliable and secure AMI solutions; and
290 any reader who wishes to find information related to AMI security requirements. While this
291 document is intended for use by security professionals, solution architects and product designers,
292 much of the document is written for a broader audience seeking to understand AMI security
293 challenges, requirements and potential solutions. Lastly, this specification may provide a
294 foundation for security requirements in the procurement and implementation of AMI solutions.
295

296 This document is intended to be a living specification to be updated as the industry evolves, with
297 a focus on AMI security functionality. As such, one of the benefits of this document is to create
298 a baseline document for the utility industry that provides AMI security requirements and
299 identifies gaps between current requirements and capabilities available in the market. Ideally,
300 the AMI security specification will be referenced and reused throughout the utility industry,
301 providing a common set of semantics for enabling the development and implementation of
302 robust, reliable AMI solutions.

303 **1.1. Scope**

304 AMI Security is simply defined as those means and measures concerned with securing an AMI
305 system. For the purpose of this document, the definition of AMI is:

306 *The communications hardware and software and associated system and data*
307 *management software that creates a network between advanced meters and utility*
308 *business systems and which allows collection and distribution of information to*
309 *customers and other parties such as competitive retail providers, in addition to*

310 *providing it to the utility itself. AMI is further defined as: 1) The hardware and*
311 *software residing in, on, or closest to the customer premise for which the utility or*
312 *its legal proxies are primarily responsible for proper operation; and 2) The*
313 *hardware and software owned and operated by the utility or its legal proxies*
314 *which has as its primary purpose the facilitation of Advanced Metering.*

315 This document presents security requirements for AMI systems. This document does not address
316 business functional or other non-security related requirements.

317
318 A further understanding of the scope requires an understanding of the utility business systems
319 and associated functionality. Section 2.1 of this document discusses Utility Business Systems
320 and services. In general, this specification is a tool that can be applied broadly as defined above
321 and to peripheral systems using AMI communication services. Each individual utility should
322 decide the boundary distinction. The boundary definition and document applicability includes
323 system security maturity of the associated connecting system, organizational responsibility and
324 procurement scope.

325
326 The AMI-SEC Task Force considered HAN use cases in the development of this document and it
327 is reasonable to assume utility edge application requirements can be applied to HAN applications
328 (e.g., requirements applied to utility applications can also be applied to consumer applications).
329 Imposing requirements on the HAN requires additional considerations associated with control
330 and ownership that are outside the scope of this document.

331 **1.2. Document Overview**

332 This section describes how this document relates to the Architectural Description, Risk
333 Assessment, Component Catalog and Implementation Guide.

334
335 The path that a particular utility follows through these documents (Risk Assessment, System
336 Security Requirements, Architectural Description, Component Catalog and Implementation
337 Guide) depends upon the level of resources the utility chooses to put toward the effort. In the
338 drawing below, this level of resources tracks the “Entry Points” on the right side of the drawing.
339 For the descriptions below (Figure 1), the utility will define Architectural Elements, i.e.,
340 hardware and software.

341

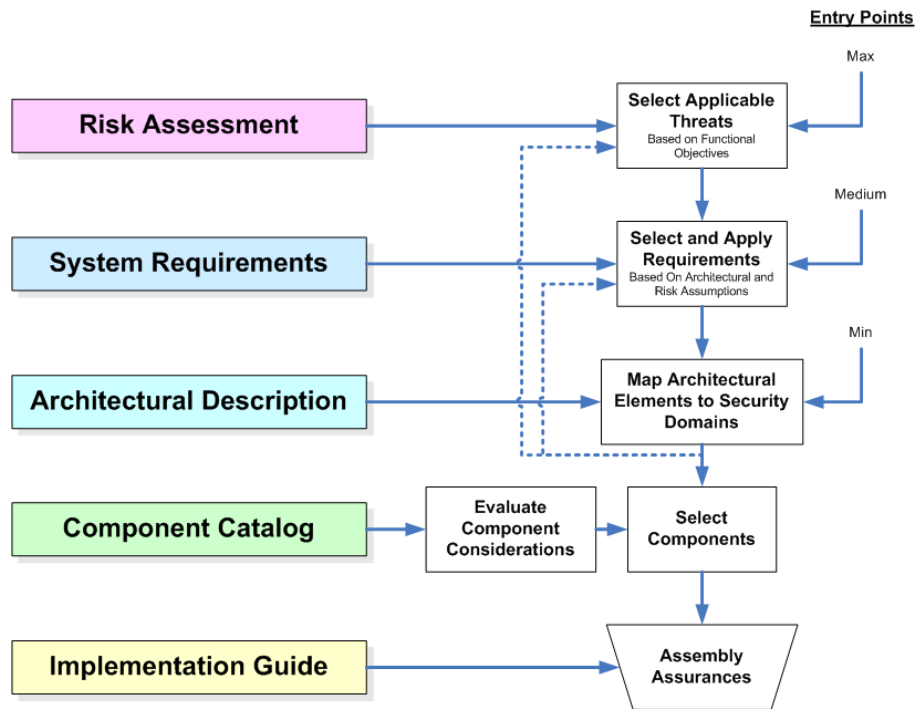


Figure 1 – Deliverables Process Flow

342
343
344
345
346
347

Maximum Level of Resources. For a utility with the ability to apply the maximum level of resources, the process to take is the following:

- Step 1 The utility will tailor the AMI-SEC Risk Assessment to their particular environment, constraints, and risk acceptance limits.
- Step 2 The utility selects which requirements apply to their potential solution architecture by combing through the AMI-SEC System Security Requirements document and assigning priority to the requirements they need in order to adequately mitigate risks.
- Step 3 The utility maps the significant Architectural Elements of potential solutions against the defined Security Domains and places selected and prioritized requirements on Architectural Elements according to the elements' placement within the Security Domains.

348
349
350

Medium Level of Resources. For a utility with a moderate (“medium”) level of resources, the process to undertake is the following:

- Step 1 The utility will review the System Security Requirements document and select which requirements apply to their potential solution architecture.
- Step 2 The utility maps the significant Architectural Elements of potential solutions against the defined Security Domains.
- Step 3 The utility accepts the AMI-SEC Risk Assessment without any modification or customization, but bears the responsibility for combing through the AMI-SEC System Security Requirements document
- Step 4 The utility assigns priority to the requirements they need to adequately mitigate risks.
- Step 5 Once the utility has selected and prioritized requirements, the requirements are placed on Architectural Elements according to the elements' placement within the Security Domains.

351
 352 **Minimum Level of Resources.** For a utility looking to utilize the minimal level of resources, the
 353 process to undertake is the following:

- Step 1 The utility will review the Architectural Description document and map the significant Architectural Elements of potential solutions against the defined Security Domains.
- Step 2 The utility accepts the AMI-SEC Risk Assessment without any modification or customization.
- Step 3 The utility accepts the AMI-SEC System Security Requirements as a whole without selecting any particular subset as applicable to their environment.
- Step 4 Requirements are placed on Architectural Elements according to the elements' placement within the Security Domains. In this scenario, the utility pushes the entire set of requirements on to the vendor. The onus lies with the vendor to push back and indicate where requirements are applicable and where they are not.

354

355 **1.3. Definitions, acronyms, and abbreviations**

356 Rather than produce an exhaustive list of AMI and security terms, links have been provided to
 357 well known, extensively used definitions, acronyms and abbreviations. Other terminology is
 358 addressed as encountered throughout this document.

359

Resource	Location
SmartGridipedia	http://www.smartgridipedia.org
NIST IR 7298 - Glossary of Key Information Security Terms	http://csrc.nist.gov/publications/nistir/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf
International Electrotechnical Commission 62351-2 Security Terms	http://std.iec.ch/terms/terms.nsf/ByPub?OpenView&Count=-1&RestrictToCategory=IEC%2062351-2
Electropedia	http://www.electropedia.org/

360

361

Table 1 - Terminology References

362 **1.4. References**

363 Advanced Metering Infrastructure (AMI) Program – AMI Use Case (Draft). 2006. Southern
 364 California Edison. Retrieved from
 365 [http://www.sce.com/PowerandEnvironment/smartconnect/open-](http://www.sce.com/PowerandEnvironment/smartconnect/open-innovation/usecasechart.htm)
 366 [innovation/usecasechart.htm](http://www.sce.com/PowerandEnvironment/smartconnect/open-innovation/usecasechart.htm)

367 Clements, P.; Bachmann, F.; Bass, L.; Garlan, D.; Ivers, J.; Little, R.; Nord, R.; & Stafford, J.
 368 *Documenting Software Architectures: Views and Beyond*. 2002. Boston, MA: Addison-
 369 Wesley.

370 Department of Homeland Security, National Cyber Security Division. 2008, January. Catalog of
371 Control Systems Security: Recommendations for Standards Developers. Retrieved from
372 http://www.us-cert.gov/control_systems/

373 Federal Information Processing Standard (FIPS) 140-2. 2004, March 24. National Institute of
374 Standards and Technology Information Technology Library – Computer Security
375 Division – Computer Security Resource Center Cryptographic Module Validation
376 Program (CMVP). Retrieved from <http://csrc.nist.gov/groups/STM/cmvp/>

377 Houseman, Doug and Frances Cleveland. 2008. Scope of Security Requirements for Business
378 Processes. Retrieved from
379 <http://osgug.ucauiug.org/utilisec/amisec/Reference%20Material/Forms/AllItems.aspx>

380 IEEE Standard 1471-2000. 2000. IEEE Recommended Practice for Architectural Description of
381 Software-Intensive Systems, by IEEE Computer Society.

382 National Institute of Standards and Technology. 2007, December. NIST SP 800-53 Rev. 2 -
383 Recommended Security Controls for Federal Information Systems. NIST Information
384 Technology Library – Computer Security Division – Computer Security Resource Center
385 Special Publications. Retrieved from <http://csrc.nist.gov/publications/PubsSPs.html>

386 National Institute of Standards and Technology. 2007, September 28. NIST SP 800-82 - Guide to
387 Industrial Control Systems (ICS) Security (2nd DRAFT). NIST Information Technology
388 Library – Computer Security Division – Computer Security Resource Center Special
389 Publications (SP). Retrieved from <http://csrc.nist.gov/publications/PubsSPs.html>

390 North American Electric Reliability Corporation. 2006, June 1. NERC Critical Infrastructure
391 Protection (CIP). Retrieved from <http://www.nerc.com/page.php?cid=2|20>

392 The Common Criteria. 2007, September. Common Criteria v3.1 – Part 2: Security Functional
393 Requirements Release 2. The Common Criteria. Retrieved from
394 <http://www.commoncriteriaportal.org/thecc.html>

395 The Common Criteria. 2007, September. Common Criteria v3.1 – Part 3: Security Assurance
396 Requirements Release 2. The Common Criteria. Retrieved from
397 <http://www.commoncriteriaportal.org/thecc.html>

398 **2. General system description**

399 **2.1. Use Cases**

400 AMI Use Cases have been organized into five different categories consistent with the primary
401 value streams they support. These five categories/value streams are:

- 402 • Billing

- 403 • Customer
- 404 • Distribution System
- 405 • Installation
- 406 • System

407 Reference 2.A - Business Functions as Stakeholders in AMI Systems provides additional
408 extensions to the use cases presented here, as well as describing business functions and
409 scenarios.

410 **2.1.1. Billing**

411 There are four primary use cases in the Billing category.

- 412 1. Multiple Clients Read Demand and Energy Data Automatically from Customer Premises
- 413 2. Utility remotely limits usage and/or connects and disconnects customer
- 414 3. Utility detects tampering or theft at customer site
- 415 4. Contract Meter Reading (or Meter Reading for other Utilities)

416 1 and 4 are directly related to the electronic capture and processing of time-based energy and
417 demand data from customer meters to support the core Billing process of the electric utility (1)
418 or, on a contract basis, for a gas or water utility (4) . The other Billing Use Cases explore other
419 functionality that can be leveraged from having installed AMI meters in the field. Use case 2
420 explores utilization of the remote connect/disconnect functionality of AMI meters. Use case 3
421 considers how AMI meters and the data they capture can be leveraged to support the detection of
422 energy theft.

423 Business value in the Billing area is created in several different ways. By automating the
424 collection of time-based energy usage and demand, the utility is able to significantly transform
425 the process for collecting energy and demand information to support the billing process. The
426 traditional process for collecting meter data (manually recording meter dial settings on a monthly
427 basis) is replaced by a fully automated, electronic capture process. Because the energy data is
428 captured in intervals of time (typically 15 minute intervals), AMI systems enable time-based
429 rates. Time-based billing rates vary throughout the day, reflecting changes in the balance
430 between energy supply and demand. Although the primary implementers of AMI have been
431 electric utilities, the potential exists for the infrastructure to be leveraged to capture gas and
432 water meter data as well – either for the host utility if they deliver those commodities or for
433 another utility (on a contract basis).

434 Other business value accrues from functionality that the AMI meters can provide. AMI meters
435 typically are outfitted with remote connect and remote disconnect capability. This allows the
436 utility to initiate or terminate service remotely, without having to send a field technician. This
437 functionality supports the routine Move-In/Move-Out processes as well as the credit/collections
438 processes. Disconnects for non-payment (and subsequent reconnects) can be accomplished
439 remotely rather than requiring on-site presence. AMI meters also come with functionality
440 that can help utilities identify potential meter tampering or energy theft/diversion.

441 Finally, AMI provides a wealth of data that various entities within the utility to use to create
442 additional business value. These areas include the following:

- 443 • Distribution system design – granular data on actual customer energy usage can be
- 444 utilized for more optimal design of distribution system components
- 445 • Distribution planning – the utility has a wealth of usage and demand data by circuit that
- 446 can be analyzed to better target investments in new distribution facilities to meet growth
- 447 in demand
- 448 • Distribution operations and maintenance – the Distribution organization has a wealth of
- 449 data for improved state estimation, contingency planning, and asset management
- 450 • Marketing – AMI data can be analyzed to develop energy services/products to meet
- 451 customer needs

452 The following table summarizes the major business processes supported by the Billing Use
 453 Cases and the key areas of business value that they enable.
 454

Use Case 1: Auto-Capture Customer Energy and Demand Data		
Major Processes Supported	Business Value	Security Concerns
<ul style="list-style-type: none"> • Read Meters • Validate Meter Reads • Generate Customer Bills 	<ul style="list-style-type: none"> • Eliminate meter reader labor cost and meter reading infrastructure cost • Increase billing accuracy • Enable time-based rates • Enable improved <ul style="list-style-type: none"> ○ Distribution system design ○ Distribution planning ○ Distribution operations and maintenance ○ Marketing 	Confidentiality (privacy) of customer data Integrity of meter data Availability of meter data (for remote read)
Use Case 2: Remote Connect/Disconnect		
Major Processes Supported	Business Value	Security Concerns
<ul style="list-style-type: none"> • Establish service • Terminate service • Manage credit/collection 	<ul style="list-style-type: none"> • Reduce field service truck rolls <ul style="list-style-type: none"> ○ Labor ○ Transportation • Reduce bad debt • Reduce energy losses 	Integrity of signal (correct message and location) Confidentiality (privacy) of signal Availability of connect/disconnect service
Use Case 3: Tamper Detection		
Major Processes Supported	Business Value	Security Concerns
<ul style="list-style-type: none"> • Protect revenue; reduce energy theft 	<ul style="list-style-type: none"> • Reduce lost revenue 	Integrity of tamper indication Availability of tamper indication Confidentiality (privacy) of location data
Use Case 4: Meter Reading for Other Utilities		
Major Processes Supported	Business Value	Security Concerns
<ul style="list-style-type: none"> • Read gas/water meters 	<ul style="list-style-type: none"> • Eliminate meter reader labor cost and meter reading 	Confidentiality (privacy) of customer data

<ul style="list-style-type: none"> • Read gas/water meters (other utilities) • Transfer meter reading data to other utility 	infrastructure cost <ul style="list-style-type: none"> • Create additional source of revenue • Leverage AMI investment 	Integrity of meter data Availability of meter data (for remote read) Availability of meter data to contracting utility through B2B infrastructure
---	--	---

455

Table 2 – Billing Use Cases

456 **2.1.2. Customer**

457 Four Use Cases have also been defined under the category of Customer:

- 458 1. Customer reduces their usage in response to pricing or voluntary load reduction events
- 459 2. Customer has access to recent energy usage and cost at their site
- 460 3. Customer prepays for electric services
- 461 4. External clients use the AMI to interact with devices at customer site

462 Use Case 1 explores how the AMI system, working together with customers, can create
 463 mutually-beneficial programs to manage energy demand/consumption. Use Case 2 is related to 1
 464 in that it describes ways that customers can access information about their energy costs and
 465 consumption, and how they can receive messaging from the utility informing the customer of an
 466 upcoming peak energy event, requiring/requesting customer load reductions. Customer Use
 467 Case 4 is directly related to the previous use cases as well in that it describes how a customer’s
 468 energy cost/consumption data can be shared with a third party energy service provider to
 469 outsource the customer’s energy consumption. Use Case 3 describes how AMI functionality can
 470 be leveraged to enable customer pre-payment for energy.

471 The primary business value in the Customer Use Cases comes from an enhanced ability to
 472 manage peak load on the distribution network. By communicating pricing signals and upcoming
 473 peak load events to customers, customers can modify their energy consumption behavior to
 474 reduce their energy costs. The utility benefits by reducing the potential for outages resulting
 475 from overload of the system and deferring new capital investments to provide increased capacity.
 476 Another source of business value unique to Use Case 3 (Customer Prepayment) accrues to the
 477 utility through reduction in bad debt and improved cash flow.

478 The following table summarizes the major business processes supported by the Customer Use
 479 Cases and the key areas of business value that they enable.

480

Use Case 1: Demand Response / Load Reduction		
Major Processes Supported	Business Value	Security Concerns
<ul style="list-style-type: none"> • Manage Energy Demand/Consumption 	<ul style="list-style-type: none"> • Reduce peak load <ul style="list-style-type: none"> ○ Defer new construction ○ Green benefits ○ Reduce outages 	Confidentiality (access control) of customer equipment Integrity of control messaging and message information Availability of customer devices
Use Case 2: Customer Access to Energy Data		
Major Processes Supported	Business Value	Security Concerns
<ul style="list-style-type: none"> • Provide Energy 	<ul style="list-style-type: none"> • Customer energy awareness 	Confidentiality (access control)

Information to Customers and Third Parties	<ul style="list-style-type: none"> • Reduce peak load 	of customer equipment via price signals and messages Integrity of control messaging and message information Availability of customer devices
Use Case 3: Customer Prepayment		
Major Processes Supported	Business Value	Security Concerns
<ul style="list-style-type: none"> • Collect Revenue from Energy Sales 	<ul style="list-style-type: none"> • Reduce bad debt • Improve cash flow • Improve customer convenience/satisfaction 	Confidentiality (privacy) of customer data and payments Integrity of control messaging and message information containing prepayment data Availability of customer payment data and usage balances
Use Case 4: Third Party Energy Management		
Major Processes Supported	Business Value	Security Concerns
<ul style="list-style-type: none"> • Manage Energy Demand/Consumption 	<ul style="list-style-type: none"> • Reduce peak load • Customer satisfaction 	Confidentiality (privacy) of customer data Integrity of usage data, rate information Availability of usage data, rate information

481

Table 3 - Customer Use Cases

482 **2.1.3. Distribution System**

483 Four Use Cases have been defined for the Distribution System category:

- 484 1. Distribution Operations curtails customer load for grid management
- 485 2. Distribution Engineering or Operations optimize network based on data collected by the
- 486 AMI system
- 487 3. Customer Provides Distributed Generation
- 488 4. Distribution Operator locates Outage Using AMI Data and Restores Service

489 Distribution System Use Case 1 is similar to Customer Use Case 1. Both use cases describe the

490 process to send signals to customers for the purpose of reducing load on the system, typically

491 during a system peak. Customer Use Case 1 describes demand response events that the customer

492 can voluntarily participate in using a price signal or a load control signal that the customer may

493 ignore. Distribution System Use Case 1 describes demand response events that are non-voluntary

494 using load control signals or meter disconnection commands. Distribution Use Case 2 explores

495 how data gathered by the AMI system can be utilized (either online or offline) to improve power

496 quality and the overall performance of the distribution network. Distribution Use Case 3

497 describes how the AMI system can interface with distributed generation (small, customer-owned

498 generation) to improve network operations and reduce off-system energy purchases. Use Case 4

499 investigates how the AMI system can be leveraged to support the identification of outages on the

500 system and to facilitate the restoration of power following an outage.

501 The primary areas of business value in the Distribution System Use Cases are related to
 502 improving network operations. Optimizing network operations can result in reduced energy
 503 losses, reduced outage frequency, and increased customer satisfaction (improved power quality).
 504 In addition, Use Case 4 explicitly describes processes to reduce outage duration and, therefore,
 505 customer satisfaction.
 506 The following table summarizes the major business processes supported by the Distribution
 507 System Use Cases and the key areas of business value that they enable.
 508

Use Case 1: Emergency Demand Response		
Major Processes Supported	Business Value	Security Concerns
<ul style="list-style-type: none"> • Manage Energy Demand/Consumption 	<ul style="list-style-type: none"> • Reduce peak load <ul style="list-style-type: none"> ○ Defer new construction ○ Reduce outages 	Confidentiality (access control) of customer equipment (including remote service switch and HAN devices) Integrity of control messaging and message information Availability of customer devices
Use Case 2: Distribution Network Optimization		
Major Processes Supported	Business Value	Security Concerns
<ul style="list-style-type: none"> • Manage Power Quality • Optimize Distribution Network • Manage Outages 	<ul style="list-style-type: none"> • Customer satisfaction • Reduce energy losses • Improve outage performance 	Integrity of system data Availability of system data Confidentiality of system data
Use Case 3: Distributed Generation		
Major Processes Supported	Business Value	Security Concerns
<ul style="list-style-type: none"> • Optimize Distribution Network • Manage/Dispatch Distributed Resources 	<ul style="list-style-type: none"> • Network Optimization • Reduced Off-System Energy Purchases 	Integrity of system data Availability of system data Confidentiality of system data
Use Case 4: Outage Location and Restoration		
Major Processes Supported	Business Value	Security Concerns
<ul style="list-style-type: none"> • Manage outages 	<ul style="list-style-type: none"> • Reduced outage duration • Customer satisfaction 	Availability of system data Integrity of system data Confidentiality of system data

509 **Table 4 - Distribution Use Cases**

510 **2.1.4. Installation**

511 Three Use Cases have been defined for the Installation category:

- 512 1. Utility installs, provisions, and configures the AMI system
- 513 2. Utility Manages End-to-End Lifecycle of the Meter System
- 514 3. Utility upgrades AMI to address future requirements.

515 Use Case 1 describes the process for deploying an AMI system, including the initial deployment
 516 plan, the forecasting and procurement process, logistical support, and field
 517 installation/testing/configuration. Use Case 2 focuses on managing the AMI system components
 518 through their life cycle, including maintenance and asset retirement. Use Case 3 explores future
 519 upgrades to the AMI system functionality and performance with particular attention to future
 520 deployment and integration of customer Home Area Network (HAN).
 521 The key areas of business value in the Installation Use Cases include optimization of deployment
 522 costs and schedule for AMI system implementation, minimizing AMI operations and
 523 maintenance costs, maintaining billing accuracy, minimizing risk, and accommodating future
 524 growth and development within the AMI infrastructure.
 525 The following table summarizes the major business processes supported by the Distribution
 526 System Use Cases and the key areas of business value that they enable.
 527

Use Case 1: AMI System Deployment		
Major Processes Supported	Business Value	Security Concerns
<ul style="list-style-type: none"> • Deploy AMI system 	<ul style="list-style-type: none"> • Optimize deployment costs/schedule 	Integrity of system data for registration Availability of system data supporting deployment and registration Confidentiality of system data
Use Case 2: AMI System Maintenance		
Major Processes Supported	Business Value	Security Concerns
<ul style="list-style-type: none"> • Maintain AMI system 	<ul style="list-style-type: none"> • Minimize AMI O&M costs • Maintain billing accuracy 	Integrity of system data for remote diagnostics Availability of system data supporting maintenance and work orders Confidentiality of system data
Use Case 3: AMI System Upgrade		
Major Processes Supported	Business Value	Security Concerns
<ul style="list-style-type: none"> • Upgrade/enhance AMI system functionality/performance • Deploy/support customer HAN 	<ul style="list-style-type: none"> • Minimize risk • Accommodate growth and future functionality 	Integrity of system data for registration of new devices and remote firmware upgrades Availability of system data supporting deployment and remote upgrades Confidentiality of system data and customer data

528 **Table 5 - Installation Use Cases**

529 **2.1.5. System**

530 The final Use Case category is System. Only one Use Case has been defined for this category:

- 531 1. AMI system recovers after outage, communications or equipment failure.

532 System Use Case 1 explores how the AMI system responds and recovers to individual
 533 component failures, communications failures, and broader outages/disasters. The primary
 534 business value in this use case comes from maintaining AMI system integrity through unplanned
 535 equipment failures or distribution system outages.

Use Case 1: AMI System Recovery		
Major Processes Supported	Business Value	Security Concerns
<ul style="list-style-type: none"> Recover from AMI component and telecommunications failures Recover from major area outages/disasters 	<ul style="list-style-type: none"> Maintain system integrity 	Integrity of system data Availability of system data Confidentiality of system data

536 **Table 6 - AMI System Use Cases**

537 **2.2. System Context**

538 AMI is the convergence of the power grid, the communications infrastructure, and the supporting
 539 information infrastructure. However, AMI security must exist in the real world with many
 540 stakeholders, other interested parties and overlapping responsibilities.

541
 542 Consider an individual system that is part of an AMI solution to be made up of: 1) Software; 2)
 543 Hardware; 3) People and; 4) Information. Now, consider the entire AMI solution to be made up
 544 of a collection of various systems, each made up of software, hardware, workers and information
 545 – a system of systems. Systems-of-Systems are hierarchical in nature, that is, they naturally
 546 break down into parts.

547
 548 The value of a logical decomposition comes from its ability to view a complex system at
 549 multiple levels of abstraction (decomposition) while maintaining forward and reverse traceability
 550 through the different levels of decomposition. Logical decomposition is can also be mapped to
 551 physical decomposition to correlate the model elements. The security domain model shown
 552 below (Figure 2) was developed to boundary the complexity of specifying the security required
 553 to implement a robust, secure AMI solution as well as serve as a tool to guide utilities in
 554 applying the security requirements in this document to their AMI implementation.

555
 556

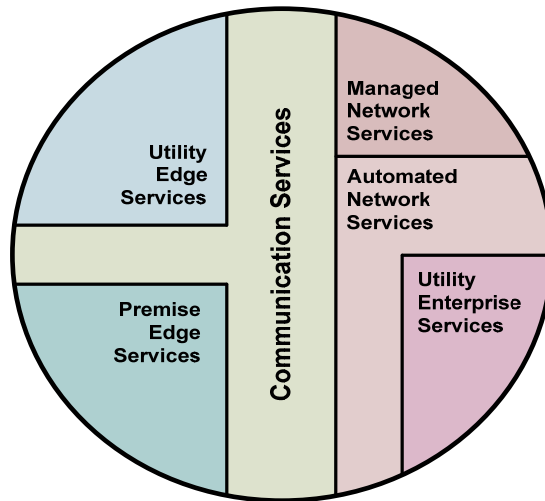


Figure 2 – AMI Security Domain Model

557
558
559
560
561
562
563

The following “services” are a description of each of the six security domains shown in the model above.

Security Domain	Description
Utility Edge Services	All field services applications including monitoring, measurement and control controlled by the Utility
Premise Edge Services	All field services applications including monitoring, measurement and control controlled by the Customer (Customer has control to delegate to third party)
Communications Services	are applications that relay, route, and field aggregation, field communication aggregation, field communication management information
Management Services	attended support services for automated and communication services (includes device management)
Automated Services	unattended collection, transmission of data and performs the necessary translation, transformation, response, and data staging
Business Services	core business applications (includes asset management)

564
565
566
567
568
569
570

Table 7 - AMI Security Domain Descriptions

Each utility’s AMI implementation will vary based on the specific technologies selected, the policies of the utility company and the deployment environment. The application of the security requirements should guide the AMI system’s capabilities.

571 Advanced Metering Infrastructure system use can be mapped across applicable security domains
 572 based on the collection of capabilities that enable use of the AMI. Security requirements in this
 573 document shall map to specific security domains based on the location of an enabling capability
 574 that enables a particular use for the AMI system. For any particular use of the AMI system, in
 575 the context of the enabling capability, the security requirements for that domain should be
 576 applied.

577
 578 For example: If the use of the AMI system is “Remote Service Switch Operation” to support a
 579 customer “move-in” or “move-out” event then the analysis of which security requirements would
 580 apply for this use would be to map sequence of capabilities to domains.

581 *(Note: there are a number of intermediate steps related to account updates, customer*
 582 *verification, policy enforcements and validations as well as error conditions not shown in this*
 583 *example.)*

584

Process step	Enabling Capabilities (components)	Security Domain
Triggering event – Move-out request received from customer for a particular time and date	Request received via call center or via web (IVR or Company Website)	Utility Enterprise Services
Switch operation scheduled and validated	Customers Information System (CIS) or Meter Data Management Systems (MDMS)	Utility Enterprise Services
Command messages generated at scheduled time	CIS or MDMS	Utility Enterprise Services
Command received by head-end system	Network Management System (aka DCA or head-end)	Automated Network Services
Grid protection module validates command against rules (i.e. how many total service switch commands are pending in the next 10 min.)	Network Management System	Automated Network Services
Command transmitted to Meter	Network Management System	Automated Network Services
Command routed to the customer’s meter	Wide-Area Network, Neighborhood Area Network (aka LAN)	Communication Services
Command received by meter	Meter	Utility Edge Services
Service Switch “opened”	Meter	Utility Edge Services
Acknowledgement message created	Meter	Utility Edge Services
Acknowledgement message transmitted	Wide-Area Network, Neighborhood Area Network (aka LAN)	Communications Services
Acknowledgement message	Network Management System	Automated Network Services

received		
Account status updated	CIS and or MDMS	Utility Enterprise Services

585
586 **Table 8 - Mapping of AMI Security Domain Services to Utility Processes**
587

588 It should be noted that this specification and the method of mapping security requirements to
589 specific domains based on use is lifecycle agnostic. Meaning, some uses of the system (i.e. key
590 placement in devices) may happen prior to the commencement of operations.
591

592 **2.3. System Constraints**

593 A number of system constraints need to be taken into account when satisfying security
594 requirements found in this document. The requirements described do not prescribe which of a
595 range of solutions (e.g., the use of narrow- or wide-band communications technologies) is most
596 appropriate in a given setting. Such a decision is typically based on making prudent trade-offs
597 among a collection of competing concerns, such as the following
598

- 599 • Other business or non-functional requirements
 - 600 ○ Performance (e.g., response time)
 - 601 ○ Usability (e.g., complexity of interactions for users)
 - 602 ○ Upgradability (e.g., ease of component replacement)
 - 603 ○ Adaptability (e.g., ease of reconfiguration for use in other applications)
 - 604 ○ Effectiveness (e.g., information relevant and pertinent to the business process as
605 well as being delivered in a timely, correct, consistent and usable manner)
 - 606 ○ Efficiency (e.g., the provision of information through the most productive and
607 economical use of resources)
 - 608 ○ Confidentiality (e.g., protection of sensitive information from unauthorized
609 disclosure)
 - 610 ○ Integrity (e.g., accuracy, completeness and validity of information in accordance
611 with business values and expectations)
 - 612 ○ Availability (e.g., information being available when required by the business
613 process)
 - 614 ○ Compliance – (e.g., complying with the laws, regulations and contractual
615 arrangements)
 - 616 ○ Reliability (e.g., the provision of appropriate information for management to
617 operate the entity and exercise its fiduciary and governance responsibilities)

618
619 It is important to consider system constraints when developing applying security requirements.
620 The requirements themselves do not take into account the trade-offs involved with design phase
621 of AMI. Therefore, satisfying these requirements should not be done in isolation from the design.
622

- 623 • Constraints
 - 624 ○ Computational (e.g., available computing power in remote devices)
 - 625 ○ Networking (e.g., bandwidth, throughput, or latency)
 - 626 ○ Storage (e.g., required capacity for firmware or audit logs)
 - 627 ○ Power (e.g., available power in remote devices)

- 628 ○ Personnel (e.g., impact on time spend on average maintenance)
- 629 ○ Financial (e.g., cost of bulk devices)
- 630 ○ Temporal (e.g., rate case limitations)
- 631 ○ Technology
- 632 ○ Availability
- 633 ○ Maturity
- 634 ○ Integration / Interoperability (e.g., legacy systems)
- 635 ○ Lifecycle
- 636 ○ Interconnectedness of infrastructure
- 637 ○ Applications (e.g., the automated user systems and manual procedures that
- 638 process the information)
- 639 ○ Information (e.g., the data, in all their forms, input, processed and output by the
- 640 information systems in whatever form is used by the business)
- 641 ○ Infrastructure (e.g., the technology and facilities i.e., hardware, operating systems,
- 642 database management systems, networking, multimedia, and the environment that
- 643 houses and supports them, that enable the processing of the applications.)
- 644 ○ People (e.g., the personnel required to plan, organize, acquire, implement,
- 645 deliver, support, monitor and evaluate the information systems and services. They
- 646 may be internal, outsourced or contracted as required.)
- 647 ○ Time
- 648 ○ Financial
- 649 ○ Technical
- 650 ○ Operational
- 651 ○ Cultural
- 652 ○ Ethical
- 653 ○ Environmental
- 654 ○ Legal
- 655 ○ Ease of Use
- 656
- 657 ● Regulatory requirements
 - 658 ○ Scope / sphere of influence
 - 659 ○ Acceptance vs. transference

660 **2.4. Security States and Modes**

661 This section discusses the states and modes that may apply to the system as a whole and/or the
 662 component level. A component may be a sub-system or individual element of the system.
 663 Security modes and states are considered in the evaluation of security requirements because they
 664 pose special circumstances for which the requirements may change. Evaluating these special
 665 circumstances is important because in any given state or mode the risk of a system or sub-system
 666 component may increase or decrease, thus needing supplemental requirement treatment (less or
 667 more).

668
 669 Definitions of terms:

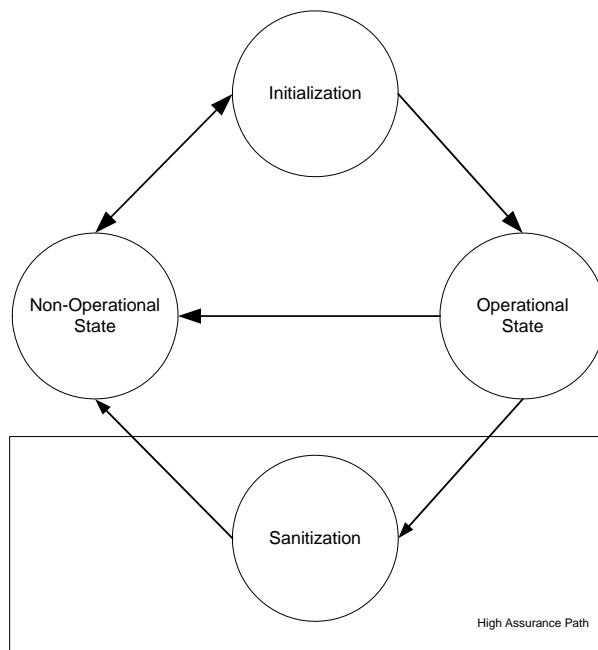
- 670 ● State – a temporal condition of a system or component; implies a “snapshot”.
 - 671 ○ Typically within a time-based consideration
 - 672 ○ Sometimes overlap

673 • Mode – describes operational intent (implies action taken).

674 2.4.1. System States

675 The term *state* for the purposes of this document implies a snapshot of the system. The goal is to
676 identify the state as they relate to security.

677
678 The System State Flow Diagram (Figure 3) assists in understanding the transition between states
679 and the direction in which changes in state are allowed to occur. The System State Flow Diagram
680 is used in defining the AMI system transitions. It is important to understand and control state
681 flow in order to prevent an undesired, inadvertent system state. Transition of states for security
682 components should be defined and understood with respect to defining requirements. The
683 Sanitization State is also a shown as a path where high assurance is required.
684



685
686
687
688
689
Figure 3 - Example of a System State Flow Diagram

System State	Description
Operational	Includes all functionality supportive of on-going operations (set by policy)
Non-operational	Not performing functionality indicative of on-going operations
Initialization	Used to configure system prior to operation
Sanitization	Removal and/or storing of information representative or residual of any running condition (e.g., sensitive data)

690
691

Table 9 - System States

692

693 **2.4.1.1. System State Security Requirements**

- State.1 Activities allowed during non-operational state shall be limited to system activities needed to enter initialization. (Excludes interactions w/stakeholders, execution of business functions, etc.)
- State.2 Activities allowed during initialization state shall be limited to system activities needed to enter operations. (Excludes interactions w/stakeholders, execution of business functions, etc.)
- State.3 Activities allowed during initialization state shall include management functions necessary for element configuration.
- State.4 Activities allowed during the initialization state shall include policy establishment (i.e., creation and configuration).
- State.5 Activities allowed during the initialization state shall include security domain establishment.
- State.6 A system shall transition into the operational state only upon completion of the critical initialization activities.
- State.7 An operational system shall perform only those activities conformant to policy.
- State.8 A system shall be capable of operating in a degraded mode while in an operational state. In this mode, “degraded” refers to a system that has non-operational or impaired components/elements. While services may be denied to some components/elements in the degraded mode, critical functions and security features of the system are still in force for the remaining components/elements.
- State.9 A system shall transition into the non-operational state upon detection of a critical failure.
- State.10 Supporting activities pertaining to the health of the system (e.g., diagnostics, maintenance, training, etc.) shall only be allowed during the operational state. Support activities may be performed in other system states, however they will be performed by systems external to the SUD.

694

695 **2.4.2. System Modes**

696 At the highest level, a system or component can be placed into a “normal” or “limited” mode of
697 operation. At a minimum, modes should be taken into consideration during Protection Profile
698 development. In a Protection Profile, criteria for entering and exiting each mode should be
699 defined (pay close attention to risk associated with transition between modes – i.e., target mode
700 must be defined before leaving current mode). For a more granular analysis, one may consider
701 the following refinement examples:

- 702 • On-Line/Off-Line – system or element is accessible (or non-accessible) from a
703 communication point of view
- 704 • Lock – certain functions are not accessible / intentionally disabled
- 705 • Maintenance – configuring / patching
- 706 • Diagnostics – monitoring for purposes of problem resolution (i.e., debugging)
- 707 • Commissioning/Decommissioning – initialization/establishment of functionality or service
708 (decommissioning is reverse)
- 709 • Learning – acquiring new parameters and/or functionality for purposes of optimization
- 710 • Training – utilizing system functions for purposes of familiarization and simulation. (“Real”
711 outputs are not engaged.)
- 712 • Sleep/Power saving – certain functions are temporarily disabled or degraded for decreased
713 energy consumption.
- 714 • Special/Emergency – configurations based on criticality of function and preferential and/or
715 prioritized treatment of certain operations. (Example needed, i.e., impending natural
716 disaster.)

717 **2.5. Security Objectives**

718 As currently envisioned, Smart Grid services promise unprecedented levels of automation,
719 situational awareness, and fine-grained control of the generation, transmission, distribution and
720 use of electric power. If fully realized, such services should significantly increase the
721 effectiveness, efficiency and reliability of the electric power system providing lower operating
722 costs associated with many of today's labor-intensive tasks and would provide the incentives and
723 technical capability for customers to automatically manage their usage patterns. Customers
724 would specify demand-response usage policies based on pricing signals from the market or
725 would permit direct supplier control of end-user load (automatically shedding load to reduce
726 peak demand or mitigate emergency situations). In conjunction with end-user control, demand
727 response would make the most efficient use of available generating capacity, while supporting
728 conservation and environmental efforts.

729
730 Smart Grid services typically require complex distributed applications (some with near real-time
731 constraints), communication over highly-networked information infrastructures, that include a
732 broad range of Internet technologies. For the vision of the Smart Grid to be realized, system
733 security must be maintained at a consistently high levels of assurance. Security concerns must
734 be addressed from the outset of any Systems Development Life Cycle (SDLC) activity
735 throughout every systems engineering, including architecture, acquisition, implementation,
736 integration, deployment, operations, maintenance, and decommissioning. Security solutions must
737 be comprehensive or *holistic* in nature (obligatory clichés: you’re only as strong as your weakest
738 line” and "the devil is in the details") and capable of evolving in response to changes in the threat
739 or technological environment.

740
741 The Smart Grid's primary (cyber) security objectives are as follows:
742

- 743• Protect all Smart Grid services from malicious attack¹ and unintended adverse cyber and
744 physical events that threaten the mission of the service (i.e., *security events*).
- 745 ○ Ensure that sufficient information about a security events are available when and where
746 needed to support the decision making necessary to protect (or minimize the disruption
747 to) the mission of the affected Smart Grid service. This includes the collection and
748 delivery of the real-time data needed for situational awareness as well as the collection
749 and protection of forensics data needed for post-mortem analysis to improve the security
750 and survivability of the system in the face of future security events.
 - 751 ○ Ensure the integrity, availability, and (where appropriate) the confidentiality of the
752 information regarding security services, survivability services and mechanisms used to
753 protect the Smart Grid services. These security and survivability services and
754 mechanisms shall not provide an attack vector or incorrectly respond to malicious or
755 benign stimuli in a manner that would create or worsen a security event.
- 756• Prevent security incidents associated with a Smart Grid service from contributing to or
757 complicating the safety and protection of personnel, stakeholders, stakeholder services and the
758 electrical system.
- 759 ○ Do not allow any Smart Grid service or its associated technology (e.g., communications
760 networks and gateways) to be used as a stepping stone or conduit for attacks (or
761 amplifying the effects of attacks) on other Smart Grid services, end users, external
762 service providers (e.g., cell phone networks, ISPs), or any other interconnected entity.
 - 763 ○ Smart Grid services shall not amplify the adverse effects of any accident, natural disaster,
764 or human error.
- 765• Provide sufficient evidence to support the assurance of justifiable confidence (i.e., trust) in the
766 integrity, confidentiality, and availability of Smart Grid services. (For example, provide
767 evidence to support public trust in the accuracy of billing statements, the safety and reliability of
768 electricity services, and the fairness of energy markets.)
- 769
- 770 Smart Grid security involves a system of systems approach in engineering design and operations,
771 which requires that security responsibility be extend beyond the Smart Grid. While security
772 requirements for the broader Smart Grid may or may not be within the scope of a single utility's
773 responsibility, imposing the requirements through agreements and/or regulatory mandates upon
774 cooperating interconnecting systems and corresponding capabilities will meet and/or support
775 some aspects of the Smart Grid security objectives. Moreover, interdependencies among the
776 power grid, the communications infrastructure, and the information infrastructure pose a
777 particularly serious challenge to the design of a secure and survivable Smart Grid.
- 778
- 779 As an example, AMI system security must protect the missions of all AMI business functions
780 and must not be allowed to be used as a conduit for attacking some method of control of the grid.
781 This does not imply that AMI security architects are solely responsible for ensuring this, but
782 rather that responsibility must be assigned for a systems of systems perspective wherein potential
783 AMI impacts on the larger grid are analyzed, anticipated, and defended against in some portion
784 of the overall system of systems (SoS) architecture and implementation.
- 785
- 786 Here are a few examples of what the Smart Grid security objectives are meant to prevent:

¹ Includes cyber and physical attacks, such as attempts to physically tamper with a meter, and disruption of the supporting communications infrastructure.

- 787
- 788
- 789
- 790
- 791
- 792
- 793
- 794
- 795
- 796
- 797
- 798
- 799
- 800
- 801
- 802
- 803
- 804
- 805
- 806
- 807
- Reputational Loss - Attacks or accidents that destroy trust in Smart Grid services, including their technical and economic integrity
 - Business Attack - Theft of money or services or falsifying business records
 - Gaming the system - Ability to collect, delay, modify, or delete information to gain an unfair competitive advantage (e.g., in energy markets)
 - Safety - Attack on safety of the grid, its personnel or users
 - Assets - Damaging physical assets of the grid or assets of its users
 - Short-term Denial or Disruption of Service
 - Long-term Denial or Disruption of Service (including significant physical damage to the grid)
 - Privacy violations
 - Hijacking control of neighbor's equipment
 - Physical and logical tampering
 - Subverting situational awareness so that operators take fatal actions that disrupt the system
 - Cause automated system to waste resources on false alarms.
 - Hijacking services
 - Using Smart Grid services or the supported communication mechanisms to attack end users residential or industrial networks (e.g., allowing end-users to compromise other end-users' networked systems.)

808 **2.5.1. Holistic Security**

809 The magnitude of the challenge posed by melding the complexity of the power grid with open,
810 distributed, highly networked technologies, crossing multiple organizational and administrative
811 boundaries, in the presence of intelligent adversaries, is such that traditional security approaches
812 alone are insufficient to meet them.

813

814 The primary concern is with protecting the business missions embodied in each of the Smart
815 Grid services individually and collectively, not merely in enforcing security requirements or
816 protecting IT components. *Survivability* is the capability of a system to fulfill its mission in a
817 timely manner despite attack, accident or subsystem failure. *Survivability* is a blend of security
818 and business risk management that builds upon traditional security approach by adding domain-
819 specific strategies and tactics to create a holistic perspective. The characteristics of a survivable
820 system include its ability to prevent or resist attacks, accidents, other forms of stress, recognize a
821 survivability event and the state of the system under stress and to recover from the adverse
822 impact of a survivability event in a timely manner. *Survivability* is marked by graceful
823 degradation under stress, with essential services maintained.

824 **2.6. User Characteristics**

825 Many of the security requirements within this document are written with respect to a generic
826 notion of an actor or user, rather than identifying specific users such as a maintenance engineer
827 or residential customer. When such a requirement is applied to an architectural element, it should
828 be tailored to specific types of users by taking into account the characteristics of each type of
829 user and how that informs the requirement.

830 Typical classes of users (at a high level) include (refer to the Contextual View for insight into
831 these classes of users)

- 832 • Utility
- 833 • Customer
- 834 • Third-party

835 Some of the characteristics that distinguish these classes of users, and even different types of
836 users within these classes, are:

- 837 • Organizational responsibility
- 838 • Organizational authority
- 839 • Ability to delegate authority
- 840 • Privileges within the domain
- 841 • Access of users

842 When tailoring a requirement, one might generate several versions of a requirement, each of
843 which differs by identifying a different user and requiring slightly different responses (e.g., level
844 of access control required for a given behavior).

845 **2.7. Assumptions and Dependencies**

846 This document is an ad hoc security specification, and as such does not contain requirements
847 pertaining to business (functional) requirements or quality of service (non-functional)
848 requirements (e.g., performance, usability, or maintainability issues). It is assumed that business
849 requirements have already been established for deploying an AMI solution. It does contain a
850 collection of security requirements that have been drawn from industry best practices and
851 government sources documenting best practices for security.

852
853 It is not the intent of this document to specify the security requirements for any particular AMI
854 system. Instead, the goal is to provide guidance likely to be suitable across a variety of different
855 AMI implementations. No assumptions are made regarding context specific characteristics such
856 as available computing, software and/or infrastructure resources, unless specifically cited. No
857 assumptions are made regarding the presence or absence of specific business requirements.

858
859 This document contains high-level requirements, not detailed specifications. Details such as
860 specific interfaces, algorithms, protocols, and technology solutions are not addressed. These
861 requirements should provide the impetus for the creation of more detailed specifications for AMI
862 systems, the specifics of which depend on each AMI system's context (e.g., actual assets and
863 information flows, business requirements, and detailed risk assessments).

864 **3. System Security Requirements**

865 The requirements found throughout this section are fine grained. A given section may contain
866 related requirements addressing the same need that differ in terms of the strength of mechanism,
867 rigor and protection each offers.

868 Requirements are given a lettering scheme as follows:

- 869 • Requirements that begin with an “F” are functional requirements.
- 870 • Requirements that end with an “S” are supporting services to functional requirements.
- 871 • Requirements that begin with an “A” are assurance requirements.
- 872 • Remaining letters in the identifier help associate the requirement to its requirement class.

873 **3.1. Primary Security Services**

874 This area uses business/mission needs to define requirements. It answers the question, “What
875 security is needed?”

876 **3.1.1. Confidentiality and Privacy (FCP)**

877 This class contains confidentiality and privacy requirements. These requirements provide a user,
878 service or object protection against discovery and misuse of identity by other users/subjects.
879

FCP.1	The security function shall ensure that [assignment: set of unauthorized users and/or subjects] are unable to determine the real user name bound to [assignment: list of subjects and/or operations and/or objects].
FCP.2	The security function shall provide [selection: an authorized user, [assignment: list of trusted subjects]] a capability to determine the user identity based on the provided alias only under the following [assignment: list of conditions].
FCP.3	The security function shall be able to provide [assignment: number of aliases] aliases of the real identity (e.g., user name) to [assignment: list of subjects].
FCP.4	The security function shall [selection, choose one of: determine an alias for a user, accept the alias from the user] and verify that it conforms to the [assignment: alias metric].
FCP.5	The security function shall provide an alias to the real user name which shall be identical to an alias provided previously under the following [assignment: list of conditions] otherwise the alias provided shall be unrelated to previously provided aliases.
FCP.6	The security function shall ensure that [assignment: list of users and/or subjects] are unable to determine whether [assignment: list of operations][selection: were caused by the same user, are related as follows[assignment: list of relations]].
FCP.7	The security function shall ensure that [assignment: list of users and/or subjects] are unable to observe the operation [assignment: list of operations] on [assignment: list of objects] by [assignment: list of protected users and/or subjects].
FCP.8	The security function shall allocate the [assignment: unobservability related information] among different parts of the module such that the following conditions hold during the lifetime of the information: [assignment: list of conditions].
FCP.9	The security function shall provide [assignment: list of services] to [assignment: list of subjects] without soliciting any reference to [assignment: privacy related information (e.g., real username)].
FCP.10	The security function shall provide [assignment: list of authorized users] with the capability to observe the usage of [assignment: list of resources and/or services].
FCP.11	The security function shall prevent unauthorized and unintended information transfer via shared system resources.
FCP.12	The functions provided by the security function to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding [assignment: quantification] for loss of security function data or objects under the control of the module's security function.
FCP.13	The security function shall protect security function data from unauthorized disclosure when it is transmitted between separate parts of the system.
FCP.14	The security function shall identify and handle error conditions in an expeditious manner without providing information that could be exploited by adversaries.
FCP.15	The authentication mechanisms in the system shall obscure feedback of authentication information during the authentication process to protect the information from possible exploitation or use by unauthorized individuals.
FCP.16	The security function shall ensure that the security attributes, when exported outside the system, are

unambiguously associated with the exported user data.

880

881 3.1.2. Integrity (FIN)

882 "Maintaining a control system, including information integrity, increases assurance that sensitive
883 data have neither been modified nor deleted in an unauthorized or undetected manner. The
884 security controls described under the system and information integrity family provide policy and
885 procedure for identifying, reporting, and correcting control system flaws. Controls exist for
886 malicious code detection, spam protection, and intrusion detection tools and techniques. Also
887 provided are controls for receiving security alerts and advisories and the verification of security
888 functions on the control system. In addition, there are controls within this family to detect and
889 protect against unauthorized changes to software and data, restrict data input and output, check
890 the accuracy, completeness, and validity of data, and handle error conditions." [DHS]
891

FIN.1	The security function shall preserve a secure state when the following types of failures occur: [List of types of failure in the module]
FIN.2	The security function shall provide the capability to detect modification of all security function data during transmission between the security function and another trusted IT product within the following metric: [assignment: a defined modification metric].
FIN.3	The security function shall provide the capability to verify the integrity of all security function data transmitted between the security function and another trusted IT product and perform [assignment: action to be taken] if modifications are detected.
FIN.4	The security function shall provide the capability to correct [assignment: type of modification] of all security function data transmitted between the security function and another trusted IT product.
FIN.5	The security function shall be able to detect [selection: modification of data, substitution of data, re-ordering of data, deletion of data, [assignment: other integrity errors]] for security function data transmitted between separate parts of the module.
FIN.6	Upon detection of a data integrity error, the security function shall take the following actions: [assignment: specify the action to be taken].
FIN.7	The security function shall provide detection of physical tampering that might compromise the module's security function.
FIN.8	The security function shall provide the capability to determine whether physical tampering with the module's security function's devices or module's security function's elements has occurred.
FIN.9	For [assignment: list of security function devices/elements for which active detection is required], the security function shall monitor the devices and elements and notify [assignment: a designated user or role] when physical tampering with the module's security function's devices or module's security function's elements has occurred.
FIN.10	The security function shall resist [assignment: physical tampering scenarios] to the [assignment: list of security function devices/elements] by responding automatically such that the integrity is maintained.
FIN.11	After [assignment: list of failures/service discontinuities] the security function shall enter a [assignment: mode (e.g., maintenance mode)] where the ability to return to a secure state is provided.
FIN.12	For [assignment: list of failures/service discontinuities], the security function shall ensure the return of the module to a secure state using automated procedures.
FIN.13	When automated recovery from [assignment: list of failures/service discontinuities] is not possible, the security function shall enter [assignment: mode (e.g., a maintenance mode)] where the ability to

	return to a secure state is provided.
FIN.14	The utility provided by the security function to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding [assignment: quantification] for loss of module's security function data or objects under the control of the module's security function.
FIN.15	If the security function and/or system experience failure or service discontinuity, the security function shall provide the capability to determine the objects that were or were not capable of being recovered; as a result, the following actions should be taken [assignment: action to be taken].
FIN.16	The security function shall detect replay for the following entities: [assignment: list entities].
FIN.17	The security function shall use [assignment: list of interpretation rules to be applied by the module's security function] to consistently interpret security function data from another trusted IT product.
FIN.18	The security function shall run a suite of tests [selection: during initial start-up, periodically during normal operation, at the request of an authorized user, [assignment: other conditions]] to check the fulfillment of [assignment: list of properties of the external entities]. If the test fails, the security function shall [assignment: action(s)].
FIN.19	The security function shall ensure that security function data is consistent when replicated between [assignment: parts of the system].
FIN.20	When parts of the module containing replicated security function data are disconnected, the security function shall ensure the consistency of the replicated security function data upon reconnection before processing any requests for [assignment: list of functions dependent on security function data replication consistency].
FIN.21	The security function shall run a suite of <i>self-tests</i> during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self-test should occur] to demonstrate the correct operation of [selection: [assignment: parts of security function (e.g. key management)], the module's security function.
FIN.22	The security function shall provide authorized users with the capability to verify the integrity of [selection: [assignment: parts of module's security function], security function data].
FIN.23	The security function shall provide authorized users with the capability to verify the integrity of stored security function executable code.
FIN.24	The security function shall verify the correct operation of security utilities [Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): notifies [assignment: user, etc. (e.g., system administrator), shuts the system down, restarts the system] when anomalies are discovered.
FIN.25	The security function shall detect and protect against unauthorized changes to software and information.
FIN.26	The security function shall restrict the capability to input information to the information system to authorized personnel.
FIN.27	The security function shall check information for accuracy, completeness, validity, and authenticity.
FIN.28	The organization shall handle and retain output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.
FIN.29	The organization shall develop, disseminate, and periodically review/update: <ol style="list-style-type: none"> 1. Formal, documented, system and control integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 2. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.
FIN.30	The organization shall identify, report, and remediate control system flaws per organizational, legal, and/or regulatory policies.

FIN.31	The security function employs malicious code protection.
FIN.32	The security function shall verify the correct operation of security functions within the control system upon system startup and restart; upon command by user with appropriate privilege; periodically; and/or at defined time periods. The security function notifies the [assignment: system administrator, system component, etc.] when anomalies are discovered.
FIN.33	The security function shall monitor and detect unauthorized changes to software and information.
FIN.34	The security function shall implement security measures to restrict information input to the control system to authorized personnel only.
FIN.35	The security function shall employ mechanisms to check information for accuracy, completeness, validity, and authenticity.
FIN.36	The organization shall handle and retain output from the security function in accordance with applicable laws, regulations, standards, and organizational policy, as well as operational requirements of the control process.
FIN.37	The security function shall protect the integrity of transmitted information.
FIN.38	The security function shall reliably associate [assignment: security parameters] with information exchanged between [assignment: information systems].
FIN.39	The security function that provides name/address resolution service for local clients shall perform data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.
FIN.40	The security function that collectively provides name/address resolution service for an organization shall be fault tolerant and implement role separation.
FIN.41	The security function shall protect security function data from modification when it is transmitted between separate parts of the system.
FIN.42	The security function shall mark output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.
FIN.43	The security function shall provide [assignment: list of subjects] with the ability to verify evidence of the validity of the indicated information and the identity of the [assignment: user, object, etc.] that generated the evidence.

892

893 **3.1.3. Availability (FAV)**

894 This involves the ability of the system to continue to operate and satisfy business/mission needs
895 under diverse operating conditions, including but not limited to peak load conditions, attacks,
896 maintenance operations, and normal operating conditions.

897

FAV.1	The security function shall ensure the operation of [assignment: list of system's capabilities] when the following failures occur: [assignment: list of type of failures].
FAV.2	The security function shall assign a priority to each subject in the system's security function in terms of availability.
FAV.3	The security function shall ensure that each access to [assignment: controlled resources] shall be mediated on the basis of the subjects assigned priority.
FAV.4	The security function shall ensure that each access to all shareable resources shall be mediated on the basis of the subjects assigned priority.
FAV.5	The security function shall enforce maximum quotas of the following resources: [assignment: controlled resources] that [selection: individual user, defined group of users, subjects] can use [selection: simultaneously, over a specified period of time].

FAV.6	The security function shall ensure the provision of minimum quantity of each [assignment: controlled resource] that is available for [selection: an individual user, defined group of users, subjects] to use [selection: simultaneously, over a specified period of time].
FAV.7	The security function shall protect against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined list of types of denial of service attacks or reference to source for current list].
FAV.8	The security function shall limit the use of resources by priority.
FAV.9	The functions provided by the security function to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding [assignment: quantification] for loss of security function data or objects under the control of the module's security function.
FAV.10	The security function shall ensure the availability of [assignment: list of types of security function data] provided to another trusted IT product within [assignment: a defined availability metric] given the following conditions [assignment: conditions to ensure availability].

898

899 **3.1.4. Identification (FID)**

900 This section covers requirements around who an actor claims to be.

901

FID.1	The security function shall require each user to be successfully identified before allowing any other system's security function-mediated actions on behalf of that user unless is one of the following: [list of system's security function-mediated actions] that may be allowed before the user is identified.
FID.2	The security function shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: list of user security attributes].
FID.3	The security function shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: rules for the initial association of attributes].
FID.4	The security function shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: rules for the changing of attributes].
FID.5	The security function shall uniquely identify (and authenticate) [assignment: users, processes acting on behalf of users, devices, etc.] before establishing a connection.
FID.6	The organization shall manage user identifiers by: <ol style="list-style-type: none"> 1. Uniquely identifying each user; 2. Verifying the identity of each user; 3. Receiving authorization to issue a user identifier from an appropriate organization official; 4. Issuing the user identifier to the intended party; 5. Disabling the user identifier after [Assignment: organization-defined time period] of inactivity; and 6. Archiving user identifiers.
FID.7	The security function shall have mechanisms to uniquely identify (and authenticate) [assignment: users, processes acting on behalf of users, etc.].
FID.8	The security function shall appropriately label information in storage, in process and in transmission.

902

903 **3.1.5. Authentication (FAT)**

904 This section covers requirements around the proof of identity of an actor.

905

FAT.1	After a predetermined period of inactivity, the system shall prevent further access to the system by
--------------	--

	initiating a session lock that remains in effect until the user reestablishes access using appropriate (identification and) authentication procedures.
FAT.2	The security function shall employ a mechanism to authenticate specific devices before establishing a connection.
FAT.3	The security function shall employ authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.
FAT.4	The security function shall have mechanisms to authenticate users (or processes acting on behalf of users).
FAT.5	The security function enforces assigned authorizations for controlling access to the system in accordance with applicable policy.
FAT.6	The security function shall employ authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.
FAT.7	The security function shall enforce assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.
FAT.8	The security function shall enforce the most restrictive set of rights and privileges or accesses needed by [assignment: users, processes acting on behalf of users, etc.] for the performance of specified tasks.
FAT.9	The security function shall (identify and) authenticate specific devices before establishing a connection.
FAT.10	The security function shall obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and unauthorized use.
FAT.11	The security function shall uniquely authenticate [assignment: users, processes acting on behalf of users, etc.].
FAT.12	The organization shall authorize all methods of remote access to the system.
FAT.13	The organization shall develop and enforce policies and procedures for system users concerning the generation and use of passwords. These policies stipulate rules of complexity, based on the criticality level of the systems to be accessed.
FAT.14	The organization shall develop, disseminate and periodically review and update: <ol style="list-style-type: none"> 1. A formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.
FAT.15	The organization shall develop, disseminate and periodically review and update: <ol style="list-style-type: none"> 1. A formal, documented, authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated authentication controls.
FAT.16	The organization shall employ mechanisms in the design and implementation of a system to restrict public access to the system from the organization's enterprise network.
FAT.17	The organization shall establish terms and conditions for authorized individuals to: <ol style="list-style-type: none"> 1. Access the information system from an external information system; and 2. Process, store, and/or transmit organization-controlled information using an external information system.
FAT.18	The organization shall identify and document specific user actions (authorizations) that can be performed on the information system without identification or authentication.

FAT.19	The organization shall manage information system authenticators by: <ol style="list-style-type: none"> 1. Defining initial authenticator content; 2. Establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; 3. Changing default authenticators upon information system installation; and 4. Changing/refreshing authenticators periodically
FAT.20	The organization shall supervise and review the activities of users with respect to the enforcement and usage of system access controls.
FAT.21	The organization shall: <ol style="list-style-type: none"> 1. Establish usage restrictions and implementation guidance for [assignment: devices (e.g., wireless technologies, portable and mobile devices and media)]; and, 2. Authorize, monitor and control access to the system. 3. Document, monitor, log, and limit access of these devices to the organization's system. 4. Appropriate organizational officials shall authorize the use of these devices per organization's established security policy and procedures.
FAT.22	The security function authenticates specific devices before establishing a connection.
FAT.23	The security function shall [selection: detect, prevent] use of authentication data that has been copied or forged by any actor of the system.
FAT.24	The security function shall allow [assignment: list of security function mediated actions] on behalf of the user to be performed before the user is authenticated.
FAT.25	The security function shall allow the [assignment: the authorized identified roles] to specify alternative initial values to override the default values when an object or information is created.
FAT.26	The security function shall authenticate any user's claimed identity according to the [assignment: rules describing how the multiple authentication mechanisms provide authentication].
FAT.27	The security function shall be able to associate [assignment: users] with roles.
FAT.28	The security function shall be able to enforce the use of security function generated secrets for [assignment: list of functions].
FAT.29	The security function shall enforce the [assignment: access control security function policy] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the security function's policy.
FAT.30	The security function shall enforce the [assignment: access control security function policy] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated security function policy, and for each, the security function policy-relevant security attributes, or named groups of security function policy-relevant security attributes].
FAT.31	The security function shall enforce the [assignment: access control security function policy(s), information flow control security function policy(s)] to restrict the ability to [selection: change, default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorized identified roles].
FAT.32	The security function shall enforce the [assignment: access control security function policy, information flow control security function policy] to provide [selection, choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the security function policy.
FAT.33	The security function shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].
FAT.34	The security function shall enforce the rules [assignment: specification of revocation rules].
FAT.35	The security function shall ensure that all operations between any subject controlled by the security function and any object controlled by the security function are covered by an access control security function policy.

FAT.36	The security function shall ensure that the conditions [assignment: conditions for the different roles] are satisfied.
FAT.37	The security function shall explicitly [selection: authorize, deny] an information flow based on the following rules: [assignment: rules, based on security attributes that explicitly [selection: authorize, deny] information flows].
FAT.38	The security function shall explicitly deny access of subjects to objects based on the [assignment: rules, based on security attributes that explicitly deny access of subjects to objects].
FAT.39	The security function shall maintain the following list of security attributes belonging to individual users: [assignment: list of security attributes].
FAT.40	The security function shall maintain the roles: [assignment: authorized identified roles].
FAT.41	The security function shall prevent reuse of authentication data related to [assignment: identified authentication mechanism(s)].
FAT.42	The security function shall provide [assignment: list of multiple authentication mechanisms] to support user authentication.
FAT.43	The security function shall provide a mechanism to <i>generate</i> secrets that meet [assignment: a defined quality metric].
FAT.44	The security function shall provide a mechanism to <i>verify</i> that secrets meet [assignment: a defined quality metric].
FAT.45	The security function shall provide only [assignment: list of feedback] to the user while the authentication is in progress.
FAT.46	The security function shall re-authenticate the user under the conditions [assignment: list of conditions under which re-authentication is required].
FAT.47	The security function shall require an explicit request to assume the following roles: [assignment: the roles].
FAT.48	The security function shall require each user to be successfully authenticated before allowing any other system's security function-mediated actions on behalf of that user.
FAT.49	The security function shall restrict the ability to [selection: change, default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of security function data] to [assignment: the authorized identified roles].
FAT.50	The security function shall restrict the ability to [selection: determine the behavior of, disable, enable, modify the behavior of] the functions [assignment: list of functions] to [assignment: the authorized identified roles].
FAT.51	The security function shall restrict the ability to revoke [assignment: list of security attributes] associated with the [selection: users, subjects, objects, [assignment: other additional resources]] under the control of the security function to [assignment: the authorized identified roles].
FAT.52	The security function shall restrict the capability to specify an expiration time for [assignment: list of security attributes for which expiration is to be supported] to [assignment: the authorized identified roles].
FAT.53	The security function shall restrict the specification of the limits for [assignment: list of security function data] to [assignment: the authorized identified roles].
FAT.54	The security function shall use the following rules to set the value of security attributes: [assignment: rules for setting the values of security attributes]
FAT.55	Based on the criticality level of the systems to be accessed, the organization shall develop and enforce policies and procedures for system users concerning the generation, use and rules of complexity for passwords.
FAT.56	The security function shall prevent further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity, and the session lock remains in effect

	until the user reestablishes access using appropriate identification and authentication procedures.
FAT.57	When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed], the security function shall [assignment: list of actions].

906

907 3.1.6. Authorization (FAZ)

908 Authorization is the approval of an actor to perform an action.

909

FAZ.1	The security function shall enforce assigned authorizations for controlling access to the system in accordance with applicable policy.
FAZ.2	The security function shall enforce separation of duties through assigned access authorizations.
FAZ.3	The security function shall enforce assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.
FAZ.4	The organization shall document authorization and approval policies and procedures and maintains a list of personnel authorized to perform maintenance on the control system. Only authorized and qualified organization or vendor personnel perform maintenance on the system.
FAZ.5	The organization shall develop and keep current a list of personnel with authorized access to the facility where [assignment: type of system (e.g., control system, information system)] resides (except for those areas within the facility officially designated as publicly accessible) and issues appropriate authorization credentials (e.g., badges, identification cards, smart cards). Designated officials within the organization review and approve the access list and authorization credentials [Assignment: organization-defined frequency, at least annually].
FAZ.6	The organization shall control all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. The organization shall control access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.
FAZ.7	The organization shall review information system and facility access authorizations when personnel are reassigned or transferred to other positions within the organization and initiates appropriate actions
FAZ.8	The organization shall limits physical access to all control system facilities and assets and verifies individual access authorizations before granting access. The organization shall limit access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.
FAZ.9	The organization shall authorize (i.e., accredit) the system for processing before operations and periodically update the authorization [assignment: organization-defined frequency] or when there is a significant change to the system. A senior organizational official shall sign and approve the security accreditation.
FAZ.10	The security function shall enforce the most restrictive set of rights, privileges or accesses needed by users or workstations (or processes acting on behalf of users) for the performance of specified tasks.
FAZ.11	The security function shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes that explicitly authorize access of subjects to objects].
FAZ.12	The security function shall enforce a limit of [assignment: organization-defined number] consecutive invalid access attempts by a user during a [assignment: organization-defined time period] time period. The security function shall automatically [Selection: locks the account/node for an [assignment: organization-defined time period], delays next login prompt according to [assignment: organization-defined delay algorithm.]] when the maximum number of unsuccessful attempts is exceeded.

FAZ.13	The security function automatically terminates a remote session after [assignment: defined period of inactivity] for [assignment: workstations, servers, etc.] that are used for [assignment: system monitoring, maintenance activities, etc.] based on the risk assessment of the system and the organization's security policy.
FAZ.14	The security function shall limit the number of concurrent sessions for any user to [assignment: organization-defined number of sessions] on the system.

910

911 **3.1.7. Non-Repudiation (FNR)**

912 Non-repudiation is the ability to irrefutably, tie an actor to an action.

913

FNR.1	The security function shall be able to generate evidence of origin for transmitted [assignment: list of information types] at the request of the [selection: originator, recipient, [assignment: list of third parties]].
FNR.2	The security function shall be able to relate the [assignment: list of attributes] of the originator of the information, and the [assignment: list of information fields] of the information to which the evidence applies.
FNR.3	The security function shall provide a capability to verify the evidence of origin of information to [selection: originator, recipient, [assignment: list of third parties]] given [assignment: limitations on the evidence of origin].
FNR.4	The security function shall enforce the generation of evidence of origin for transmitted [assignment: list of information types] at all times.
FNR.5	The security function shall be able to generate evidence of receipt for received [assignment: list of information types] at the request of the [selection: originator, recipient, [assignment: list of third parties]].
FNR.6	The security function shall be able to relate the [assignment: list of attributes] of the recipient of the information, and the [assignment: list of information fields] of the information to which the evidence applies.
FNR.7	The security function shall provide a capability to verify the evidence of receipt of information to [selection: originator, recipient, [assignment: list of third parties]] given [assignment: limitations on the evidence of receipt].
FNR.8	The security function shall enforce the generation of evidence of receipt for received [assignment: list of information types] at all times.
FNR.9	The security function shall provide mechanisms to protect the authenticity of communications sessions.
FNR.10	The security function shall provide a capability to generate evidence that can be used as a guarantee of the validity of [assignment: list of objects or information types].
FNR.11	The security function shall provide the capability to determine whether a [assignment: given individual, system, etc.] took a particular [assignment: action].

914

915 **3.1.8. Accounting (FAC)**

916 This section covers the recording of activity by actors/elements throughout the system.

917 Accounting requirements provide the means to perform a successful audit of events that occur on
918 the system.

919

FAC.1	The security function shall take [assignment: list of actions] upon detection of a potential security
--------------	---

	violation.
FAC.2	The security function shall be able to generate an accounting record of the following auditable events: <ol style="list-style-type: none"> 1. Start-up and shutdown of the audit functions; 2. All auditable events for the [selection, choose one of: minimum, basic, detailed, not specified] level of audit; and 3. [assignment: other specifically defined auditable events]
FAC.3	The security function shall generate audit records, at a minimum, for the following events whether or not the attempts were successful: <ol style="list-style-type: none"> 1. Attempts to logon; 2. Attempts to change local account attributes such as privileges; 3. Attempts to change local security policy
FAC.4	The security function shall provide [assignment: authorized users] with the capability to read [assignment: list of audit information] from the audit records.
FAC.5	The security function shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.
FAC.6	The security function shall ensure that [assignment: metric for saving audit records] stored audit records will be maintained when the following conditions occur: [selection: audit storage exhaustion, failure, attack]
FAC.7	The security function shall generate audit records for the following events: [Assignment: organization-defined auditable events].
FAC.8	The security function shall record within each accounting record at least the following information: <ol style="list-style-type: none"> 1. Date and time of the event, type of event, subject identity and/or source of the event, and the outcome (e.g., success or failure) of the event; and 2. For each audit event type [assignment: other audit relevant information].
FAC.9	For audit events resulting from actions of identified users, the security function shall be able to associate each auditable event with the identity of the user that caused the event.
FAC.10	The security function shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the security function requirements.
FAC.11	The security function shall enforce the following rules for monitoring audited events: <ol style="list-style-type: none"> 1. Accumulation or combination of [assignment: subset of defined auditable events] known to indicate a potential security violation; 2. [assignment: any other rules]
FAC.12	The security function shall be able to maintain profiles of system usage, where an individual profile represents the historical patterns of usage performed by the member(s) of [assignment: the profile target group].
FAC.13	The security function shall be able to maintain a suspicion rating associated with each user whose activity is recorded in a profile, where the suspicion rating represents the degree to which the user's current activity is found inconsistent with the established patterns of usage represented in the profile.
FAC.14	The security function shall be able to indicate a possible violation of the enforcement of the security function requirements when a user's suspicion rating exceeds the following threshold conditions [assignment: conditions under which anomalous activity is reported by the module's security function].
FAC.15	The security function shall be able to maintain an internal representation of the following signature events [assignment: a subset of system events] that may indicate a violation of the enforcement of the security function requirements.
FAC.16	The security function shall be able to compare the signature events against the record of system activity discernible from an examination of [assignment: the information used to determine system activity].

FAC.17	The security function shall be able to indicate a potential violation of the enforcement of the security function requirements when a system event is found to match a signature event or event sequence that indicates a potential violation of the enforcement of the security function requirements.
FAC.18	The security function shall be able to maintain an internal representation of the following event sequences of known intrusion scenarios [assignment: list of sequences of system events whose occurrence are representative of known penetration scenarios] and the following signature events [assignment: a subset of system events] that may indicate a potential violation of the enforcement of the security function requirements.
FAC.19	The security function shall be able to compare the signature events and event sequences against the record of system activity discernible from an examination of [assignment: the information to be used to determine system activity].
FAC.20	The security function shall provide the audit records in a manner suitable for the user to interpret the information.
FAC.21	The security function shall provide the ability to apply [assignment: methods of selection and/or ordering] of audit data based on [assignment: criteria with logical relations].
FAC.22	The security function shall be able to select the set of audited events from the set of all auditable events based on the following attributes: <ol style="list-style-type: none"> 1. [selection: object identity, user identity, subject identity, host identity, event type] 2. [assignment: list of additional attributes that audit selectivity is based upon]
FAC.23	The security function shall be able to [selection, choose one of: prevent, detect] unauthorized modifications to the stored audit records in the audit trail.
FAC.24	The security function shall protect audit information and audit tools from unauthorized access, modification, and deletion.
FAC.25	The security function shall [assignment: actions to be taken in case of possible audit storage failure] if the audit trail exceeds [assignment: pre-defined limit].
FAC.26	The security function shall [selection, choose one of: "ignore audited events", "prevent audited events, except those taken by the authorized user with special rights", "overwrite the oldest stored audit records"] and [assignment: other actions to be taken in case of audit storage failure] if the audit trail is full.
FAC.27	The organization shall allocate sufficient audit record storage capacity and configures auditing to reduce the likelihood of exceeding storage capacity.
FAC.28	The security function shall alert appropriate organizational officials in the event of an audit processing failure and takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].
FAC.29	The security function shall provide an audit reduction and report generation capability.
FAC.30	The security function shall provide time stamps for use in audit record generation.
FAC.31	The security function/system shall notify the user, upon successful logon, of the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.
FAC.32	The security function shall display an approved, system use notification message before granting system access informing potential users: <ol style="list-style-type: none"> 1. That the user is accessing a [assignment: name of organization's information system]; 2. That system usage may be monitored, recorded, and subject to audit; 3. That unauthorized use of the system is prohibited and subject to criminal and civil penalties; and 4. That use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

921 **3.2. Supporting Security Services**

922 Supporting Security Services requirements are how security is realized for primary security
923 requirements. Each requirement in this section maps to requirements in Section 3.1. The
924 mapping should indicate which requirements from Section 3.1 are satisfied (in whole or in part)
925 given satisfaction of the identified 3.2 requirement. The litmus test for inclusion in this section is
926 simple. If any requirement in this section cannot be mapped to at least two requirements across
927 confidentiality, integrity and availability (CIA), then it should appear in Section 3.1.
928 Policy requirements can appear in this section, so long as they are relevant to a specific
929 supporting security service area.

930 **3.2.1. Anomaly Detection Services (FAS)**

931 Detection services detect events outside of the bounds of normally anticipated or desired
932 behavior such as attacks, intrusions, or errors.
933

FAS.1	Upon detection of a data integrity error, the security function shall take the following actions: [assignment: specify the action to be taken].
FAS.2	The security function shall provide unambiguous detection of physical tampering that might compromise the module's security function.
FAS.3	For [assignment: list of security function devices/elements for which active detection is required], the security function shall monitor the devices and elements and notify [assignment: a designated user or role] when physical tampering with the module's security function's devices or module's security function's elements has occurred.
FAS.4	The security function shall take [assignment: list of actions] upon detection of a potential security violation.
FAS.5	The organization shall employ and maintain fire suppression and detection devices/systems that can be activated in the event of a fire.
FAS.6	The organization shall implement and maintain fire suppression and detection devices/systems that can be activated in the event of a fire.
FAS.7	The organization shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
FAS.8	The organization shall implement control system incident handling capabilities for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

934

935 **3.2.2. Boundary Services (FBS)**

936 This section provides requirements around boundary services. Boundary services provide
937 isolation between system elements or between the system and external entities. Boundary
938 services explain what occurs at the transition between two separate security domains such as
939 examination or changing constraints on the border relationship.
940 Boundary requirements are oriented towards maintaining the strength and integrity of the
941 boundary (isolation) between inside and outside of the system boundary. The requirements for a
942 firewall configuration are one set of examples.
943

FBS.1	The security function shall restrict the scope of the session security attributes [assignment: session security attributes], based on [assignment: attributes].
--------------	--

FBS.2	The security function shall restrict the maximum number of concurrent sessions that belong to the same user.
FBS.3	The security function shall enforce, by default, a limit of [assignment: default number] sessions per user.
FBS.4	The security function shall restrict the maximum number of concurrent sessions that belong to the same user according to the rules [assignment: rules for the number of maximum concurrent sessions].
FBS.5	The security function shall lock an interactive session after [assignment: time interval of user inactivity] by: a) clearing or overwriting display devices, making the current contents unreadable; b) disabling any activity of the user's data access/display devices other than unlocking the session.
FBS.6	The security function shall require the following events to occur prior to unlocking the session: [assignment: events to occur].
FBS.7	The security function shall allow user-initiated locking of the user's own interactive session, by: a) clearing or overwriting display devices, making the current contents unreadable; b) disabling any activity of the user's data access/display devices other than unlocking the session.
FBS.8	The security function shall terminate an interactive session after a [assignment: time interval of user inactivity].
FBS.9	The security function shall allow user-initiated termination of the user's own interactive session.
FBS.10	Before establishing a user session, the security function shall display an advisory warning message regarding unauthorized use of the module.
FBS.11	Upon successful session establishment, the security function shall display the [selection: date, time, method, location] of the last successful session establishment to the user.
FBS.12	Upon successful session establishment, the security function shall display the [selection: date, time, method, location] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.
FBS.13	The security function shall not erase the access history information from the user interface without giving the user an opportunity to review the information.
FBS.14	The security function shall be able to deny session establishment based on [assignment: attributes].
FBS.15	The security function shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FBS.16	The security function shall permit [selection: the module's security function, another trusted IT product] to initiate communication via the trusted channel.
FBS.17	The security function shall initiate communication via the trusted channel for [assignment: list of functions for which a trusted channel is required].
FBS.18	The security function shall provide a communication path between itself and [selection: remote, local] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [selection: modification, disclosure, [assignment: other types of integrity or confidentiality violation]].
FBS.19	The security function shall permit [selection: the module's security function, local users, remote users] to initiate communication via the trusted path.
FBS.20	The security function shall require the use of the trusted path for [selection: initial user authentication, [assignment: other services for which trusted path is required]].

FBS.21	The organization shall develop, implement, and periodically review and update: <ol style="list-style-type: none"> 1. A formal, documented, control system security policy that addresses: <ol style="list-style-type: none"> a. The purpose of the security program as it relates to protecting the organization's personnel and assets; b. The scope of the security program as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities, and management accountability structure of the security program to ensure compliance with the organization's security policy and other regulatory commitments. 2. Formal, documented procedures to implement the security policy and associated requirements. A control system security policy considers controls from each of the families contained in this document.
FBS.22	The organization shall establish policies and procedures to define roles, responsibilities, behaviors, and practices for the implementation of an overall security program.
FBS.23	The organization shall define a framework of management leadership accountability. This framework establishes roles and responsibilities to approve cyber security policy, assign security roles, and coordinate the implementation of cyber security across the organization.
FBS.24	Baseline practices that organizations employ for organizational security include, but are not limited to: <ol style="list-style-type: none"> 1. Executive management accountability for the security program; 2. Responsibility for control system security within the organization includes sufficient authority and an appropriate level of funding to implement the organization's security policy; 3. The organization's security policies and procedures that provide clear direction, accountability, and oversight for the organization's security team. The security team assigns roles and responsibilities in accordance with the organization's policies and confirms that processes are in place to protect company assets and critical information; 4. The organization's contracts with external entities that address the organization's security policies and procedures with business partners, third-party contractors, and outsourcing partners; 5. The organization's security policies and procedures ensure coordination or integration with the organization's physical security plan. Organization roles and responsibilities are established that address the overlap and synergy between physical and control system security risks.
FBS.25	The organization's security policies and procedures shall delineate how the organization implements its emergency response plan and coordinates efforts with law enforcement agencies, regulators, Internet service providers and other relevant organizations in the event of a security incident.
FBS.26	The organization shall hold external suppliers and contractors that have an impact on the security of the control center to the same security policies and procedures as the organization's own personnel; and shall ensure security policies and procedures of second- and third-tier suppliers comply with corporate cyber security policies and procedures if they will impact control system security.
FBS.27	The organization shall establish procedures to remove external supplier access at the conclusion/termination of the contract.
FBS.28	The security function shall monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.

944

945 **3.2.3. Cryptographic Services (FCS)**

946 Cryptographic services include encryption, signing, key management and key revocation.
947 The security function may employ cryptographic functionality to help satisfy several high-level
948 security objectives. These include, but are not limited to identification and authentication, non-
949 repudiation, trusted path, trusted channel and data separation. This class is used when the security
950 component implements cryptographic functions, the implementation of which could be in hardware,
951 firmware and/or software.

952 The FCS: Cryptographic support class is composed of two families: Cryptographic key
 953 management (FCS_CKM) and Cryptographic operation (FCS_COP). The Cryptographic key
 954 management (FCS_CKM) family addresses the management aspects of cryptographic keys,
 955 while the Cryptographic operation (FCS_COP) family is concerned with the operational use of
 956 those cryptographic keys. [DHS]
 957

FCS.1	The security function shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].
FCS.2	The security function shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: cryptographic key distribution method] that meets the following: [assignment: list of standards].
FCS.3	The security function shall perform [assignment: type of cryptographic key access] in accordance with a specified cryptographic key access method [assignment: cryptographic key access method] that meets the following: [assignment: list of standards].
FCS.4	The security function shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: cryptographic key destruction method] that meets the following: [assignment: list of standards].
FCS.5	The security function shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].
FCS.6	For information requiring cryptographic protection, the information system shall implement cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

958

959 3.2.4. Notification and Signaling Services (FNS)

960 Notification and signaling services are oriented towards providing system activity information
 961 and command result logging.

962

FNS.1	For [assignment: list of security function devices/elements for which active detection is required], the security function shall monitor the devices and elements and notify [assignment: a designated user or role] when physical or logical tampering with the module's security function's devices or module's security function's elements has occurred.
FNS.2	The security function verifies the correct operation of security utility [Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): notifies system administrator, shuts the system down, restarts the system] when anomalies are discovered.
FNS.3	The organization shall verify the correct operation of security functions within the control system upon system startup and restart; upon command by user with appropriate privilege; periodically; and/or at defined time periods. The security function notifies the system administrator when anomalies are discovered.
FNS.4	The security function shall notify the user, upon successful logon, of the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.
FNS.5	The security function shall display an approved, system use notification message before granting system access informing potential users: <ol style="list-style-type: none"> 1. That the user is accessing a [assignment: organization] information system; 2. That system usage may be monitored, recorded, and subject to audit; 3. That unauthorized use of the system is prohibited and subject to criminal and civil penalties;

	<p>and</p> <p>4. That use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.</p>
FNS.6	The security function shall perform [assignment: list of specific actions] when replay is detected.

963

964 **3.2.5. Resource Management Services (FRS)**

965 This section covers resource management services requirements. Resource Management
 966 Services include management of runtime resources, such as network/communication paths,
 967 processors, memory or disk space (e.g., for audit log capacity), and other limited system
 968 resources.
 969

FRS.1	<p>The organization shall develop, disseminate, and periodically review and update:</p> <ol style="list-style-type: none"> 1. A formal, documented system and communication protection policy that addresses: <ol style="list-style-type: none"> a. The purpose of the system and communication protection policy as it relates to protecting the organization's personnel and assets; b. The scope of the system and communication protection policy as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities and management accountability structure of the security program to ensure compliance with the organization's system and communications protection policy and other regulatory commitments; 2. Formal, documented procedures to facilitate the implementation of the control system and communication protection policy and associated systems and communication protection controls
FRS.2	The security function shall separate telemetry/data acquisition services from management port functionality.
FRS.3	The security function shall isolate security functions from non-security functions.
FRS.4	The security function shall prevent unauthorized or unintended information transfer via shared system resources.
FRS.5	The security function shall protect against or limits the effects of denial-of-service attacks based on an organization's defined list of types of denial-of-service attacks.
FRS.6	The security function shall limit the use of resources by priority.
FRS.7	The organization shall define the external boundary(ies) of the control system. Procedural and policy security functions define the operational system boundary, the strength required of the boundary, and the respective barriers to unauthorized access and control of system assets and components. The control system monitors and manages communications at the operational system boundary and at key internal boundaries within the system.
FRS.10	The security function shall establish a trusted communications path between the user and the system.
FRS.11	When cryptography is required and employed within the system, the organization shall establish and manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures.
FRS.12	The organization shall develop and implement a policy governing the use of cryptographic mechanisms for the protection of control system information. The organization shall ensure all cryptographic mechanisms comply with applicable laws, regulatory requirements, directives, policies, standards, and guidance.
FRS.13	The use of collaborative computing mechanisms on control system is strongly discouraged and provides an explicit indication of use to the local users.

FRS.14	The system shall reliably associate security parameters (e.g., security labels and markings) with information exchanged between the enterprise information systems and the system.
FRS.15	The organization shall issue public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.
FRS.16	The organization shall: <ol style="list-style-type: none"> 1. Establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the control system if used maliciously; 2. Document, monitor, and manage the use of mobile code within the control system. Appropriate organizational officials should authorize the use of mobile code.
FRS.17	The organization shall: <ol style="list-style-type: none"> 1. Establish usage restrictions and implementation guidance for Voice over Internet Protocol (VOIP) technologies based on the potential to cause damage to the information system if used maliciously; and 2. Authorize, monitor, and limit the use of VOIP within the control system.
FRS.18	All external system and communication connections shall be identified and adequately protected from tampering or damage.
FRS.19	The system design and implementation shall specify the security roles and responsibilities for the users of the system.
FRS.20	The system shall provide mechanisms to protect the authenticity of device-to-device communications.
FRS.21	The system's devices that collectively provide name/address resolution services for an organization shall be fault tolerant and implement address space separation.
FRS.22	The system resource (i.e., authoritative DNS server) that provides name/address resolution service shall provide additional artifacts (e.g., digital signatures and cryptographic keys) along with the authoritative DNS resource records it returns in response to resolution queries.
FRS.23	The system resource (i.e., resolving or caching name server) that provides name/address resolution service for local clients shall perform data origin authentication and data integrity verification on the resolution responses it receives from authoritative DNS servers when requested by client systems.
FRS.24	The security function shall restrict the ability to [selection: determine the behavior of, disable, enable, modify the behavior of] the functions [assignment: list of functions] to [assignment: the authorized identified roles].
FRS.25	The security function shall enforce the [assignment: access control security function policy(s), information flow control security function policy(s)] to restrict the ability to [selection: change, default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorized identified roles].
FRS.26	The security function shall ensure that only secure values are accepted for [assignment: list of security attributes].
FRS.27	The security function shall enforce the [assignment: access control security function policy, information flow control security function policy] to provide [selection, choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the security function policy.
FRS.28	The security function shall allow the [assignment: the authorized identified roles] to specify alternative initial values to override the default values when an object or information is created.
FRS.29	The security function shall use the following rules to set the value of security attributes: [assignment: rules for setting the values of security attributes]
FRS.30	The security function shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of security function data] to [assignment: the authorized identified roles].
FRS.31	The security function shall restrict the specification of the limits for [assignment: list of security function data] to [assignment: the authorized identified roles].

FRS.32	The security function shall take the following actions, if the security function data are at, or exceed, the indicated limits: [assignment: actions to be taken].
FRS.33	The security function shall ensure that only secure values are accepted for [assignment: list of security function data].
FRS.34	The security function shall restrict the ability to revoke [assignment: list of security attributes] associated with the [selection: users, subjects, objects, [assignment: other additional resources]] under the control of the security function to [assignment: the authorized identified roles].
FRS.35	The security function shall enforce the rules [assignment: specification of revocation rules].
FRS.36	The security function shall restrict the capability to specify an expiration time for [assignment: list of security attributes for which expiration is to be supported] to [assignment: the authorized identified roles].
FRS.37	For each of these security attributes, the security function shall be able to [assignment: list of actions to be taken for each security attribute] after the expiration time for the indicated security attribute has passed.
FRS.38	The security function shall be capable of performing the following management functions: [assignment: list of management functions to be provided by the module's security function].
FRS.39	The security function shall maintain the roles [assignment: the authorized identified roles].
FRS.40	The security function shall be able to associate users with roles.
FRS.41	The security function shall maintain the roles: [assignment: authorized identified roles].
FRS.42	The security function shall ensure that the conditions [assignment: conditions for the different roles] are satisfied.
FRS.43	The security function shall require an explicit request to assume the following roles: [assignment: the roles].
FRS.44	The security function shall terminate the network session at the end of a session or after [Assignment: organization-defined time period] of inactivity.

970

971 **3.2.6. Trust and Certificate Services (FTS)**

972 Description of relationships between entities and the faith placed on the relationship certificates
 973 that have uses outside of cryptography for example, material relating to creation, storage, and
 974 revocation of certificates.
 975

FTS.1	The security function shall issue public key certificates based on an appropriate certificate policy or obtain public key certificates under an appropriate certificate policy from an [assignment: approved service provider].
FTS.2	When cryptography is required and employed within the security function, the organization shall establish and manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures.

976

977 **3.3. Assurance**

978 **3.3.1. Development Rigor (ADR)**

979 Not all solutions are created equal. Differing degrees of care and consideration can go into
 980 developing solutions that satisfy any given security requirement. This section contains

981 requirements regarding the activities involved in developing smart grid system solutions. Topics
 982 including:

- 983 • acquisition issues
- 984 • configuration management
- 985 • development practices

986 This is about the creation of smart grid systems, not their deployment, operation, or maintenance.
 987

ADR.1	The organization shall develop, disseminate, and periodically review/update: <ol style="list-style-type: none"> 1. A formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.
ADR.2	The organization shall schedule, perform, document and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.
ADR.3	The organization shall approve, control and monitor the use of information system maintenance tools and maintains the tools on an ongoing basis.
ADR.4	The organization shall authorize, monitor and control any remotely executed maintenance and diagnostic activities, if employed.
ADR.5	The organization shall allow only authorized personnel to perform maintenance on the information system.
ADR.6	The organization shall obtain maintenance support and spare parts for [Assignment: organization-defined list of key information system components] within [Assignment: organization-defined time period] of failure.
ADR.7	The organization shall develop, disseminate, and periodically review/update: <ol style="list-style-type: none"> 1. A formal, documented, system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.
ADR.8	The organization shall determine, document and allocate as part of its capital planning and investment control process, the resources required to adequately protect the information system.
ADR.9	The organization shall manage the information system using a system development life cycle methodology that includes information security considerations.
ADR.10	The organization shall include security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.
ADR.11	The organization shall obtain, protect as required, and make available to authorized personnel, adequate documentation for the information system.
ADR.12	The organization shall comply with software usage restrictions.
ADR.13	The organization shall enforce explicit rules governing the installation of software by users.
ADR.14	The organization shall design and implement the information system using security engineering principles.
ADR.15	The organization shall: <ol style="list-style-type: none"> 1. Requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies,

	<p>regulations, standards, guidance, and established service-level agreements; and</p> <p>2. Monitors security control compliance</p>
ADR.16	The organization shall require that information system developers create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.
ADR.17	The organization shall require that information system developers create a security test and evaluation plan, implement the plan, and document the results.
ADR.18	<p>The organization shall develop, disseminate and periodically review/update:</p> <ol style="list-style-type: none"> 1. A formal, documented, system and services acquisition policy that addresses: <ol style="list-style-type: none"> a. The purpose of the security program as it relates to protecting the organization's personnel and assets; b. The scope of the security program as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities and management accountability structure of the security program to ensure compliance with the organization's security policy and other regulatory commitments. 2. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.
ADR.19	The organization shall implement a process to determine, document, approve, and allocate the resources required to adequately protect the control system as part of its capital planning and investment control process.
ADR.20	The organization shall manage the control system using a system development life-cycle methodology that includes control system security considerations.
ADR.21	The organization shall include security requirements and/or security specifications, either explicitly or by reference, in control system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.
ADR.22	The organization shall ensure that adequate documentation for the control system and its constituent components are available, protected when required, and are accessible to authorized personnel.
ADR.23	The organization's security program shall deploy policy and procedures to enforce compliance with software license usage restrictions.
ADR.24	The organization shall implement policies and procedures to enforce explicit rules and management expectations governing user installation of software.
ADR.25	The organization shall design and implement the control system using security engineering principles and best practices.
ADR.26	The organization shall ensure that third-party providers of control system services employ adequate security mechanisms in accordance with established service-level agreements and monitor compliance.
ADR.27	<p>The control system vendor shall create and implement a configuration management plan and procedures that limit changes to the control system during design and installation. This plan tracks security flaws. The vendor shall obtain the organization's written approval for any changes to the plan.</p> <p>The vendor shall provide documentation of the plan and its implementation.</p>
ADR.28	The control system vendor shall develop a security test and evaluation plan. The vendor shall submit the plan to the organization for approval and implements the plan once written approval is obtained. The vendor shall then documents the results of the testing and evaluation and submits them to the organization for approval.
ADR.29	The control system vendor shall adopt appropriate software development life-cycle practices to eliminate common coding errors that affect security, particularly with respect to input data validation and buffer management.
ADR.30	The organization shall develop, disseminate, and periodically review and update:

	<ol style="list-style-type: none"> 1. A formal, documented Configuration Management policy that addresses: <ol style="list-style-type: none"> a. The purpose of the configuration management policy as it relates to protecting the organization's personnel and assets; b. The scope of the configuration management policy as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities and management accountability structure contained in the configuration management policy to ensure compliance with the organization's security policy and other regulatory commitments 2. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. 3. The personnel qualification levels required to make changes, the conditions under which changes are allowed, and what approvals are required for those changes.
ADR.31	The organization shall develop, document, and maintain a current baseline configuration of the control system and an inventory of the system's constituent components.
ADR.32	The organization shall authorize, document and manage changes to the control system.
ADR.33	The organization shall implement a process to monitor changes to the control system and conducts security impact analyses to determine the effects of the changes.
ADR.34	The organization shall: <ol style="list-style-type: none"> 1. Approves individual access privileges and enforces physical and logical access restrictions associated with configuration changes to the control system; 2. Generates, retains, and reviews records reflecting all such changes.
ADR.35	The organization shall: <ol style="list-style-type: none"> 1. Establishes mandatory configuration settings for IT products employed within the control system; 2. Configures the security settings of control systems technology products to the most restrictive mode consistent with control system operational requirements; 3. Documents the changed configuration settings.
ADR.36	The organization shall configure the control system to provide only essential capabilities and specifically prohibit and/or restrict the use of functions, ports, protocols, and/or services as defined in an organizationally generated "prohibited and/or restricted" list.
ADR.37	The organization shall create and maintains a list of all end-user configurable assets and the configurations of those assets used by the organization.
ADR.38	The organization shall implement policy and procedures to address the addition, removal, and disposal of all control system equipment. All control system assets and information shall be documented, identified and tracked so that their location and function are known.
ADR.39	The organization shall change all factory default authentication credentials on control system components and applications upon installation.
ADR.40	The organization shall develop, disseminate, and periodically review/update: <ol style="list-style-type: none"> 1. A formal, documented, control system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 2. Formal, documented procedures to facilitate the implementation of the control system maintenance policy and associated system maintenance controls.
ADR.41	The organization shall develop policies and procedures to upgrade existing legacy control systems to include security mitigating measures commensurate with the organization's risk tolerance and the risk to the system and processes controlled.
ADR.42	The organization shall conduct periodic security vulnerability assessments according to the risk management plan. Then, the control system shall be updated to address any identified vulnerabilities in accordance with organization's control system maintenance policy.
ADR.43	The organization shall make and secure backups of critical system software, applications and data

	for use if the control system operating system software becomes corrupted or destroyed.
ADR.44	The organization shall review and follow security requirements for a control system before undertaking any unplanned maintenance activities of control system components (including field devices). Documentation includes the following: <ol style="list-style-type: none"> 1. The date and time of maintenance; 2. The name of the individual(s) performing the maintenance; 3. The name of the escort, if necessary; 4. A description of the maintenance performed; 5. A list of equipment removed or replaced (including identification numbers, if applicable).
ADR.45	The organization shall schedule, perform and document routine preventive and regular maintenance on the components of the control system in accordance with manufacturer or vendor specifications and/or organizational policies and procedures.
ADR.46	The organization shall approve, manage, protect and monitor the use of control system maintenance tools and maintains the integrity of tools on an ongoing basis.
ADR.47	The organization shall document authorization and approval policies and procedures and maintains a list of personnel authorized to perform maintenance on the control system. Only authorized and qualified organization or vendor personnel shall perform maintenance on the control system.
ADR.48	The organization shall authorize, manage, and monitor remotely executed maintenance and diagnostic activities on the control system. When remote maintenance is completed, the organization (or control system in certain cases) shall terminate all sessions and remote connections invoked in the performance of that activity. If password-based authentication is used to accomplish remote maintenance, the organization shall change the password following each remote maintenance service.
ADR.49	The organization shall acquire maintenance support and spare parts for key control system components within a specified time period of failure.
ADR.50	The organization shall: <ol style="list-style-type: none"> 1. Establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and 2. Authorize, monitor, and control the use of mobile code within the information system.
ADR.51	The security function shall separate user data from security function data when such data is transmitted between separate parts of the module.
ADR.52	The organization shall require that information system developers create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.

988

989 **3.3.2. Organizational Rigor (AOR)**

990 This section contains requirements regarding the policies employed by the organization(s) with
991 access to assets of a deployed smart grid system. These requirements reflect on an organization's
992 ability to continue to operate a smart grid system reliably over time. Topics include

- 993 • training procedures
- 994 • personnel security
- 995 • strategic planning
- 996 • monitoring and reviewing security policies

997

AOR.1	The organization shall develop, disseminate, and periodically review/update: <ol style="list-style-type: none"> 1. A formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.
AOR.2	The organization shall provide basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and [Assignment: organization-defined frequency, at least annually] thereafter.
AOR.3	The organization shall identify personnel that have significant information system security roles and responsibilities during the system development life cycle, documents those roles and responsibilities, and provides appropriate information system security training: <ol style="list-style-type: none"> 1. Before authorizing access to the system or performing assigned duties; 2. When required by system changes; and 3. [Assignment: organization-defined frequency] thereafter
AOR.4	The organization shall document and monitor individual information system security training activities including basic security awareness training and specific information system security training.
AOR.5	The organization shall establish and maintain contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations to stay up to date with the latest recommended security practices, techniques, and technologies and to share the latest security-related information including threats, vulnerabilities, and incidents.
AOR.6	The organization shall develop, disseminate, and periodically review/update: <ol style="list-style-type: none"> 1. A formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.
AOR.7	The organization shall restricts access to information system media to authorized individuals.
AOR.8	The organization shall: <ol style="list-style-type: none"> 1. Affix external labels to removable information system media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information; and 2. Exempt [Assignment: organization-defined list of media types or hardware components] from labeling so long as they remain within [Assignment: organization-defined protected environment].
AOR.9	The organization shall physically control and securely store information system media within controlled areas.
AOR.10	The organization shall protect and control information system media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel.
AOR.11	The organization shall sanitize information system media, both digital and non-digital, prior to disposal or release for reuse.
AOR.12	The organization shall develop, disseminate, and periodically review/update: <ol style="list-style-type: none"> 1. A formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

AOR.13	The organization shall develop and keep a current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and issues appropriate authorization credentials. Designated officials within the organization shall review and approve the access list and authorization credentials [Assignment: organization-defined frequency, at least annually].
AOR.14	The organization shall control all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. The organization shall control access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.
AOR.15	The organization shall control physical access to information system distribution and transmission lines within organizational facilities.
AOR.16	The organization shall control physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.
AOR.17	The organization shall monitor physical access to the information system to detect and respond to physical security incidents.
AOR.18	The organization shall control physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.
AOR.19	The organization shall maintain visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: <ol style="list-style-type: none"> 1. Name and organization of the person visiting; 2. Signature of the visitor; 3. Form of identification; 4. Date of access; 5. Time of entry and departure; 6. Purpose of visit; and 7. Name and organization of person visited. Designated officials within the organization shall review the visitor access records [Assignment: organization-defined frequency].
AOR.20	The organization shall protect power equipment and power cabling for the information system from damage and destruction.
AOR.21	The organization shall provide, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.
AOR.22	The organization shall provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.
AOR.23	The organization shall employ and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes.
AOR.24	The organization shall employ and maintain fire suppression and detection devices/systems that can be activated in the event of a fire.
AOR.25	The organization shall regularly maintain, within acceptable levels, and monitor the temperature and humidity within the facility where the information system resides.
AOR.26	The organization shall protect the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.
AOR.27	The organization shall authorize and control information system-related items entering and exiting the facility and maintains appropriate records of those items.

AOR.28	The organization shall employ appropriate management, operational, and technical information system security controls at alternate work sites.
AOR.29	The organization shall position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.
AOR.30	The organization shall protect the information system from information leakage due to electromagnetic signals emanations.
AOR.31	The organization shall develop, disseminate, and periodically review/update: <ol style="list-style-type: none"> 1. A formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.
AOR.32	The organization shall develop and implement a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization shall review and approve the plan
AOR.33	The organization shall review the security plan for the information system [Assignment: organization-defined frequency, at least annually] and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.
AOR.34	The organization shall establish and make readily available to all information system users, a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization shall receive signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.
AOR.35	The organization shall conduct a privacy impact assessment on the information system in accordance with regulatory and the organization's policy.
AOR.36	The organization shall plan and coordinate security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.
AOR.37	The organization shall develop, disseminate, and periodically review/update: <ol style="list-style-type: none"> 1. A formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls
AOR.38	The organization shall assign a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization shall review and revise position risk designations [Assignment: organization-defined frequency].
AOR.39	The organization shall screen individuals requiring access to organizational information and information systems before authorizing access.
AOR.40	The organization, upon termination of individual employment, shall terminate information system access, conducts exit interviews, retrieves all organizational information system-related property, and provide appropriate personnel with access to official records created by the terminated employee that are stored on organizational information systems.
AOR.41	The organization shall review information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization and initiates appropriate actions
AOR.42	The organization shall complete appropriate signed access agreements for individuals requiring access to organizational information and information systems before authorizing access and reviews/updates the agreements [Assignment: organization-defined frequency].

AOR.43	The organization shall establish personnel security requirements including security roles and responsibilities for third-party providers and monitors provider compliance.
AOR.44	The organization shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.
AOR.45	The organization shall develop, disseminate, and periodically review and update: <ol style="list-style-type: none"> 1. A formal, documented, personnel security policy that addresses: <ol style="list-style-type: none"> a. The purpose of the security program as it relates to protecting the organization's personnel and assets; b. The scope of the security program as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities, and management accountability structure of the security program to ensure compliance with the organization's security policy and other regulatory commitments; 2. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls. 3. Formal procedure to review and document list of approved personnel with access to control systems.
AOR.46	The organization shall assign a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization shall review and revise position risk designations periodically based on the organization's requirements or regulatory commitments.
AOR.47	The organization shall screen individuals requiring access to the control system before access is authorized.
AOR.48	When an employee is terminated, the organization shall revoke logical and physical access to control systems and facilities and ensure all organization-owned property is returned and that organization-owned documents and/or data files relating to the control system that are in the employee's possession be transferred to the new authorized owner within the organization. Complete execution of this control shall occur within 24 hours for employees or contractors terminated for cause.
AOR.49	The organization shall review logical and physical access permissions to control systems and facilities when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions. Complete execution of this control shall occur within 7 days for employees or contractors who no longer need to access control system resources.
AOR.50	The organization shall complete appropriate agreements for control system access before access is granted. This requirement applies to all parties, including third parties and contractors, who desire access to the control system. The organization shall review and update access agreements periodically.
AOR.51	The organization shall enforce security controls for third-party personnel and monitors service provider behavior and compliance.
AOR.52	The organization shall employ a formal accountability process for personnel failing to comply with established control system security policies and procedures and clearly documents potential disciplinary actions for failing to comply.
AOR.53	The organization shall provide employees and contractors with complete job descriptions and unambiguous and detailed expectations of conduct, duties, terms and conditions of employment, legal rights, and responsibilities.
AOR.54	The organization develops, implements, and periodically reviews and updates: <ol style="list-style-type: none"> 1. A formal, documented physical security policy that addresses: <ol style="list-style-type: none"> a. The purpose of the physical security program as it relates to protecting the organization's personnel and assets; b. The scope of the physical security program as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities and management accountability structure of the physical security program to ensure compliance with the organization's security policy and other regulatory commitments. 2. Formal, documented procedures to facilitate the implementation of the physical and

	environmental protection policy and associated physical and environmental protection controls.
AOR.55	The organization shall develop and maintain lists of personnel with authorized access to facilities containing control systems (except for areas within facilities officially designated as publicly accessible) and issue appropriate authorization credentials (e.g., badges, identification cards, smart cards). Designated officials within the organization shall review and approve the access list and authorization credentials at least annually.
AOR.56	The organization shall limit physical access to all control system facilities and assets and verify individual access authorizations before granting access. The organization shall limit access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.
AOR.57	The organization shall monitor physical access to the control system facilities to detect and respond to physical security incidents.
AOR.58	The organization shall limit physical access to control systems by authenticating visitors before authorizing access to facilities or areas other than areas designated as publicly accessible.
AOR.59	The organization shall maintain visitor access records to the control system facility (except for those areas within the facility officially designated as publicly accessible) that include: Name and organization of the person visiting; <ol style="list-style-type: none"> 1. Signature of the visitor; 2. Form of identification; 3. Date of access; 4. Time of entry and departure; 5. Purpose of visit; 6. Name and organization of person visited.
AOR.60	The organization shall retain all physical access logs for as long as dictated by any applicable regulations or based on an organization-defined period by approved policy.
AOR.61	For specific locations within a facility containing concentrations of control system resources (e.g., control centers, server rooms), the organization shall provide the capability of shutting off power to any component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without compromising personnel safety.
AOR.62	The organization shall provide a short-term Uninterruptible Power Supply (UPS) to facilitate an orderly shutdown of non-critical control system components in the event of a primary power source loss.
AOR.63	The organization shall employ and maintain automatic emergency lighting systems that activate in the event of a power outage or disruption and includes lighting for emergency exits and evacuation routes.
AOR.64	The organization shall implement and maintain fire suppression and detection devices/systems that can be activated in the event of a fire.
AOR.65	The organization shall regularly monitors the temperature and humidity within facilities containing control system assets and ensures they are maintained within acceptable levels.
AOR.66	The organization shall protect the control systems from water damage resulting from broken plumbing lines, fire control systems or other sources of water leakage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel.
AOR.67	The organization shall authorize and limit the delivery and removal of control system components (i.e., hardware, firmware, software) from control system facilities and maintain appropriate records and control of that equipment. The organization shall document policies and procedures governing

	the delivery and removal of control system assets in the control system security plan.
AOR.68	The organization shall establish an alternate control center with proper equipment and communication infrastructure to compensate for the loss of the primary control system worksite. The organization shall implement appropriate management, operational, and technical security measures at alternate control centers.
AOR.69	The organization shall monitor and prohibit the use of unapproved portable media use on the control system.
AOR.70	The organization shall implement asset location technologies to track and monitor the movements of personnel and vehicles within the organization's controlled areas to ensure they stay in authorized areas, to identify personnel needing assistance, and to support emergency response.
AOR.71	The organization shall locate control system assets to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.
AOR.72	The organization shall protect the control system from information leakage.
AOR.73	The organization shall protect control system power equipment and power cabling from damage and destruction.
AOR.74	The organization shall employ hardware (cages, locks, cases, etc.) to detect and deter unauthorized physical access to control system devices.
AOR.75	The organization shall develop, disseminate, and periodically review and update: <ol style="list-style-type: none"> 1. A formal, documented, planning policy that addresses: <ol style="list-style-type: none"> a. The purpose of the strategic planning program as it relates to protecting the organization's personnel and assets; b. The scope of the strategic planning program as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities, and management accountability structure of the strategic planning program to ensure compliance with the organization's security policy and other regulatory commitments. 2. Formal, documented procedures to facilitate the implementation of the strategic planning policy and associated strategic planning controls.
AOR.76	The organization shall develop and implement a security plan for the control system that provides an overview of the security requirements for the system and a description of the security measures in place or planned for meeting those requirements. Designated officials within the organization shall review and approve the control system security plan.
AOR.77	The organization shall identify potential interruptions and classify them as to "cause," "effects," and "likelihood."
AOR.78	The organization's control system security plan shall define and communicate the specific roles and responsibilities in relation to various types of incidents.
AOR.79	The organization shall include training on the implementation of the control system security plans for employees, contractors, and stakeholders into the organization's planning process.
AOR.80	The organization shall regularly test security plans to validate the control system objectives.
AOR.81	The organization shall include investigation and analysis of control system incidents in the planning process.
AOR.82	The organization shall include processes and mechanisms in the planning to ensure that corrective actions identified as the result of a cyber security and system incidents are fully implemented.
AOR.83	Risk-reduction mitigation measures shall be planned and implemented and the results monitored to ensure effectiveness of the organization's risk management plan.
AOR.84	The organization shall regularly, at prescribed frequencies, review the security plan for the control system and revise the plan to address system/organizational changes or problems identified during system security plan implementation or security controls assessment.

AOR.85	The organization shall establish and make readily available to all control system users a set of rules that describes their responsibilities and expected behavior with regards to control system usage. The organization shall obtain signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to the control system.
AOR.86	The organization shall plan and coordinate security-related activities affecting the control system before conducting such activities to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, or individuals.
AOR.87	The organization shall develop, disseminate, and periodically review/update: <ol style="list-style-type: none"> 1. A formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.
AOR.88	The organization shall provide basic security awareness training to all control system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and at least annually thereafter. The effectiveness of security awareness training, at the organization level, shall be reviewed at a minimum [assignment: once a year, etc.].
AOR.89	The organization shall identify and train personnel with significant control system security roles and responsibilities. The organization shall document the roles and responsibilities and provide appropriate control system security training before authorizing access to the system, when required by system changes, and with periodic training thereafter.
AOR.90	The organization shall document, maintain, and monitor individual control system security training activities, including basic security awareness training and specific information and control system security training in accordance with the organization's records retention policy.
AOR.91	The organization shall establish, participate with, and maintain contacts with special interest groups, industry vendor forums, specialized public or governmental forums, or professional associations to stay up to date with the latest recommended security practices, techniques, and technologies and to share the latest security-related information including threats, vulnerabilities, and incidents.
AOR.92	The organization shall document and test the knowledge of personnel on security policies and procedures based on their roles and responsibilities to ensure that they understand their responsibilities in securing the control system.
AOR.93	The organization shall develop, disseminate, and periodically review/update: <ol style="list-style-type: none"> 1. A formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 2. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.
AOR.94	The organization shall ensure that only authorized users have access to information in printed form or on digital media, whether integral to or removed from the control system.
AOR.95	The organization shall review and classify all removable information storage media and the control system output to determine distribution limitations [assignment: public, confidential, classified, etc.].
AOR.96	The organization shall affix external labels to removable information system media and to the control system output that indicate the distribution limitations [assignment: public, confidential, classified, etc.] and handling caveats of the information. The organization may exempt specific types of media or hardware components from labeling as long as they remain within a secure environment (as defined by the organization).
AOR.97	The organization shall physically manage and securely store control system media within protected areas. The sensitivity of the material delineates how the media is stored.
AOR.98	The organization shall develop security measures for paper and digital media extracted from the control system and restricts the pickup, receipt, transfer, and delivery of such media to authorized personnel.

AOR.99	The organization shall sanitize control system digital and non-digital media, before disposal or release for reuse.
AOR.100	The organization shall develop, disseminate, and periodically review/update: <ol style="list-style-type: none"> 1. A formal, documented, monitoring and reviewing control system security management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 2. Formal, documented procedures to facilitate the implementation of the monitoring and reviewing control system security management policy and associated audit and accountability controls.
AOR.101	The organization's security program shall implement continuous improvement practices to ensure that industry lessons-learned and best practices are incorporated into control system security policies and procedures.
AOR.102	The organization shall include a process for monitoring and reviewing the performance of their cyber security policy.
AOR.103	The organization shall incorporate industry best practices into the organization's security program for control systems.
AOR.104	The organization shall authorize (i.e., accredit) the control system for processing before operations and periodically updates the authorization based on organization-defined frequency or when there is a significant change to the system. A senior organizational official shall sign and approve the security accreditation.
AOR.105	The organization shall conduct an assessment of the security mechanisms in the control system to determine the extent to which the security measures are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
AOR.106	The organization shall establish policies and procedures to define roles, responsibilities, behaviors, and practices for the implementation of an overall security program.
AOR.107	The organization shall define a framework of management leadership accountability. This framework establishes roles and responsibilities to approve cyber security policy, assign security roles, and coordinate the implementation of cyber security across the organization.
AOR.108	Baseline practices that the organization shall employ for organizational security include, but are not limited to: <ol style="list-style-type: none"> 1. Executive management accountability for the security program; 2. Responsibility for control system security within the organization includes sufficient authority and an appropriate level of funding to implement the organization's security policy; 3. The organization's security policies and procedures that provide clear direction, accountability, and oversight for the organization's security team. The security team assigns roles and responsibilities in accordance with the organization's policies and confirms that processes are in place to protect company assets and critical information; 4. The organization's contracts with external entities that address the organization's security policies and procedures with business partners, third-party contractors, and outsourcing partners; 5. The organization's security policies and procedures ensure coordination or integration with the organization's physical security plan. Organization roles and responsibilities are established that address the overlap and synergy between physical and control system security risks.
AOR.109	The organization's security policies and procedures shall delineate how the organization implements its emergency response plan and coordinates efforts with law enforcement agencies, regulators, Internet service providers and other relevant organizations in the event of a security incident.
AOR.110	The organization shall hold external suppliers and contractors that have an impact on the security of the control center to the same security policies and procedures as the organization's own personnel. The organization shall ensure security policies and procedures of second- and third-tier suppliers comply with corporate cyber security policies and procedures if they will impact control system security.

AOR.111	The organization shall establish procedures to remove external supplier access at the conclusion/termination of the contract.
AOR.112	The organization shall: <ol style="list-style-type: none"> 1. Establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and 2. Authorize, monitor, and control the use of VoIP within the information system.
AOR.113	The organization shall display an approved system use notification (message) before granting access to the system.
AOR.114	The organization shall develop a formal written policy and appropriate security procedures to address and protect against the risks of remote access to the system, field devices, and communication facilities.
AOR.115	The organization shall restrict the use of personally owned information copied to the system or system user workstation that is used for official organization business. This includes the processing, storage, or transmission of organization business and critical system information. The terms and conditions need to address, at a minimum: <ol style="list-style-type: none"> 1. The types of applications that can be accessed from personally owned IT, either remotely or from within the organization's system; 2. The maximum security category of information that can processed, stored, and transmitted; 3. How other users of the personally owned system will be prevented from accessing organization information; 4. The use of virtual private networking (VPN) and firewall technologies; 5. The use of and protection against the vulnerabilities of wireless technologies; 6. The maintenance of adequate physical security mechanisms; 7. The use of virus and spyware protection software; and 8. How often the security capabilities of installed software are to be updated (e.g., operating system and other software security patches, virus definitions, firewall version updates, malware definitions).
AOR.116	The organization shall develop, disseminate and periodically review and update: <ol style="list-style-type: none"> 1. A formal, documented identification policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the identification policy and associated identification controls.
AOR.117	The organization shall develop, disseminate, and periodically review and update: <ol style="list-style-type: none"> 1. A formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 2. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.
AOR.118	The organization shall manage system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews system accounts at least [assignment: period of time (e.g., annually)].
AOR.119	The organization shall develop, disseminate, and periodically review/update: <ol style="list-style-type: none"> 1. A formal, documented, accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the accountability policy and associated audit and accountability controls.
AOR.120	The organization shall regularly review and analyze information system audit records: <ol style="list-style-type: none"> 1. For indications of inappropriate or unusual activity 2. To investigate suspicious activity or suspected violations 3. To report findings to appropriate officials, and 4. Take necessary actions.

AOR.121	The organization shall conduct audits at planned intervals to determine whether the security objectives, measures, processes, and procedures: <ol style="list-style-type: none"> 1. Conform to the requirements and relevant legislation or regulations; 2. Conform to the identified information security requirements; 3. Are effectively implemented and maintained; 4. Perform as expected; 5. Identify inappropriate activities.
AOR.122	The organization's audit program shall specify auditor qualifications in accordance with the organization's documented training program.
AOR.123	The organization under the audit program shall specify strict rules and careful use of audit tools when auditing control system functions.
AOR.124	The organization shall demonstrate compliance to the organization's security policy through audits in accordance with the organization's audit program.

998

999 **3.3.3. Handling/Operating Rigor (AHR)**

1000 This section contains requirements regarding the activities involved in the day-to-day operation
1001 of deployed smart grid systems. Topics include

- 1002 • information and document management policies
- 1003 • incident response procedures
- 1004 • maintenance procedures
- 1005 • physical and environmental security
- 1006 • media protection

1007

AHR.1	The organization shall develop, disseminate, and periodically review/update: <ol style="list-style-type: none"> 1. A formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.
AHR.2	The organization shall develop and implement a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization shall review and approve the contingency plan and distribute copies of the plan to key contingency personnel.
AHR.3	The organization shall train personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [Assignment: organization-defined frequency, at least annually].
AHR.4	The organization shall: <ol style="list-style-type: none"> 1. Test and/or exercise the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and/or exercises] to determine the plan's effectiveness and the organization's readiness to execute the plan; and 2. Review the contingency plan test/exercise results and initiates corrective actions.
AHR.5	The organization shall review the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

AHR.6	The organization shall identify an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.
AHR.7	The organization shall identify an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within [Assignment: organization-defined time period] when the primary processing capabilities are unavailable.
AHR.8	The organization shall identify primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable.
AHR.9	The organization shall conduct backups of user-level and system-level information (including system state information) contained in the information system [Assignment: organization-defined frequency] and protects backup information at the storage location.
AHR.10	The organization shall employ mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.
AHR.11	The organization shall develop, disseminate, and periodically review/update: <ol style="list-style-type: none"> 1. A formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.
AHR.12	The organization shall train personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training [Assignment: organization-defined frequency, at least annually].
AHR.13	The organization shall test and/or exercise the incident response capability for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and/or exercises] to determine the incident response effectiveness and documents the results.
AHR.14	The organization shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
AHR.15	The organization tracks and documents information system security incidents on an ongoing basis.
AHR.16	The organization promptly reports incident information to appropriate authorities.
AHR.17	The organization shall provide an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incident (The support resource is an integral part of the organization's incident response capability).
AHR.18	The organization shall develop, disseminate and periodically review/update: <ol style="list-style-type: none"> 1. A formal, documented, control system information and document management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. 2. Formal, documented procedures to facilitate the implementation of the control system information and document management policy and associated system maintenance controls.
AHR.19	The organization shall manage control system related data, including establishing retention policies and procedures for both electronic and paper data, and manages access to the data based on formally assigned roles and responsibilities.
AHR.20	Organization implemented policies and procedures detailing the handling of information shall be developed and periodically reviewed and updated.
AHR.21	All information shall be classified to indicate the protection required commensurate with its sensitivity and consequence.
AHR.22	Formal contractual and confidentiality agreements shall be established for the exchange of

	information and software between the organization and external parties.
AHR.23	The organization shall develop policies and procedures to classify data, including establishing: <ol style="list-style-type: none"> 1. Retention policies and procedures for both electronic and paper media; 2. Classification policies and methods, (e.g., restricted, classified, general, etc.); 3. Access and control policies, to include sharing, copying, transmittal, and distribution appropriate for the level of protection required; 4. Access to the data based on formally assigned roles and responsibilities for the control system.
AHR.24	The organization shall develop policies and procedures that provide details of the retrieval of written and electronic records, equipment, and other media for the control system in the overall information and document management policy.
AHR.25	The organization shall develop policies and procedures detailing the destruction of written and electronic records, equipment, and other media for the control system, without compromising the confidentiality of the data.
AHR.26	The organization shall perform periodic reviews of compliance with the control system information and document security management policy to ensure compliance with any laws and regulatory requirements.
AHR.27	The control system shall automatically marks data output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.
AHR.28	The control system shall automatically label information in storage, in process and in transmission.
AHR.29	The organization shall develop, disseminate, and periodically review/update: <ol style="list-style-type: none"> 1. A formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.
AHR.30	The organization shall develop and implement a continuity of operations plan dealing with the overall issue of maintaining or re-establishing production in case of an undesirable interruption for a control system. The plan shall address roles, responsibilities, assigned individuals with contact information, and activities associated with restoring system operations after a disruption or failure. Designated officials within the organization shall review and approve the continuity of operations plan.
AHR.31	The organization's continuity of operations plan shall define and communicate the specific roles and responsibilities for each part of the plan in relation to various types of control system incidents.
AHR.32	The organization shall train personnel in their continuity of operations plan roles and responsibilities with respect to the control system. The organization shall provide refresher training at least annually. The training covers employees, contractors, and stakeholders in the implementation of the continuity of operations plan.
AHR.33	The organization shall test the continuity of operations plan to determine its effectiveness and documents the results. Appropriate officials within the organization shall review the documented test results and initiate corrective actions if necessary. The organization shall test the continuity of operations plan for the control system at least annually, using organization prescribed tests and exercises to determine the plan's effectiveness and the organization's readiness to execute the plan.
AHR.34	The organization shall review the continuity of operations plan for the control system at least annually and updates the plan to address system, organizational, and technology changes or problems encountered during plan implementation, execution, or testing.
AHR.35	The organization shall implement control system incident handling capabilities for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
AHR.36	The organization shall track and document control system network security incidents on an ongoing basis.
AHR.37	The organization shall promptly report cyber and control system security incident information to the appropriate authorities.

AHR.38	The organization shall provide an incident response support resource that offers advice and assistance to users of the control system for the handling and reporting of security incidents (The support resource is an integral part of the organization's incident response capability).
AHR.39	The organization shall document its policies and procedures to show that investigation and analysis of incidents are included in the planning process. The procedures shall ensure that the control system is capable of providing event data to the proper personnel for analysis and for developing mitigation steps. The organization shall ensure that a dedicated group of personnel is assigned to periodically review the data at a minimum monthly.
AHR.40	The organization shall include processes and mechanisms in the planning to ensure that corrective actions identified as the result of a cyber security incident are fully implemented.
AHR.41	The organization shall identify an alternate storage site and initiates necessary agreements to permit the storage of control system configuration information.
AHR.42	The organization shall identify alternate command/control methods for the control system and initiates necessary agreements to permit the resumption of operations for the safe operation of the control system within an organization-defined time period when the primary system capabilities are unavailable.
AHR.43	The organization shall identify an alternate control center, necessary telecommunications, and initiates necessary agreements to permit the resumption of control system operations for critical functions within [assignment: an organization-prescribed time period] when the primary control center is unavailable.
AHR.44	The organization shall conduct backups of critical control system information, including state of the user-level and system level information, process formulas, system inventories, etc., contained in the control system, on a regular schedule as defined by the organization, and stores the information at an appropriately secured location.
AHR.45	The organization shall employ mechanisms with supporting procedures to allow the control system to be recovered and reconstituted to the system's original state after a disruption or failure.
AHR.46	The control system shall have the ability to execute an appropriate fail safe procedure upon the loss of communications with the control system or the loss of the control system itself.
AHR.47	The organization shall retain audit records for [Assignment: organization-defined time period] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

1008

1009 3.3.4. Accountability (AAY)

1010 "Security auditing involves recognizing, recording, storing, and analyzing information related to
1011 security relevant activities (i.e. activities controlled by the TSF). The resulting audit records can
1012 be examined to determine which security relevant activities took place and whom (which user) is
1013 responsible for them." [CC]

1014

AAY.1	The organization shall manage control system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization shall review control system accounts [assignment: time period (e.g., at least annually)].
AAY.3	The organization shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization shall review information system accounts [Assignment: organization-defined frequency, at least annually].
AAY.4	The information system shall enforce a limit of [Assignment: organization-defined number] consecutive invalid access attempts by a user during a [Assignment: organization-defined time period] time period. The information system automatically [Selection: locks the account/node for an [Assignment: organization-defined time period], delays next login prompt according to [Assignment: organization-defined delay algorithm.]] when the maximum number of unsuccessful attempts is

	exceeded.
AAY.5	The organization shall develop, disseminate, and periodically review/update: <ol style="list-style-type: none"> 1. A formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.
AAY.6	The organization shall develop, disseminate, and periodically review/update: <ol style="list-style-type: none"> 1. A formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 2. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.
AAY.7	The control system shall generate audit records, at a minimum, for the following events whether or not the attempts were successful: <ol style="list-style-type: none"> 1. Attempts to logon; 2. Attempts to change local account attributes such as privileges; 3. Attempts to change local security policy.
AAY.8	The organization shall develop, implement, and periodically review and update: <ol style="list-style-type: none"> 1. A formal, documented, control system security policy that addresses: <ol style="list-style-type: none"> a. The purpose of the security program as it relates to protecting the organization's personnel and assets; b. The scope of the security program as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities, and management accountability structure of the security program to ensure compliance with the organization's security policy and other regulatory commitments. 2. Formal, documented procedures to implement the security policy and associated requirements. A control system security policy considers controls from each of the families contained in this document.
AAY.9	The organization shall define a framework of management leadership accountability. This framework establishes roles and responsibilities to approve cyber security policy, assign security roles, and coordinate the implementation of cyber security across the organization.
AAY.10	Baseline practices that organizations employ for organizational security shall include, but are not limited to: <ol style="list-style-type: none"> 1. Executive management accountability for the security program; 2. Responsibility for control system security within the organization includes sufficient authority and an appropriate level of funding to implement the organization's security policy; 3. The organization's security policies and procedures that provide clear direction, accountability, and oversight for the organization's security team. The security team assigns roles and responsibilities in accordance with the organization's policies and confirms that processes are in place to protect company assets and critical information; 4. The organization's contracts with external entities that address the organization's security policies and procedures with business partners, third-party contractors, and outsourcing partners; 5. The organization's security policies and procedures ensure coordination or integration with the organization's physical security plan. Organization roles and responsibilities are established that address the overlap and synergy between physical and control system security risks.
AAY.11	The organization shall develop, disseminate, and periodically review and update: <ol style="list-style-type: none"> 1. A formal, documented system and communication protection policy that addresses: <ol style="list-style-type: none"> a. The purpose of the system and communication protection policy as it relates to protecting the organization's personnel and assets; b. The scope of the system and communication protection policy as it applies to all

	<p>the organizational staff and third-party contractors;</p> <ol style="list-style-type: none"> c. The roles, responsibilities and management accountability structure of the security program to ensure compliance with the organization's system and communications protection policy and other regulatory commitments; <ol style="list-style-type: none"> 2. Formal, documented procedures to facilitate the implementation of the control system and communication protection policy and associated systems and communication protection controls.
AA.Y.12	<p>The organization shall develop, disseminate, and periodically review/update:</p> <ol style="list-style-type: none"> 1. A formal, documented, system and services acquisition policy that addresses: <ol style="list-style-type: none"> a. The purpose of the security program as it relates to protecting the organization's personnel and assets; b. The scope of the security program as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities and management accountability structure of the security program to ensure compliance with the organization's security policy and other regulatory commitments. 2. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.
AA.Y.13	<p>The organization shall develop, disseminate, and periodically review and update:</p> <ol style="list-style-type: none"> 1. A formal, documented Configuration Management policy that addresses: <ol style="list-style-type: none"> a. The purpose of the configuration management policy as it relates to protecting the organization's personnel and assets; b. The scope of the configuration management policy as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities and management accountability structure contained in the configuration management policy to ensure compliance with the organization's security policy and other regulatory commitments. 2. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. 3. The personnel qualification levels required to make changes, the conditions under which changes are allowed, and what approvals are required for those changes.
AA.Y.14	<p>The organization shall develop, disseminate, and periodically review and update:</p> <ol style="list-style-type: none"> 1. A formal, documented, personnel security policy that addresses: <ol style="list-style-type: none"> a. The purpose of the security program as it relates to protecting the organization's personnel and assets; b. The scope of the security program as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities, and management accountability structure of the security program to ensure compliance with the organization's security policy and other regulatory commitments; 2. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls. 3. Formal procedure to review and document list of approved personnel with access to control systems.
AA.Y.15	<p>The organization shall employ a formal accountability process for personnel failing to comply with established control system security policies and procedures, and clearly document potential disciplinary actions for failing to comply.</p>
AA.Y.16	<p>The organization shall develop, implement, and periodically review and update:</p> <ol style="list-style-type: none"> 1. A formal, documented physical security policy that addresses: <ol style="list-style-type: none"> a. The purpose of the physical security program as it relates to protecting the organization's personnel and assets; b. The scope of the physical security program as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities and management accountability structure of the physical security program to ensure compliance with the organization's security policy and other regulatory commitments. 2. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection

	controls.
AAY.17	The organization shall develop, disseminate, and periodically review and update: <ol style="list-style-type: none"> 1. A formal, documented, planning policy that addresses: <ol style="list-style-type: none"> a. The purpose of the strategic planning program as it relates to protecting the organization's personnel and assets; b. The scope of the strategic planning program as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities, and management accountability structure of the strategic planning program to ensure compliance with the organization's security policy and other regulatory commitments. 2. Formal, documented procedures to facilitate the implementation of the strategic planning policy and associated strategic planning controls.
AAY.18	The organization shall develop, disseminate, and periodically review/update: <ol style="list-style-type: none"> 1. A formal, documented, monitoring and reviewing control system security management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 2. Formal, documented procedures to facilitate the implementation of the monitoring and reviewing control system security management policy and associated audit and accountability controls.
AAY.19	Baseline practices that the organization employs for organizational security shall include, but are not limited to: <ol style="list-style-type: none"> 1. Executive management accountability for the security program; 2. Responsibility for control system security within the organization includes sufficient authority and an appropriate level of funding to implement the organization's security policy; 3. The organization's security policies and procedures that provide clear direction, accountability, and oversight for the organization's security team. The security team assigns roles and responsibilities in accordance with the organization's policies and confirms that processes are in place to protect company assets and critical information; 4. The organization's contracts with external entities that address the organization's security policies and procedures with business partners, third-party contractors, and outsourcing partners; 5. The organization's security policies and procedures ensure coordination or integration with the organization's physical security plan. Organization roles and responsibilities are established that address the overlap and synergy between physical and control system security risks.

1015

1016 **3.3.5. Access Control (AAC)**

1017 "The focus of access control is ensuring that resources are only accessed by the appropriate
1018 personnel and that personnel are correctly identified. The first step in access control is creating
1019 access control lists with access privileges for personnel. The next step is to implement security
1020 mechanisms to enforce the access control lists. Mechanisms also need to be put into place to
1021 monitor access activities for inappropriate activity. The access control lists need to be managed
1022 through adding, altering, and removing access rights as necessary.
1023 Identification and authentication is the process of verifying the identity of a user, process, or
1024 device, as a prerequisite for granting access to resources in a control system. Identification could
1025 be a password, a token, or a fingerprint. Authentication is the challenge process to prove
1026 (validate) the identification provided. An example would be using a fingerprint (identification) to

1027 access a computer via a biometric device (authentication). The biometric device authenticates the
 1028 identity of the fingerprint." [DHS]
 1029

AAC.1	The organization shall develop, disseminate, and periodically review/update: <ol style="list-style-type: none"> 1. A formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 2. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.
AAC.2	The organization shall supervise and review the activities of users with respect to the enforcement and usage of control system access control.
AAC.3	The security function shall enforce the [assignment: access control security function policy] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the security function policy].
AAC.4	The security function shall enforce the [assignment: access control security function policy] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the security function policy.
AAC.5	The security function shall ensure that all operations between any subject controlled by the security function and any object controlled by the security function are covered by an access control security function policy.
AAC.6	The security function shall enforce the [assignment: access control security function policy] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated security function policy, and for each, the security function policy-relevant security attributes, or named groups of security function policy-relevant security attributes].
AAC.7	The security function shall enforce the [assignment: access control security function policy(s) and/or information flow control security function policy(s)] when exporting user data, controlled under the security function policy(s), outside of the module.
AAC.8	The organization shall develop, disseminate, and periodically review/update: <ol style="list-style-type: none"> 1. A formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.
AAC.9	The organization shall supervise and review the activities of users with respect to the enforcement and usage of information system access controls.
AAC.10	The security function shall enforce the [assignment: access control security function policy(s), information flow control security function policy(s)] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorized identified roles].
AAC.11	The security function shall enforce the [assignment: access control security function policy, information flow control security function policy] to provide [selection, choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the security function policy.
AAC.12	The organization shall review logical and physical access permissions to control systems and facilities when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions. Complete execution of this control occurs within [Assignment: time period (e.g., 7 days)] for employees or contractors who no longer need to access control system resources.
AAC.13	The organization shall supervise and review the activities of users with respect to the enforcement and usage of system access control.

1030
 1031

1032 **Appendix A: Architectural Description**

1033 This appendix contains information that is non-formative to the architecture of AMI security, but
1034 provides useful background and understanding.

1035 **A.1. Scope**

1036 Advanced Metering Infrastructure (AMI) Security Architecture as defined by the AMI-SEC
1037 taskforce is:

1038 *The communications hardware and software and associated system and data management*
1039 *software that creates a network between advanced meters and utility business systems and which*
1040 *allows collection and distribution of information to customers and other parties such as*
1041 *competitive retail providers, in addition to providing it to the utility itself. AMI is further defined*
1042 *as: 1) The hardware and software residing in, on, or closest to the customer premise for which*
1043 *the utility or its legal proxies are primarily responsible for proper operation; and 2) The*
1044 *hardware and software owned and operated by the utility or its legal proxies which has as its*
1045 *primary purpose the facilitation of Advanced Metering.*

1046 The goal of this document is to describe the abstract (logical, platform-agnostic) mitigation plan
1047 for addressing requirements identified in the Risk Assessment / System Requirements Document.

1048 The following approach has been taken in designing the system:

1049 Approach

- 1050 • Architectural Representation of Security Systems
- 1051 • Logical Function Descriptions
- 1052 • System, Subsystem, and Function Boundaries
- 1053 • Reference: IEEE 1471-2000

1054 This document is intended to focus on security architecture, and is not intended to cover
1055 enterprise level AMI architecture, except to describe a security concept. The objective of
1056 architecting is to decompose the system into its primary views in order to describe the system
1057 enough to complete the mission of AMI security. The architecture does not extend beyond the
1058 external visible properties of the elements of the system. That is, non-visible properties are left to
1059 the designers, implementers and integrators of the system.

1060 The following image represents the 10,000 foot view of AMI. This document begins by
1061 explaining the interactions between external actors and the AMI system (see section 3.1). The
1062 next view zooms in on the AMI system by describing the system with a decomposition view
1063 (section 3.2). Each iteration provides deeper granularity and traceability between views.

1064
1065 AMI-SEC is developing other relevant documentation in parallel that supports the Architectural
1066 Description (AD) including the AMI Risk Analysis and System Security Requirements (SSR)
1067 documents. The Risk Analysis walks the utility through a method of determining a risk-to-value
1068 of an asset. Assets in terms of these documents are considered to be the business level value
1069 streams to the utility. The appendix of the AMI Risk Analysis includes catalogues for assets,
1070 vulnerabilities, and threats. The SSR document includes AMI-SEC's approach to conducting a
1071 requirements assessment and applying requirements. Traceability between views in the AD and
1072 requirements defined in the SSR are maintained for consistency and rationale.

1073 This document develops security around commonly known AMI use cases selected from use
1074 cases shared by utilities to AMI-SEC. It is assumed that AMI will evolve supporting additional
1075 uses and variants, but these uses cannot be predicted. Therefore, a goal of this AD is to group use
1076 cases that possess commonality in security treatment in order to support the evolution of AMI.

1077 **A.2. Mission**

1078 The mission of the AMI Security Architecture is to provide understanding of AMI security,
1079 communication among stakeholders and serve as a basis for system analysis. It is important to
1080 understand that the task of this architecture is not to provide the groundwork to build the entire
1081 AMI system, but to secure it, which is inherently nontrivial.

1082 The information contained in this document will provide an introduction to AMI Security to
1083 interested parties. Newcomers will find this document a starting point for understanding the
1084 elements, interfaces, and structure of AMI security.

1085 This document will serve to provide communication among stakeholders including designers of
1086 the system, implementers, integrators, testers and operators. All architecture is design, but not all
1087 design is considered architecture. The mission in communication is to produce sufficient
1088 guidance for stakeholders so that they understand the architecture well enough to perform their
1089 role.

1090 The architecture will also serve to provide information needed the support analysis performed for
1091 security objectives including availability, integrity, confidentiality, access control and
1092 accounting.

1093 The architecture will cross-check with information contained in the Requirements document to
1094 provide reasoning for requirements selection.

1095 **A.3. Stakeholders & Concerns**

1096 This section describes the stakeholders and their concerns. A stakeholder is any individual or
1097 group of individuals with interests or concerns associated with the system. All actors of the
1098 system are stakeholders, but not all stakeholders are actors. For example, an investor may have a
1099 stake in the success of the AMI system, but may not interact directly with the AMI system.
1100 Stakeholders identified to be relevant to the security architecture are:

- 1101 • Customer Users of the system
- 1102 • Operators of the system
- 1103 • Responsible Entities of the systems
- 1104 • Developers of the system
- 1105 • Implementers of the system
- 1106 • Maintainers of the system

1107 Concerns that stakeholders may have from a security perspective for the entire AMI system

1108 ***General Stakeholder Concerns:***

- 1109 • Integrity of the system
- 1110 • Availability of the system

- 1111 • Confidentiality of the system
- 1112 • The purpose or missions of the system as pertains to security
- 1113 • The appropriateness of the system for use in fulfilling its missions to security
- 1114 • The feasibility of constructing the system
- 1115 • The risks of system development and operation to users, acquirers, and developers of the
- 1116 system
- 1117 • Maintainability, deploy-ability, and evolve-ability of the system

1118 Each viewpoint defined for AMI security possesses specific concerns defined with each
 1119 viewpoint under the following section.

1120 Potential examples of AMI security concerns by stakeholders:

STAKEHOLDER	SECURITY CONCERN
Residential Customer	Privacy
Utility Operator	Integrity of information and system control
Regulators	Integrity of system and compliance with regulations
Telecom Provider	Compliance with contractual obligations and regulations

1121 **Table 10 – Stakeholder Security Concerns**

1122 **A.4. Security Analysis Approach**

1123 The security analysis approach is to evaluate each view under the security principles of
 1124 availability, integrity, confidentiality, access control and accountability. The high level models
 1125 are in the form of Use Cases. At least one security objective is identified with each Use Case by
 1126 evaluating against these security principles.

- 1127 • Availability
 - 1128 ○ Ensure the desired resource is available at the time it is needed.
 - 1129 ○ Ensure the desired resource is accessible in the intended manner by the
 - 1130 appropriate entity.
- 1131 • Integrity
 - 1132 ○ Ensure the desired resource contains accurate information.
 - 1133 ○ Ensure the desired resource performs precisely as intended.
- 1134 • Confidentiality
 - 1135 ○ Ensure the desired resource is only accessible to the desired targets.
 - 1136 ○ Ensure the desired resource is only accessible under the designated conditions.
- 1137 • Access Control
 - 1138 ○ Ensure resource access follows the designated procedure.

- 1139 ○ Ensure access mechanisms provide sufficient management capabilities to
- 1140 establish, modify, and remove desired criteria.
- 1141 • Accountability
- 1142 ○ Ensure system activities can be reconstructed, reviewed, and examined from
- 1143 transaction inception to output of final results.
- 1144 ○ Ensure system controls are provably compliant with established policy and
- 1145 procedures.

1146 **A.5. Architecture Description Approach**

1147 This section is an introduction to the approach of describing the AMI architecture based on IEEE
 1148 1471-2000, *IEEE Recommended Practice for Architectural Description of Software-Intensive*
 1149 *Systems*. This section serves as a Roadmap for appendix A and provides a guide for where to
 1150 locate information.

1151 This section introduces templates and patterns that will be used in subsequent sections. Each
 1152 view describes:

- 1153 • What viewpoint it realizes
 - 1154 ○ Name & definition of the viewpoint (external pointer or brief definition)
 - 1155 ○ What stakeholders and concerns it addresses (and to what extent)
 - 1156 ○ Language/notation to be used
- 1157 • One or more models, where a model includes:
 - 1158 ○ Context diagram (i.e., how it relates to AMI as a whole or to other models within
 - 1159 the same view)
 - 1160 ○ A picture or other primary presentation, always with a key or legend
 - 1161 ○ Brief descriptions (or pointers to such) for each element and relation type in the
 - 1162 primary presentation
 - 1163 ○ Related models, such as scenarios related to the view
 - 1164 ○ Known or anticipated variations (likely very important here)
 - 1165 ○ Rationale, assumptions, or other background for the decisions depicted in the
 - 1166 view

1167 **A.5.1. Viewpoints**

1168 IEEE 1471-2000 describes a viewpoint on a system as – “a form of abstraction achieved using a
 1169 selected set of architectural constructs and structuring rules, in order to focus on particular
 1170 concerns within a system. The relationship between viewpoint and view is analogous to that of a
 1171 template and an instance of that template.” Therefore, a viewpoint may contain:

- 1172 • Specifications of each viewpoint that has been selected to organize the representation of
- 1173 the architecture and the rationale for those selections
- 1174 • One or more architectural views

1175 • A record of all known inconsistencies among the architectural description's required
1176 constituents

1177 • A rationale for selection of the architecture

1178 Each viewpoint shall be specified by:

1179 1. A viewpoint name,

1180 2. The stakeholders to be addressed by the viewpoint,

1181 3. The concerns to be addressed by the viewpoint,

1182 4. The language, modeling techniques, or analytical methods to be used in constructing a
1183 view based upon the viewpoint,

1184 5. The source, for a library viewpoint (the source could include author, date, or reference to
1185 other documents, as determined by the using organization).

1186 A viewpoint specification may include additional information on architectural practices
1187 associated with using the viewpoint, as follows:

1188 • Formal or informal consistency and completeness tests to be applied to the models
1189 making up an associated view

1190 • Evaluation or analysis techniques to be applied to the models

1191 • Heuristics, patterns, or other guidelines to assist in synthesis of an associated view

1192 Viewpoint specifications may be incorporated by reference (such as to a suitable recommended
1193 practice or previously defined practice). An architectural description shall include a rationale for
1194 the selection of each viewpoint. The rationale shall address the extent to which the stakeholders
1195 and concerns are covered by the viewpoints selected.

1196 **A.5.2. Views**

1197 An architectural description is organized into one or more constituents called (architectural)
1198 views. Each view addresses one or more of the concerns of the system stakeholders. The term
1199 view is used to refer to the expression of a system's architecture with respect to a particular
1200 viewpoint.

1201
1202 The relationship between viewpoint and view is analogous to that of a template and an instance
1203 of that template. The *viewpoint* is the template and the *view* is the instance of the template.

1204 **A.6 Contextual View**

1205 The primary goal of this view is to identify the external points of interaction (physical and
1206 logical/data) between AMI and anything outside of AMI. Once these points of interaction are
1207 defined, security architecture is developed to address the concerns of the stakeholders involved.
1208 Use cases are used to model customer, third party and utility interactions with AMI in sections
1209 2.1.2, 2.1.3 and 2.1.4.

1210 Elaborations of the interactions in this view are unlikely to be complete; they should however
1211 provide representative examples of –

- 1212 • Use cases of the outside world interacting with (stimulating) AMI
- 1213 • Use cases of AMI interacting with (stimulating) the outside world
- 1214 • Misuse or abuse cases in either direction; that is, specific uses that should be prevented
- 1215 • Any actor sub-categories where the actor uses the system in a fashion that implies
- 1216 security needs that differ from major actors (e.g., leading to identification of access
- 1217 domains/privilege levels)
- 1218 • Physical interactions (e.g., installing a meter or physical access to assets like collectors)
- 1219 • Logical interactions (e.g., user monitors or modifies settings with the utility via web
- 1220 browser or utility initiates a demand-response interaction with a residence)
- 1221 Elements of the view are the AMI system (as a black box), human actors, and connected
- 1222 systems. Relations of the view are vague - "interacts with", with elaboration in the prose.

1223 A.7 Top Level Model

1224 The top level model represents a high level view of the external stakeholders that interact with
 1225 the AMI system. This model is used to provide an understanding of security concerns of
 1226 interaction with AMI for these stakeholders.

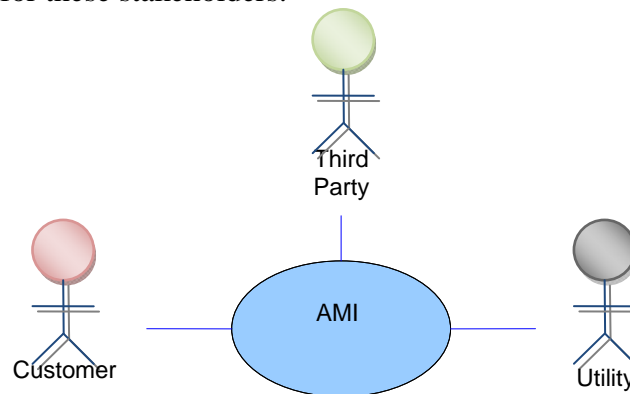


Figure 4 – AMI Top Level Model

1227 General security interaction needs:

- 1228 • Customers are the consumers of AMI services and have a primary desire of availability
 1229 and privacy from AMI and service value.
- 1230 • Third Parties manage AMI resources with delegated authority from the Customer or
 1231 Utility through an established trust relationship.
- 1232 • Utilities provide AMI services and primary desire reliably gather information from the
 1233 Customer to support the availability, resiliency and survivability of the electric grid.

1234 Constraints:

- 1235 • Bandwidth – current technologies have limited bandwidth for providing security services
 1236 (examples: encryption, network management services).

- 1237 • Latency – the time between when data is requested or generated and the time it is
1238 received. In many cases, data is only useful if received within a specific window of time.
- 1239 • Storage – devices that store information either persistently or stage data temporarily are
1240 limited in the amount of data they are capable of storing at any given time.
- 1241 • Processing – the rate at which a device can process information. It is important to keep in
1242 mind cryptographic functions require additional processing horsepower above normal
1243 processor usage.

1244 **A.7.1. Customer Model**

1245 The customer model focuses on the interactions between a customer and the AMI system.
1246 Customers may include sub-actors such as:

- 1247 • Residential Customer (Private home owners)
- 1248 • Commercial Customer (Office buildings, Apartment Complexes)
- 1249 • Industrial Customer (Manufacturing plants)
- 1250 • Municipalities Customer (Street lights, traffic lights, subways)

1251 Sub-actors may be considered in the instance that there is different security treatment applied
1252 based on the role a sub-actor plays. If the security treatment of all sub-actors is the same or
1253 similar then the group is treated as a whole. The differentiating properties are identified in the
1254 cases where sub-actors only differ slightly in the treatment of security. The following diagram
1255 represents the relationship between the customer and AMI system where the customer may
1256 perform a stimulus on the AMI system or vice versa.

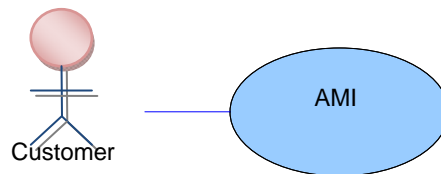


Figure 5 - Customer Model

1257 The following use cases are used to define the relationship between the customer and AMI:
1258 **Customer reduces their usage in response to pricing or voluntary load reduction event:**

- 1259 • The utility can notify customers through the AMI system that demand reduction is
1260 requested for the purposes of either improving grid reliability, performing economic
1261 dispatch (energy trading), or deferring buying energy.

1262 There are two levels of advanced warning which are envisioned for AMI demand
1263 response systems as outlined in Distribution Use Case 2. The first being predicted energy
1264 shortages—a few hours notice in advanced—and the emergency shortages—minute to
1265 sub-minute notices.

Security Objective:

- 1267 ○ Prevent false warnings from reaching the customer.

1268 ○ Ensure that only people and/or systems that are authorized by the utility can send
1269 warnings to the customer

1270 ○ Ensure that the system is resilient to periods of over-subscribed network
1271 utilization, especially in the case of emergency shortages.

1272 ● **Customer has access to recent energy usage and cost at their site:**

1273 ● Customers can view a variety of information being gathered by their meter, permitting
1274 them to make energy-efficient choices and to shift demand to off-peak periods.
1275 Customers may access this information through a variety methods.

1276 **Security Objective:**

1277 ○ Protect the variety of methods of access from unauthorized access by
1278 unauthorized persons outside of the site.

1279 ○ Protect the confidentiality of the usage and data associated with a particular
1280 customer or site.

1281 ○ Protect the devices that communicate the usage and cost data from tampering.

1282 ○ Validate that the communication of the usage and cost data is in a manner that is
1283 consistent with the utilities intent. For example, display only “need to know”
1284 data; ensure that all displayed data is consistent with respect to reality.

1285 **Customer prepays for electric services:**

1286 ● Customers of the AMI system can prepay their accounts and read their current balance.
1287 Pre-pay may be done through the internet, phone, or other method.

1288 **Security Objective:**

1289 ○ Compliance with PCI or other applicable standard is required by utilities or
1290 financial entities

1291 ○ Ensure that the AMI system and/or payment devices are resistant to payment
1292 fraud of many types

1293 ○ Ensure that payment data confidentiality is maintained

1294 **External clients use the AMI system to interact with devices at customer site:**

1295 ● The Advanced Meter Infrastructure (AMI) will enable third parties, such as energy
1296 management companies, to use the communication infrastructure as a gateway to monitor
1297 and control customer equipment located at the customer’s premise. The AMI will be
1298 required to enable on-demand requests and support a secure environment for the
1299 transmission of customer confidential information.

1300 **Security Objective:**

1301 ○ Ensure that all third-parties agree to some standard of data confidentiality
1302 agreement.

1303 ○ Ensure that all third-parties agree to some standard of granting access to systems
1304 which allow access to monitor and control customer equipment at the premise.

- 1305 ○ Ensure that all communications that result in an action with equipment at a
- 1306 customer premise is authorized, authenticated, non-repudiated, logged.
- 1307 ○ Ensure that the communication path to a customer premise that allows control of
- 1308 equipment is secured and tamper proof.
- 1309 ○ Ensure that customers are required to agree to specific third-party access to their
- 1310 premise gateway.

1311 **A.7.2. Third Party Model**

1312 The third party model represents the interaction between third parties and the AMI system. Third
 1313 parties include utility contracted organizations such as a telecom provider, other utility, etc.
 1314 Third parties may also include organizations that have established contracts with the customer
 1315 for managing their premise devices within the home area network, for example an energy
 1316 management system.

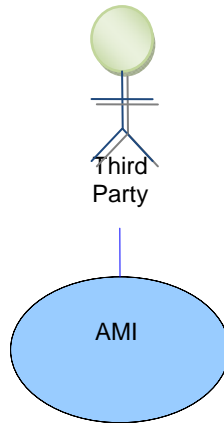


Figure 6 - Third Party Model

1317 The following are use cases describing the relationships between potential third parties and the
 1318 AMI system.
 1319

1320 **Multiple Clients Read Demand and Energy Data Automatically from Customer Premises:**

- 1321 • The AMI system can be used to permit gas and water utilities, contract meter readers,
- 1322 aggregators and other third parties to read electrical meters, read gas and water meters, or
- 1323 control third-party equipment on customer premises.

1324 **Security Objective:**

- 1325 ○ To protect customer information. Customer grants the right to what information is
- 1326 disseminated and to whom.
- 1327 ○ To maintain integrity of meter data. Meter data should be protected from
- 1328 manipulation or deletion.
- 1329 ○ To establish timely availability of the meter data to the clients for direct scheduled
- 1330 and non-scheduled reads.

1331 **A.7.3. Utility Model**

1332 The utility model describes interactions between the Utility stakeholder and the AMI system in
1333 order to describe the security treatments that need to be applied.

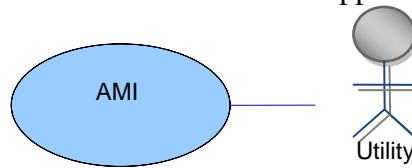


Figure 7 - Utility Model

1334
1335 Utility stakeholder security concerns about AMI:

- 1336 • Loss of competitive advantage
- 1337 • Loss of billing integrity
- 1338 • Service degraded
- 1339 • Increased cost
- 1340 • Regulatory compliance

1341 The following are use cases describing the relationships between the Utility and AMI.

1342 **Remote Meter Reads**

- 1343 • The AMI system permits the utility to remotely read meter data in intervals so that
1344 customers may be billed on their time of use, and demand can therefore be shifted from
1345 peak periods to off-peak periods, improving energy efficiency.

1346 **Security Objective:**

- 1347 ○ To maintain privacy of customer information in transit and within temporary and
1348 permanent memory storage.
- 1349 ○ To protect meter data from manipulation or deletion.
- 1350 ○ To provide timely availability of meter data.

1351 **Remote Connect / Disconnect**

- 1352 • The AMI system permits customers' electrical service to be remotely connected or
1353 disconnected for a variety of reasons, eliminating the need for utility personnel to visit
1354 the customer premises.

1355 **Security Objective:**

- 1356 ○ To protect integrity of connect/disconnect control messages; avoiding fake
1357 messages, fake senders, unintended receivers, manipulated messages
- 1358 ○ To establish a secure connection in transporting connect/disconnect control
1359 messages
- 1360 ○ To establish timely connectivity to connect/disconnect service

- 1361 • It should also provide an efficient way in which to initiate/terminate a service agreement
1362 between customer and utility via remote switching service(on/off)

1363 **Security Objective:**

- 1364 ○ To establish timely connectivity to connect/disconnect service

- 1365 • Posses the ability to remotely limit customer usage as a response to constrained supply as
1366 well as the customer’s inability to pay the cost for the service

1367 **Security Objective:**

- 1368 ○ To protect integrity of connect/disconnect/limit control messages; avoiding fake
1369 messages, fake senders, unintended receivers, manipulated messages

- 1370 ○ To establish a secure connection in transporting connect/disconnect/limit control
1371 messages

- 1372 • In addition to the aforementioned the following business transactions should also be
1373 made available to the customer and utility:

- 1374 ○ Routine shut-off of service (move out)
1375 ○ Routine turn-on of service (move in)
1376 ○ Credit & Collections termination of service
1377 ○ Local/on site shut-off of service
1378 ○ Local/on site turn-on of service
1379 ○ Credit and Collection Service Limiting

1380 **Security Objective:**

- 1381 ○ To establish timely connectivity to connect/disconnect/limit service
1382 ○ To produce historical, non-reputable record of event

1383 **Energy Theft**

- 1384 • The AMI system can be used to report when customers are stealing energy or tampering
1385 with their meter.

1386 **Security Objective:**

- 1387 ○ To produce reliable tamper indication
1388 ○ To successfully transmit and receive a tamper signal
1389 ○ To securely transmit tamper signal from a non-reputable source

1390 **Outage Management**

- 1391 • The AMI system can be used to report outages with greater precision than other sources,
1392 or verify outage reports from other sources.

1393 **Security Objective:**

1394 **Power Quality Analysis**

- 1395 • The AMI system can be used to analyze the quality of electrical power by reporting
1396 harmonic data, RMS variations, Voltage and VARs, and can communicate directly with
1397 distribution automation networks to improve power quality and fault recovery times.

1398 **Security Objective:**

- 1399 ○ To maintain integrity of meter data sent; avoid manipulation and deletion
1400 ○ To security meter data being transmitted; avoid customer's private data being
1401 released or intercepted
1402 ○ To maintain availability of quality analysis information

1403 **Distributed Generation Management**

- 1404 • The AMI system can be used to dispatch, measure, regulate and detect distributed
1405 generation by customers.

1406 **Security Objective:**

- 1407 ○ To maintain integrity of AMI data being transmitted and stored to avoid
1408 manipulation and deletion
1409 ○ To provide timely availability to system data
- 1410 • Additional benefits include, but are not limited, to the following:
- 1411 ○ An increase in customer's willingness to participate in a load management
1412 program with the utilities
1413 ○ Provides a channel of communication from utility to load management devices
1414 ○ Reduction in the costs associated with the installation of AMI system components
1415 which would enable customer-provided distributed generation (this could increase
1416 customer's willingness to participate as well since there wouldn't be any out of
1417 pocket costs for the customer)
1418 ○ Creates an avenue for the utilities to dispatch and monitor those participants in
1419 distributed generation

1420 **Security Objective:**

- 1421 ○ To protect confidentiality of customer's data and maintain customer trust

1422 **Optimizing Lifetime of Network**

- 1423 • With the advent of new communications, in particular: wireless communication systems,
1424 PLC, and BPL, AMI devices would have the ability to interact with the critical physical
1425 infrastructure (e.g. IED's such as CBC (Capacitor Bank Controller) systems in order to
1426 improve: circuit efficiency, loss reduction, and energy savings). This will help optimize
1427 the lifetime of the physical infrastructure. (Ref: Distribution Use Case 2)

1428 **Security Objective:**

- 1429 ○ To protect integrity of data stored and in transit between AMI/Smart Grid devices

- 1430 ○ To provide AMI/Smart Grid device information in a timely manner
- 1431 ○ To protect AMI/Smart Grid communications from manipulation, deletion and
- 1432 interception

1433 **Management of the End-to-End Lifecycle of the Metering System**

- 1434 ● An important requirement of such an AMI system would be the ability of the system to
- 1435 diagnose itself. The system should be able to: collect information about the status/health
- 1436 of certain devices, conduct remote diagnostics, and optimize operating parameters
- 1437 remotely.

1438 **Security Objective:**

- 1439 ○ To protect diagnostic data from being manipulated, deleted or masqueraded
- 1440 ○ To validate the authenticity of the diagnostic messages being transmitted
- 1441 ○ To provide timely availability to diagnostic data
- 1442 ○ To secure diagnostic data from eavesdropping or capture

1443 **AMI system adaptability**

- 1444 ● The system should be able to adapt to anticipated changes that may or may not occur
- 1445 such as:
 - 1446 ○ New physical communications methods
 - 1447 ○ New features available from equipment vendors
 - 1448 ○ New tariffs possibly with certain restrictions (e.g. number of rates or time)
 - 1449 ○ Connections to new types of load control equipment
 - 1450 ○ New communications protocols
 - 1451 ○ Changes to operating parameters
 - 1452 ○ New computing applications

1453 **Security Objective:**

- 1454 ● The aforementioned should be accomplishable with minimal incremental cost in stark
- 1455 contrast to a wholesale system replacement

1456 **Security Objective:**

- 1457 ○ Objectives to be determined and prioritized based on technology implemented

1458 **Prepay**

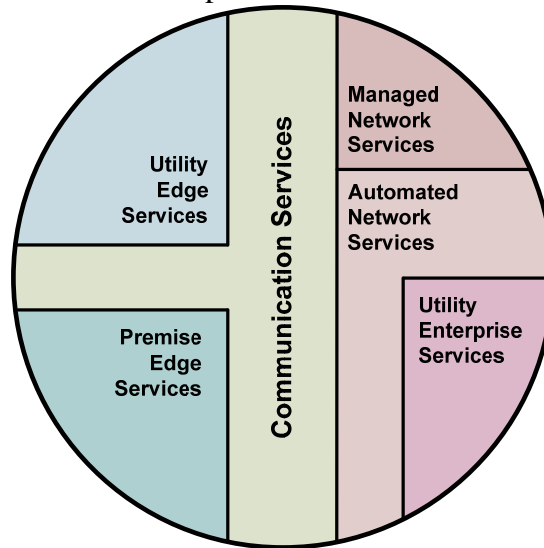
- 1459 ● Utilities use the AMI system to enforce disconnection when the prepayment balance
- 1460 reaches zero.

1461 **Security Objective:**

- 1462 ○ To provide confidentiality to customer payment and associated information; avoid
- 1463 eavesdropping, interception or collection of customer data stored (temporary or
- 1464 permanent) or in transit
- 1465 ○ To provide integrity of data being transmitted including non-repudiation and
- 1466 validation of customer information transmitted
- 1467 ○ To provide the customer availability to their respective account(s) within
- 1468 customer payment services

1469 A.8 Security Domains View

1470 This section describes the internal use cases; cases where activity is stimulated from entirely
 1471 within AMI itself. Examples are automation and intelligent responses. The following diagram
 1472 describes the internal services provided by AMI. Assumption is made that measurement,
 1473 monitoring, and application control encompass all services.



1474 **Figure 8 - AMI Service Domains**

1475 **Legend:**

- 1477 • **Utility Edge Services** – All field services applications including monitoring,
- 1478 measurement and control controlled by the Utility
- 1479 • **Premise Edge Services** – All field services applications including monitoring,
- 1480 measurement and control controlled by the Customer (Customer has control to delegate
- 1481 to third party)
- 1482 • **Communications Services** – are applications that relay, route, and field aggregation,
- 1483 field communication aggregation, field communication distribution information.
- 1484 • **Management Services** – attended support services for automated and communication
- 1485 services (includes device management)
- 1486 • **Automated Services** – unattended collection, transmission of data and performs the
- 1487 necessary translation, transformation, response, and data staging
- 1488 • **Business Services** – core business applications (includes asset management)

1489 Stakeholders:

- 1490 • Customer Users of the system
- 1491 • Operators of the system
- 1492 • Responsible Entities of the systems
- 1493 • Implementers of the system
- 1494 • Maintainers of the system

1495 Concerns:

- 1496 How is integrity maintained for processes?
- 1497 How is integrity maintained for data?
- 1498 How is confidentiality of customer data maintained (e.g. customer usage)?
- 1499 How is availability to utility assets maintained?

1500 Viewpoint language:

- 1501 Use Cases (Misuse Cases)
- 1502 Note: Potentially move down from business functions.

1503 Analytic Methods:

- 1504 Penetration Testing
- 1505 Auditing

1506 Rationale:

- 1507 This viewpoint was selected because it shows the relationship between AMI services
- 1508 requiring security measures. Drivers for this viewpoint include control, ownership,
- 1509 environmental, and functionality (capability) concerns.

1510 **A.8.1. Utility Edge Services Domain**

1511 Summary

- 1512 The Utility Edge Services Domain allows the utility to interact with non-customer-owned
- 1513 edge assets, such a meter (electric, gas, or water) or other end-point device.

1514 Assumptions

- 1515 The Utility Edge Services Domain assumes a singular service endpoint (point of service).

1516 Ownership and Control Concerns

- 1517 The utility owns at least some of the assets within the Utility Edge Services Domain. Any
- 1518 asset not owned by the utility in question is owned by a peer entity, such as another
- 1519 utility.
- 1520 The utility controls all assets within the Utility Edge Services Domain. Assets owned by
- 1521 another entity are controlled by the utility as a proxy for the owner.

1522 **A.8.2 Premise Edge Services Domain**

1523 Summary

- 1524 The Premise Edge Services Domain allows the utility to interact with customer-owned
- 1525 edge assets, such as Home Area Network (HAN) devices.

1526 Assumptions

- 1527 The Premise Edge Services Domain assumes a singular customer.

1528 Ownership and Control Concerns

1529 The utility may own the assets within the Premise Edge Services Domain. Alternatively,
1530 assets in the Premise Edge Services Domain may be owned by the Customer or a Third
1531 Party Service Provider.
1532 The utility controls all assets within the Premise Edge Services Domain. Control of assets
1533 owned by another entity is delegated to the utility as part of admission to the Premise
1534 Edge Services Domain.

1535 **A.8.3. Communication Services Domain**

1536 Summary

1537 The Communication Services Domain facilitates communication between assets in
1538 adjacent service domains (Utility Edge, Premise Edge, Managed Network, and
1539 Automated Network) and may facilitate communication between assets within the same
1540 domain.

1541 Assumptions

1542 The Communication Services Domain assumes interfaces to multiple Utility Edge and
1543 Premise Edge Services Domains, and may include interfaces to multiple Managed
1544 Network and Automated Network Services Domains.

1545 Ownership and Control Concerns

1546 The utility may own the assets within the Communication Services Domain.
1547 Alternatively, assets in the Communication Services Domain may be owned by a
1548 Communication Services Provider.
1549 The utility may control assets within the Communication Services Domain. Alternatively,
1550 assets in the Communication Services Domain may be controlled by a Communication
1551 Services Provider. Assets controlled by a Communication Services Provider may be
1552 included in a contractual services agreement with the utility.

1553 **A.8.4. Managed Network Services Domain**

1554 Summary

1555 The Managed Network Services Domain allows the utility to manage communication
1556 configuration, settings, capabilities, and resources in each of the other service domains.

1557 Assumptions

1558 The utility primarily uses assets in the Managed Network Services Domain to manipulate
1559 configurations and settings in the Automated Network Services Domain (i.e., human
1560 interface).

1561 Ownership and Control Concerns

1562 The utility may own the assets within the Managed Network Services Domain.
1563 Alternatively, assets in the Managed Network Services Domain may be owned by a
1564 Communication Services Provider.
1565 The utility controls all assets within the Managed Network Services Domain. Control of
1566 assets owned by another entity is delegated to the utility as part of admission to the
1567 Managed Network Services Domain.

1568 **A.8.5. Automated Network Services Domain**

1569 Summary

1570 The Automated Network Services Domain allows the utility to implement the
1571 communication parameters specified using assets in the Managed Network Services
1572 Domain.

1573 **Assumptions**

1574 The utility primarily uses assets in the Automated Network Services Domain to perform
1575 routine and/or repetitive operations at high speed without manual intervention.

1576 **Ownership and Control Concerns**

1577 The utility may own the assets within the Automated Network Services Domain.

1578 Alternatively, assets in the Automated Network Services Domain may be owned by a
1579 Communication Services Provider.

1580 The utility controls all assets within the Automated Network Services Domain. Control of
1581 assets owned by another entity is delegated to the utility as part of admission to the
1582 Automated Network Services Domain.

1583 ***A.8.6. Utility Enterprise Services Domain***

1584 **Summary**

1585 The Utility Enterprise Services Domain allows the utility to perform the business
1586 functions required by enterprise applications.

1587 **Assumptions**

1588 The assets in the Utility Enterprise Services Domain provide the interface to AMI
1589 systems and data for the remainder of the enterprise.

1590 **Ownership and Control Concerns**

1591 The utility owns all assets within the Utility Enterprise Services Domain.

1592 The utility controls all assets within the Utility Enterprise Services Domain.

1593 **Appendix B – Supplemental Material: Business Functions as**
1594 **Stakeholders in AMI Systems**

1595 ***B.1 Introduction***

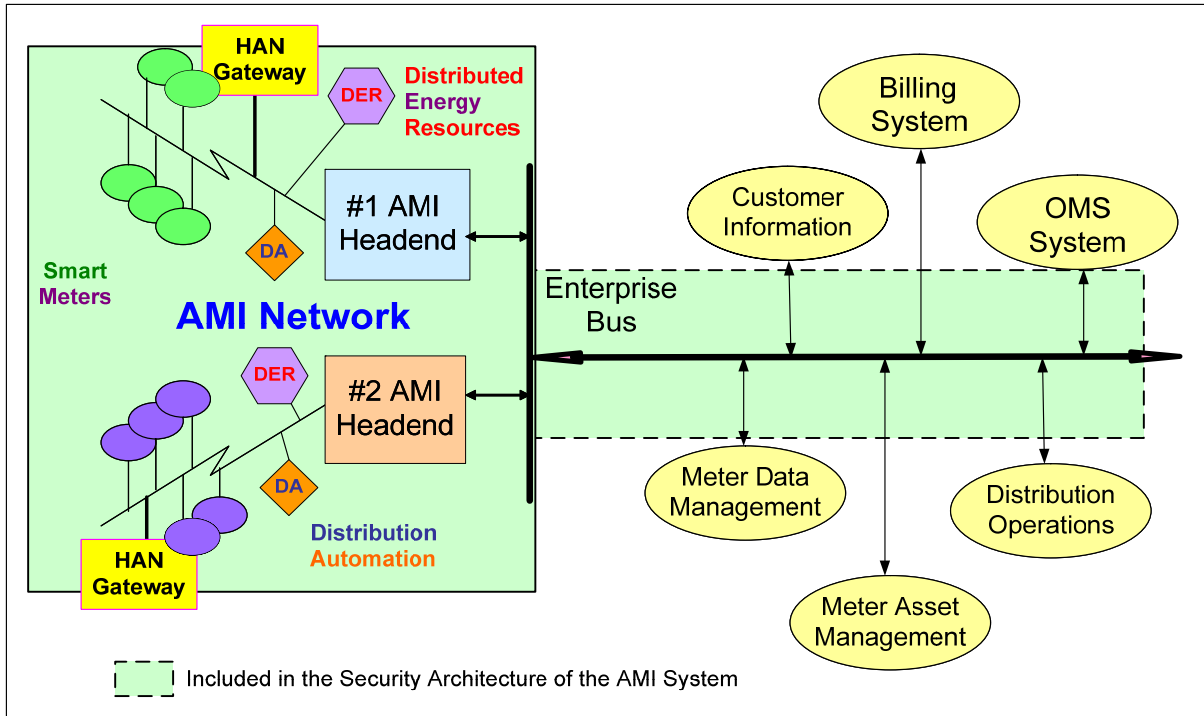
1596 The information provided in this appendix provides supplemental background material for
1597 understanding potential business functions within AMI systems. Some of the business functions
1598 provide a forward-looking perspective into AMI systems. This information may be used in the
1599 development of a utility’s specific use cases, but the information in this section is not intended to
1600 be regarded as security requirements for AMI.

1601 **B.1.2 Scope of AMI Systems**

1602 As Smart Grid requirements drive the development new technologies and the deployment of new
1603 systems, more and more new and existing Business Functions are becoming stakeholders in these
1604 new systems. Advanced Metering Infrastructure (AMI) systems are prime examples of these new
1605 technologies: they clearly can provide Smart Grid benefits. However, AMI systems are still a
1606 work in process, which can clearly benefit some business functions, but which appear potentially
1607 useful for others while not yet obviously beneficial. In addition, there will inevitably be business
1608 functions which are not yet foreseen that will suddenly become viable.

1609
1610 AMI systems consist of the hardware, software and associated system and data management
1611 applications that create a communications network between end systems at customer premises
1612 (including meters, gateways, and other equipment) and diverse business and operational systems
1613 of utilities and third parties. AMI systems provide the technology to allow the exchange of
1614 information between customer end systems and those other utility and third party systems. In
1615 order to protect this critical infrastructure, end-to-end security must be provided across the AMI
1616 systems, encompassing the customer end systems as well as the utility and third party systems
1617 which are interfaced to the AMI systems (see Figure 1).

1618



1619
1620

Figure 9 - Scope of AMI Systems

1621 **B.2 Overview of Business Functions Utilizing AMI Systems**

1622 Identifying and describing Business Functions are the most effective methods for understanding
1623 the information exchange requirements. The range of Business Functions utilizing the AMI
1624 systems is shown in Figure 2.
1625

Business Processes Utilizing the AMI/Enterprise Bus Interface

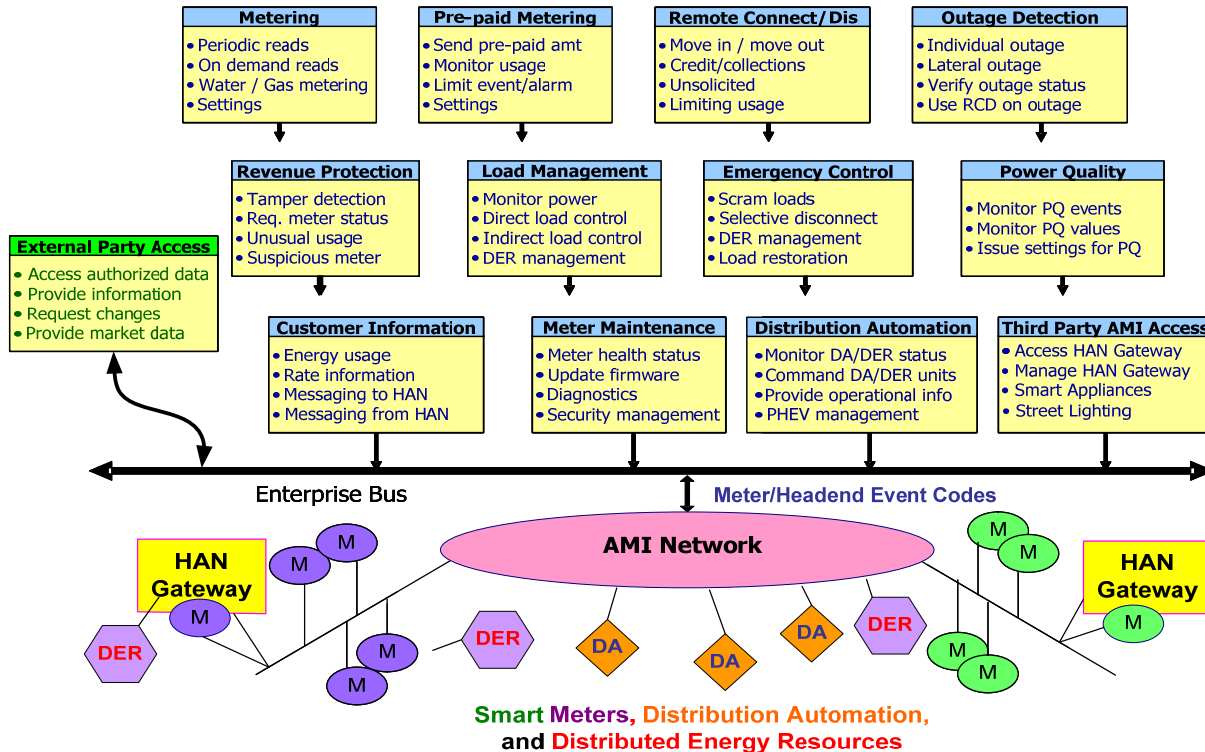


Figure 10 - Business Functions Utilizing the AMI/Enterprise Bus Interface

1626
1627
1628
1629

The following sections expand on these Business Functions.

1630 B.3 AMI Metering Business Functions

1631 B.3.1 Metering Services

1632 Metering services provide the basic meter reading capabilities for generating customer bills.
1633 Different types of metering services are usually provided, depending upon the type of customer
1634 (residential, smaller commercial, larger commercial, smaller industrial, larger industrial) and
1635 upon the applicable customer tariff.

1636 B.3.1.1 Periodic Meter Reading

1637 Traditionally for residential customers and the smaller C&I customers, periodic meter reading
1638 services are performed monthly via a meter reader, possibly using handheld or mobile meter
1639 reading tools. It takes the current index reading from the meter and records it for billing and
1640 other purposes. For Time-of-Use (TOU) data from net metering or other TOU meters, intervals
1641 can be established such as “on-peak” and “off-peak”, as defined in the utility’s tariffs. In some
1642 utilities or under certain circumstances, actual meter reading is done less frequently, and bills
1643 rely on meter reading estimates which are “trued up” later.

1644

1645 In AMI systems, periodic meter reading will retrieve interval data (usually hourly data but
1646 possibly 15-minute or 5-minute data). The frequency of retrieving the data from the meter can
1647 vary from every 5 minutes, to hourly, to daily, and to monthly.

1648
1649 Among the benefits of AMI for periodic meter readings are the increased accuracy (fewer
1650 estimated reads, more exact reading dates/times), and the availability of the to-date meter
1651 readings during the billing cycle.

1652 **B.3.1.2 On-Demand Meter Reading**

1653 Traditionally, on-demand meter reading is performed by sending a meter reader to the meter site
1654 around the time requested for the meter reading. Typically reasons for on-demand meter readings
1655 include:

- 1656 • Move in / move out
- 1657 • Limited usage tariffs
- 1658 • Billing questions by the customer
- 1659 • Revenue protection concerns

1660
1661 AMI systems will permit on-demand reads to take place almost immediately or more precisely at
1662 the scheduled date and time.

1663 **B.3.1.3 Net Metering for DER**

1664 When customers have the ability to generate or store power as well as consume power, net
1665 metering is installed to measure not only the flow of power in each direction, but also when the
1666 net power flows occurred. Often Time of Use (TOU) tariffs are employed.

1667
1668 Today larger C&I customers and an increasing number of residential and smaller C&I customers
1669 have net metering installed for their photovoltaic systems, wind turbines, combined heat and
1670 power (CHP), and other DER devices. As plug-in hybrid electric vehicles (PHEVs) become
1671 available, net metering will increasingly be implemented in homes and small businesses, even
1672 parking lots.

1673
1674 AMI systems can facilitate the management of net metering, particularly if pricing becomes
1675 more dynamic and/or more fine-grained than currently used for TOU rates.

1676 **B.3.1.4 Bill - Paycheck Matching**

1677 Today, depending on the utility bills arrive monthly, quarterly or yearly and not on a schedule
1678 selected by the customer, rather they are based on a schedule that matches the meter reading
1679 schedules. Small scale trials have proven that for customers who are living on the margin and
1680 miss occasional payments, that matching the date and frequency of the customer's paycheck
1681 reduces the number of late or missing payments significantly, cutting collection costs and
1682 reducing the cost to all customers.

1683
1684 AMI systems provide the flexibility to provide customers with bills when the customers prefer to
1685 receive them.

1686 **B.3.2 Pre-Paid Metering**

1687 **B.3.2.1 Prepayment Tariffs**

1688 Customers who either want a lower rate or have a history of slow payment can benefit from
1689 prepayment of power. Smart metering makes it easier to deploy new types of prepayment to
1690 customers and provide them with better visibility on the remaining hours of power, as well as
1691 extending time of use rates to prepayment customers.

1692
1693 AMI systems can also trigger notifications when the pre-payment limits are close to being
1694 reached and/or have been exceeded.

1695 **B.3.2.2 Limited Energy Usage**

1696 Traditionally, customers who use pre-payment tariffs need to go through the utility customer
1697 representatives to learn about their current usage or to extend their energy limits. With AMI
1698 systems, customers can see their current usage and limits, and may be able to automatically
1699 extend their limits electronically (e.g. pay over the Internet with the AMI system then updating
1700 their energy limits).

1701 **B.3.2.3 Limited Demand**

1702 Customers can also have tariffs that limit demand. Some C&I customers have rates that
1703 depended on the peak 15-minute demand. Some other customers actually have current limiting
1704 equipment to ensure limited demand.

1705
1706 AMI systems can provide the customer with the information necessary to manage their demand
1707 limits more precisely and effectively.

1708 **B.3.3 Revenue Protection**

1709 **B.3.3.1 Tamper Detection**

1710 Non-technical losses (or theft of power by another name) has long been an on-going battle
1711 between utilities and certain customers. In a traditional meter, when the meter reader arrives,
1712 they can look for visual signs of tampering, such as broken seals and meters plugged in upside
1713 down. During the analysis of the data, tampering that is not visually obvious may be detected,
1714 such as anomalous low usage.

1715
1716 With AMI systems, smart meters can immediately issue “tampering” alarms that are set off by a
1717 number of different sensors and routines in the meter. These tampering actions can include meter
1718 removal, tilt, and unauthorized access attempts (smart meters cannot be plugged in upside down).

1719 **B.3.3.2 Anomalous Readings**

1720 Some anomalous readings in the meter can trigger warning events which can be immediately
1721 investigated to determine if they are legitimate (people are on vacation or the factory has shut
1722 down an assembly line) or if they are due to tampering, such as wiring around the meter.

1723 **B.3.3.3 Meter Status**

1724 Some theft of power has occurred by the bypassing of the meter for a few days between
1725 scheduled readings by a meter reader. AMI systems will permit the status of meters to be verified
1726 at any time during the reading cycle.

1727 **B.3.3.4 Suspicious Meter**

1728 Some theft of power has occurred by the replacement of a certified meter with a “slow run”
1729 meter. AMI systems with smart meters will have each meter “registered” with an identity that
1730 cannot be tampered with without showing evidence of that tampering.

1731 **B.3.4 Remote Connect / Disconnect**

1732 **B.3.4.1 Remote Connect for Move-In**

1733 The customer initiates a request to move into a location that has electric service but is currently
1734 disconnected at the meter. The request can be for immediate action or for a connection at a
1735 specific date and time.

1736 Traditionally, utilities send a metering service person to connect the meter. With an AMI system,
1737 the connection can be performed remotely by closing the remote connect/disconnect (RCD)
1738 switch, using the following steps:

- 1739 • At the appropriate date and time, read the meter to get the latest reading and to verify that
1740 the meter is functional.
- 1741 • Determine there is no backfeed current detected by the meter
- 1742 • Issue the connect command to the meter
- 1743 • Verify that the meter is connected

1744 **B.3.4.2 Remote Connect for Reinstatement on Payment**

1745 Once a customer pays who was disconnected due to non-payment (or works out some mutually
1746 accepted agreements), the meter needs to be reconnected by closing the remote
1747 connect/disconnect (RCD) switch. The same process as for a move-in would be used.

1748 **B.3.4.3 Remote Disconnect for Move-Out**

1749 Traditionally, move-outs are handled by performing a special meter read (“soft” disconnect)
1750 around the time of the move-out. Since the power is not actually disconnected, this method can
1751 lead to illegal use of power after the move-out and before the next move-in.

1752 With an AMI system, a move-out can have a “hard” disconnect that opens the RCD switch,
1753 typically using the following steps:

- 1754 • Verify that the meter can be disconnected remotely
- 1755 • Issue the disconnect command at the appropriate date and time
- 1756 • Verify that the meter is disconnected
- 1757 • Read the meter for the final billing.

1758 In conjunction with the next meter reading during a move-in connection, any delta between the
1759 readings can be detected as a possible tampering or illegal usage of power.

1760 **B.3.4.4 Remote Disconnect for Non-Payment**

1761 The cost of collections is high, typically higher yet is the cost of disconnecting a customer – not
1762 only the lost revenue, but the cost of two special trips to the location, one to turn the power off
1763 and eventually another to turn it back on again. While remote disconnects are still pricy today,
1764 they offer a much lower cost for turning the power off and once customers understand that a
1765 disconnect can be done immediately, collections costs also seem to decline.

1766 **B.3.4.5 Remote Disconnect for Emergency Load Control**

1767 Some customers could get special rates if they agree to the temporary suspension of electric
1768 service in support emergency load shed activities. This is an alternative to wide-scale rolling
1769 blackouts and circuit level interruptions. Customers who choose to participate in such a program
1770 are eligible to have their power cut during the critical periods.

1771
1772 This type of selective black-out provides the means for reducing power demands on the overall
1773 grid while selectively maintaining service to critical customers such as public infrastructure (i.e.
1774 traffic lights) and medical facilities.

1775 **B.3.4.6 Unsolicited Connect / Disconnect Event**

1776 Unsolicited connect/disconnect events can be caused by a number of activities, covered in the
1777 following Business Functions:

- 1778 • Meter manually switched off by utility employee, including both valid and invalid
1779 switching
- 1780 • Meter manually switched off by unknown party, including both valid and invalid
1781 switching
- 1782 • Software/hardware failure switches meter off/on (also includes unauthorized command
1783 causing switch)
- 1784 • Miscellaneous event causes meter to switch off/on
- 1785 • Meter manually switched on by utility employee, including both valid and invalid
1786 switching
- 1787 • Meter manually switched on by unknown party, including both valid and invalid
1788 switching

1789 **B.3.5 Meter Maintenance**

1790 **B.3.5.1 Connectivity Validation**

1791 Determination that the customer is connected to the grid and even with the right signally which
1792 phase and circuit they are on. In several reviews of customer connectivity today for utilities the
1793 phase information is missing from many single phase connections and in some cases the circuit
1794 information is missing or wrong. Validation helps with making sure the data analysis is correct
1795 for engineering studies and other purposes.

1796 **B.3.5.2 Geo-Location**

1797 In asset data bases today many meters are literally miles (kilometers) from their physical location
1798 in the real world. During the installation of the meters GPS or other geo-location techniques can
1799 be used to provide accurate information on the meter’s location. If the location of the meter

1800 accidentally is changed in the database it is possible to flag the problem. This is possible since the
1801 location of the circuit is known, helping to eliminate problems that creep in over the long life of
1802 electric (gas and water) networks.

1803 **B.3.5.3 Battery Management**

1804 If there were no smart meters, there would be no need to do battery management, so the benefit
1805 only works for smart meter equipped networks. In an operational world the meters communicate
1806 more, running the battery down faster. It is important to have good battery management or the
1807 cost of maintaining the system will skyrocket. Remote battery monitoring (as part of the regular
1808 communications) can help deal with battery replacement planning and battery life extension.

1809 ***B.4 Distribution Operations Business Functions***

1810 **B.4.1 Distribution Automation (DA)**

1811 **B.4.1.1 DA Equipment Monitoring and Control**

1812 Some utilities are planning to use the AMI system for distribution automation, as a minimum for
1813 direct monitoring and more sophisticated control of capacitor banks and voltage regulators on
1814 feeders, rather than relying on local actions triggered by time, current, or voltage levels. Others
1815 also would like to monitor and control automated switches and fault indicators if the AMI
1816 network were able to stay alive during grid power outages, presumably via battery backup for
1817 critical nodes.

1818 **B.4.1.2 Use of Smart Meters for Power System Information**

1819 If more sensors were available in the distribution network, it would be possible to do distribution
1820 SCADA, with the deployment of smart meters and a near real-time communications network, it
1821 is possible to pick a sub-set of the smart meters and use them as bell weather devices in the grid
1822 to provide a distribution SCADA like capability. In addition some utilities are installing smart
1823 meters in place of RTUs for extending their current SCADA system further into the grid.

1824 **B.4.1.3 Power System Security/Reliability**

1825 As interference with the operation of the distribution grid becomes more common, it becomes
1826 more and more important to monitor the integrity of the grid at all times. Smart meters offer a
1827 way to get a “heart beat” from the whole of the distribution system on a regular basis thus
1828 providing assurance that the grid is intact. That it has not been attacked by a mad man in a
1829 backhoe or a copper thief with a chainsaw.

1830 **B.4.1.4 Power System Protection**

1831 Overloads on the system once were not a big issue devices could operate at two or even three
1832 times their rated capacity for several hours on a peak day. Today devices have been engineered
1833 to run at loads much closer to their ratings, and overloads of several hours can cause degradation
1834 in the devices. By being able to monitor the load on the device and with the deployment of direct
1835 load control or disconnect switches, the load on the device can be managed until it can be
1836 replaced or upgraded, the same goes for other physical assets that may be de-rated, allowing at
1837 least some of the lights to stay on.

1838 **B.4.1.5 Site/Line Status**

1839 Tag out procedures are supposed to render a segment of the network dead and safe to work on,
1840 unfortunately with the addition of true distributed generation, it is possible to have an islanding
1841 failure and to have a line that the crew expects to be ready for work, to actually still be live. With
1842 the correct smart metering system and the right connectivity mapping, it is possible to use the
1843 smart meters to determine if any power is still flowing through the lines. With the potential for
1844 the sales of plug-in hybrids to ramp up quickly in the next decade and the lack of protection
1845 schemes currently this may become an even larger issue.

1846 **B.4.1.6 Automation of Emergency Response**

1847 Today in a fire, the fire department normally handles the disconnection of the power and other
1848 utilities from the involved structures. Often with a fire axe! With the advent of remote
1849 disconnects in the meters it will be possible to cut the power to the structure, as well as gas and
1850 other utilities. This makes it easier to restore service after small problems and to more rapidly
1851 remove a possible source of problems from the structure.

1852 **B.4.1.7 Dynamic Rating of Feeders**

1853 Operators can dynamically rate feeders based on the more accurate power system information
1854 retrieved via the AMI system from strategic locations. This permits the operators to decide when
1855 they can run feeders beyond their ostensible ratings or when to perform multi-level feeder
1856 reconfigurations to balance the loads and avoid overloads.

1857 **B.4.2 Outage Detection and Restoration**

1858 **B.4.2.1 Outage Detection**

1859 Today the majority of real time information about a customer, comes from the customer, they
1860 pick up the phone and call about issues they have, such as an outage, and provide information to
1861 the utility. In the future, the smart meter will be able to provide up to date information about the
1862 customer and the status of their service.

1863 **B.4.2.2 Scheduled Outage Notification**

1864 For either scheduled outages for maintenance or for notification of a customer that the power is
1865 out in their home when they are at work or away from home, smart metering provides a needed
1866 piece. For scheduled outages, if there are in home displays deployed the metering system can
1867 provide the outage times and durations to the customers directly impacted and no others. This
1868 minimizes possible security issues of the information getting into the wrong hands as security
1869 systems that require power stop functioning, etc. It also helps with the number of phone calls that
1870 have to be placed to customers to let them know that maintenance is happening. With the
1871 connectivity verification, it is possible to really know who is on a specific path and to accurately
1872 manage the outage. For unscheduled outages, it possible to use the information coming from the
1873 meters to let customers know that they will be returning to a location with no power (water, gas)
1874 and that will let them make alternate plans, rather than walking into a surprise.

1875 **B.4.2.3 Street Lighting Outage Detection**

1876 Street lighting can be critical to safety and crime-prevention, and yet monitoring which street
1877 lights are out is currently performed haphazardly by civil servants and concerned citizens. AMI
1878 systems could be used to monitor these lights.

1879 **B.4.2.4 Outage Restoration Verification**

1880 Restoration verification has the metering system report in as the power it returned to the meters.
1881 This alert function is built into many meters that are being deployed as smart meters today and
1882 includes a timestamp for the restoration time. For some utilities this is improving their IEEE
1883 indices, since their crews may take several minutes to complete other actions before reporting the
1884 power back on. It can also be used to help isolate nested outages and help the field crews get to
1885 the root cause of those nested outages before they leave the scene.

1886 **B.4.2.5 Planned Outage Scheduling**

1887 Ideally, planned outages should be done at a time when they have the least impact on the
1888 customers. Today we use rules of thumb about when to take a planned outage, in the future with
1889 a complete data set it is possible to adjust the time of the outage to correspond with the lowest
1890 number of customers demanding power. This minimizes the impact to the customers.

1891 **B.4.2.6 Planned Outage Restoration Verification**

1892 In completing work orders, it is useful to know that all of the customers that were affected by the
1893 work order have power and that there are no outstanding issues that need to be corrected, prior to
1894 the crew leaving the area. The ability to “ping” every meter in the area that was affected by the
1895 work order and determine if there are any customers who are not communicating that they have
1896 power is useful to minimize return trips to the work area to restore single customers.

1897 **B.4.2.7 Calculation of IEEE Outage Indices**

1898 Today the IEEE indices are manually calculated in most utilities and they are not up to date,
1899 since the information needed to track them comes from field reports and other documents that do
1900 not feed into a central location. Additionally since not every single point is tracked in any system
1901 for outages, it is impossible to accurately determine the indices. Most utilities have gotten very
1902 good at the development of indices that are very close to the reality that their customers are
1903 seeing and to the limits of the information available.

1904 **B.4.2.8 Call Center Unloading**

1905 Today we rely on customers to call in when there is an outage; this normally is one of the factors
1906 in sizing call centers and staffing them. When smart metering is deployed in the right way, it is
1907 possible for the system to determine where the outages are and to let the utility call the customer
1908 with an outage message and an estimated time to repair. In the long run this will reduce the
1909 loading on the call center during periods of high outage levels.

1910 **B.4.3 Load Management**

1911 **B.4.3.1 Direct Load Control**

1912 Direct Load Control provides active control by the utility of customer appliances (e.g. cycling of
1913 air conditioner, water heaters, and pool pumps) and certain C&I customer systems (e.g. plenum
1914 pre-cooling, heat storage management). Direct load control is thus a callable and schedulable
1915 resource, and can be used in place of operational reserves in generation scheduling. Customer
1916 like it (if it is invisible), because they do not have to think about it, they sign up, allow the
1917 installation and forget it.

1918

1919 AMI systems will enhance the ability of utilities to include more customers in (appropriate)
1920 programs of direct load control, since it will increase the number of appliances accessible for
1921 participation in load control, and will improve the “near-real-time” monitoring of the results of
1922 the load control actions.

1923 **B.4.3.2 Demand Side Management**

1924 Management of the use of energy is important in a number of ways. Demand Side Management
1925 is a step beyond just tariff based load reduction. It assumes that customer will setup or allow to
1926 be set up equipment to reduce load when signals are sent to the customer’s location. The
1927 customer is in charge of making demand side management decisions.

1928 **B.4.3.3 Load Shift Scheduling**

1929 Given the ability to get customers to shift load when requested, and to do bottom up simulation it
1930 becomes possible to work with customers who have the ability to shift load to different times of
1931 the day or week. This ability to do load scheduling could have an impact on transmission and
1932 other capital expenses.

1933 **B.4.3.4 Curtailment Planning**

1934 To do proper load reduction, for either de-rated equipment or for planned outage or even to deal
1935 with load growth that has gotten ahead of system upgrades takes having data on what the loads
1936 are and what can be curtailed. In California, load curtailment has been called rolling blackouts,
1937 the best that can be done without an ability to control the demand on the system in a more
1938 granular fashion. By using curtailment planning, notice can be given in advance to the impacted
1939 customers and they have enough time to respond if they have an option in their contract to keep
1940 the power on.

1941 **B.4.3.5 Selective Load Management through Home Area Networks**

1942 With the deployment of home area networks the utility can choose to manage the load on the
1943 grid, to manage peak, to manage customer bills, to allow for a generation or transmission issue to
1944 be corrected or other reasons. This can permit, with the right equipment the reduction in the need
1945 for reserve margin in generation and for rolling reserve, the selective load management
1946 becoming a virtual power plant that is a callable and schedulable asset.

1947 **B.4.4 Power Quality Management**

1948 **B.4.4.1 Power Quality Monitoring**

1949 Today for some larger customers and at select locations on the grid we are able to monitor
1950 harmonics, wave form, phase angles and other power quality indicators. The need continues to
1951 grow as large screen televisions and other consumer electronics devices are increasingly adding
1952 harmonics to the system. With the newest metering technology some power quality monitoring is
1953 built into the meter and more is on the way. While not every house needs to monitor power
1954 quality, a percentage of the meters deployed should probably have this advanced capability.

1955 **B.4.4.2 Asset Load Monitoring**

1956 With Connectivity Verification and Geo-Location information it is possible to group the devices
1957 in a tree structure that correctly shows connection points in the grid. With the ability to read
1958 intervals from the meters it is then possible to build a picture of the load that each asset (e.g.
1959 transformers, conductors, etc.) are subjected to. This allows an operator to monitor heavily
1960 loaded assets and look for ways to off load some of the demand from that asset. It also allows a
1961 maintenance planner to prioritize what maintenance should be done to maximize the reliability of
1962 the grid, as part of a reliability centered maintenance program.

1963 **B.4.4.3 Phase Balancing**

1964 One of the least talked about issues with losses in the distribution grid today is single phase load
1965 and the imbalance it can cause between the phases. These losses have seldom been measured in
1966 the grid and little study has been done of the amount of phase imbalance on the grid today. In
1967 early studies the chronic phase imbalance in several circuits that were monitored averaged over
1968 10 percent. While correction is hard when the circuit is run as single phase laterals, in many
1969 cases there is enough load on the feeder portion of the circuit to allow rebalancing of the circuit
1970 to eliminate more than half of the chronic phase imbalance.

1971 **B.4.4.4 Load Balancing**

1972 Where there is an option to move a portion of the load from one circuit to another, the
1973 instrumentation is not always available to make good choices or to be able to forecast the load in
1974 a way that makes the movement pro-active instead of reactive. Automated feeder switches, and
1975 segmentation devices are becoming more and more common in the grid. The ability to use
1976 metering data to support the operation of these devices will only increase their value to the grid
1977 operator. Today with information only at the substation end of the circuit, it is tough to determine
1978 where on the circuit the load really is and where to position segmentation and when to activate a
1979 segmentation device when more than one is available. Operators today typically learn the right
1980 way by trial and error on the system.

1981 **B.4.5 Distributed Energy Resource (DER) Management**

1982 In the future, more and more of the resources on the grid will be connected to the distribution
1983 network and will complicate the operation of the grid for the future. Failure to integrate these
1984 resources into the grid and understand their impact will only degrade the operation of the grid
1985 and its reliability. It is no longer an option to deal with distributed resources, the time for

1986 refusing to allow them has passed. The only choice is to either embrace them and manage their
1987 impact or ignore them and suffer the consequences.

1988 **B.4.5.1 Direct Monitoring and Control of DER**

1989 Some DER units at customer sites could be monitored in “near-real-time” and possibly directly
1990 controlled by the utility or a third party (e.g. an aggregator) via the AMI system, in an equivalent
1991 manner to load control.

1992 **B.4.5.2 Shut-Down or Islanding Verification for DER**

1993 Each time an outage occurs that affect the power grid with DER, the DER should either shut
1994 down or island itself from the rest of the grid, only feeding the “microgrid” that is directly
1995 attached to. In many cases the shut-down or islanding equipment in smaller installations is
1996 poorly installed or poorly maintained. This leads to leakage of the power into the rest of the grid
1997 and potential problems for the field crews.

1998
1999 Each time an outage occurs, meters that are designed to monitor net power can tell if the
2000 islanding occurred correctly, if they are installed at the right point in the system. This reporting
2001 can minimize crew safety and allow the utility to let the customer know that maintenance is
2002 required on their DER system. In most cases when the islanding fails, other problems also exist
2003 that reduce the efficiency of the DER system, costing the customer the power that they expected
2004 to get from the system.

2005 **B.4.5.3 Plug-in Hybrid Vehicle (PHEV) Management**

2006 Depending on how plug-in hybrids are sold and how the consumers take to them, they may either
2007 become one of the largest new uses of power or they may not have an impact. A major problem
2008 is that planners are now assuming that they will be mobile generation plants, that the drivers will
2009 burn fuel and store power in the battery to be drawn during the peak times while parked in the
2010 company garage. Others have assumed that the cars will become the largest new consumer of
2011 power in the downtown grid, an overstressed part of the grid already.

2012
2013 How plug-ins are managed and how consumers will use them is a social experiment. What is not
2014 is that they will draw a large amount of power from somewhere and have the potential to store a
2015 lot of power for later use. How the power company measures which car provides or takes how
2016 many megawatt hours and proves it and bills for it, will be an interesting change. Smart meters
2017 can help with this if the right standards are place to deal with communication from the car to the
2018 meter.

2019 **B.4.5.4 Net and Gross DER Monitoring**

2020 There are two different generation results from distributed generation, the gross output of the
2021 device and the net input into the grid, after the owner takes their needed energy. The two can be
2022 very different at times when the DER is creating most power the owner may also be drawing so
2023 heavily that the net result to the grid is still negative. At other times, the demand from the owner
2024 may be less than the output, even though the output may be well under the design output of the
2025 device.

2026 Some utilities have decided to reward renewable generation owners on the gross output, while
2027 other utilities have decided to reward them on the net output, possibly with TOU rates. But to
2028 manage a utility and the reliability of the grid it is important to know both the net and the gross
2029 output of the device for simulation, load forecasting and for engineering design.

2030 **B.4.5.5 Storage Fill/Draw Management**

2031 If someone has installed distributed storage, when should it be topped off, and when should the
2032 storage discharge? Today's answer is to use a timer in most cases or a phone based trigger. For
2033 one utility the use of electric thermal storage for winter heat and time of use tariffs that
2034 encouraged topping up at a specific time of the day resulted in the destruction of a number of
2035 pieces of equipment on the grid as demand exceeded the local ability to supply that demand. The
2036 attempt to improve the load factor on the grid with this storage system resulted instead with
2037 demand that exceeded all expectations.

2038
2039 Smart metering with a home area network capability can trigger each storage device based on the
2040 total load in the area, leveling out the peaks in the system and providing better use of generation
2041 resources that may be variable in nature.

2042 **B.4.5.6 Supply Following Tariffs**

2043 DER has a strong probability of having a large percentage of renewable generation which has a
2044 strong variable component. Since the supply will be variable and highly variable on short notice,
2045 it may be that to avoid either a large component of rolling reserve that uses fossil fuels, it may be
2046 that a supply following tariff could be possible. It would require a very high speed forecasting
2047 system, excellent weather information and near real time communications to devices in the
2048 homes and in businesses with almost instant response. This is a tall order in today's world, but
2049 the cable companies have proven that millions of devices are possible to broadcast to in near
2050 real-time, so it is possible.

2051
2052 Smart meters on the right communications network and with the right in home gateway could
2053 provide a piece of this supply following tariff system.

2054 **B.4.5.7 Small Fossil Source Management**

2055 There is a large amount of diesel generation that is installed on customer sites to deal with
2056 outages on the grid. Some companies are now forming to manage these resources, not for outage,
2057 but for peak power production, bidding into the market a few megawatts at a time. While the use
2058 of these resources is a good thing, the penetration of private companies will never be as complete
2059 as if the utility were to work with their customers to equip most of this generation with controls
2060 and monitoring equipment.

2061
2062 Whether the utility operates and maintains these resources or allows third parties to take
2063 responsibility is not important. What is important is that smart metering can reduce the cost and
2064 complexity of making these resources available. In California more than 2,000 Megawatts of
2065 generation are already installed, more than enough to end most rolling blackouts (if the resources
2066 are in the right areas).

2067 **B.4.6 Distribution Planning**

2068 **B.4.6.1 Vegetation Management**

2069 Momentary outages normally increase as vegetation grows back in an area and starts to become
2070 potential issue for overhead lines. Smart metering allows the return of momentary outage
2071 information and allows the outage counts to be overlaid on a GIS system. This allows the
2072 planners to better target vegetation management people to the right locations. In the underground
2073 world, cable failures and splice failures can be found early, prior to a complete failure.

2074 **B.4.6.2 Regional and Local Load Forecasting**

2075 Given the ability to draw a full data set from the field, it is now possible to forecast regional and
2076 local loads and generation that can be used to prepare for and to set prices for both demand and
2077 supply.

2078 **B.4.6.3 Simulations of Responses to Pricing and Direct Control Actions**

2079 As more detailed information is available through AMI systems on regional and local loads and
2080 generation, it will be possible to assess the responses of both customers and the power system to
2081 price-related actions as well as direct control actions. This ability to simulate the market a day or
2082 more in advance should allow for better planning and for the system to run with smaller amounts
2083 of rolling reserve and ancillary services.

2084 **B.4.6.4 Asset Load Analysis**

2085 With the ability to have a real load history on a specific asset and to be able to do bottom up
2086 forecasting, the same can be done for assets in the connection tree. This should allow planners
2087 and others to see potential problem areas before they really exist.

2088 **B.4.6.5 Design Standards**

2089 Many of today's standards assume that complete data is not available so there are factors of
2090 safety built into the calculations at each step of the design process for the transmission and
2091 distribution grid to make sure that the design is useful for its full design life. The improvement in
2092 load and demand data from the smart meters will make it possible to remove many of the rules of
2093 thumb and design to the real needs of the customers.

2094 **B.4.6.6 Maintenance Standards**

2095 Maintenance is done with incomplete information. So the maintenance standards allow for this,
2096 in some cases too much maintenance is done and sometimes too little is done, standards call for
2097 the best possible maintenance planning that incomplete information can provide. The good news
2098 is that the reliability of the system is very high, better than any other service (including
2099 telecommunications and cable TV) that is available to a customer. The bad news is with all the
2100 retirements in the industry, the experienced technicians that are required to make the judgment
2101 calls in the field will all be replaced in a few years. Improving the standards for maintenance
2102 with better information will mean that the new field workers will be routed to the highest priority
2103 work almost every time.

2104 **B.4.6.7 Rebuild Cycle**

2105 When is the right time to rebuild a circuit and how much of it really needs to be upgraded?
2106 Today with the information we have, we hang some recorders and use a few weeks or months of
2107 data from a few locations to determine what to rebuild, with the improved data set and the
2108 improved standards it is possible to actually determine the sections of the grid to rebuild and how
2109 much to reinforce them.

2110 **B.4.6.8 Replacement Planning**

2111 Equipment replacement is based on the estimated load or a load study that is normally conducted
2112 with less than perfect information. This has resulted in the engineering team being conservative
2113 and over sizing many of the replacement equipment. Smart metering offers better information to
2114 make better sizing decisions.

2115 **B.4.7 Work Management**

2116 **B.4.7.1 Work Dispatch Improvement**

2117 Today we use manufacturers' recommendations, models, estimates, and visual inspection to
2118 determine when a lot of maintenance work should be done. While it works, in some utilities it
2119 means more maintenance than others think is required and in others it means less. In almost
2120 every case, some maintenance is performed that is not really required for reliability centered
2121 maintenance strategies. When smart metering information is available and used to do asset
2122 loading analysis and other data analysis, work can be more accurately dispatched to the crews in
2123 the field improving reliability in the system for the same number of jobs completed.

2124 **B.4.7.2 Order Completion Automation**

2125 Some utilities have the field crew log the completion of their job prior to packing up; others want
2126 the crew ready to roll prior to completion of the order. Some want the crews to look around
2127 before leaving, some want the crew to leave and let the customers call if there is still an issue in
2128 the area. With smart metering, as restoration alerts come in, it is possible to automate the time
2129 the job was completed and some of the closing paperwork, allowing the crew to stay in the field
2130 longer each day and to do less paperwork overall.

2131 **B.4.7.3 Field Worker Data Access**

2132 Today if a line worker wants to know the status of an area of the grid, she can measure power
2133 flow, she can look at meters or he can call dispatch. Access to near real time information on the
2134 status of the customers close to the worker's location is limited today. With the deployment of
2135 smart metering, depending on how the software is configured and the security setup, it may be
2136 possible for a field worker to get access to the a near real-time map of the status of the customers
2137 in their working area, minimizing the need for dispatch to tell the worker where to go next and
2138 what to do.

2139
2140 With experience, field workers have proven to be very good at determining where in their work
2141 area a likely root cause is, based on outage information, reducing the time it takes to find the
2142 cause and start the repair work.

2143 **B.4.7.4 Reliability Centered Maintenance (RCM) Planning**

2144 Today we guess at the loading on devices using models, and use that information to develop a
2145 reliability centered maintenance plan. Based on that information we do our best to perform the
2146 maintenance that the system requires to make sure that people have power. With the ability to do
2147 load monitoring and load forecasting more accurately, preseason maintenance can be scheduled
2148 based on the facts that the system generates. While it will never prevent all failures in the system,
2149 use of this information and a well designed RCM plan can result in significantly less outage for
2150 non-natural disaster causes.

2151 **B.5 Customer Interactions Business Functions**

2152 **B.5.1 Customer Services**

2153 **B.5.1.1 Remote Issue Validation**

2154 When a customer calls today with a problem, other than twenty questions on the phone or rolling
2155 a truck to the location, there is no way to understand if the customer really knows what the
2156 problem is or if they do not understand the problem. Use of near real time information from
2157 smart meters can allow the customer service representative (CSR) to provide better information
2158 to the customer and to provide better advice on what to do with the current situation. It can also
2159 reduce the dispatch of trucks for customer complaints. In general it reduces both call volume and
2160 call handling times.

2161 **B.5.1.2 Customer Dispute Management**

2162 The most frequent customer dispute is a high bill. They complain about the meter reading being
2163 wrong. In truth there are enough meter reading errors that high bills are a fact of life. But the
2164 ability to check the current meter reading directly from the meter while the customer is on the
2165 phone and re-calculate the bill if the bill was high, and to end the post call investigation, by being
2166 able to directly validate the customer dispute reduces the time to clear a complaint that is non-
2167 phone time and it reduces the call handling time of the life of the dispute. It is not unusual that
2168 the initial call time goes up, since the CSR has to explain how they are getting the information
2169 and may have to have the customer walk to the meter while on the phone and verify the numbers
2170 that show on the meter. This has reduced monthly disputes with chronic callers over a period of 3
2171 to 6 months in most utilities that have this ability.

2172 **B.5.1.3 Outbound Customer Issue Notification**

2173 Not only can customers be called at work for problems with outage, but other problems can be
2174 determined and customers notified, in one case, a meter looked like it had been tampered with,
2175 but the customer had a complaint about low voltage on file. A review of the situation determined
2176 that one of the wires was probably loose in the customer's breaker panel. That call resulted in the
2177 customer hiring an electrician and fixing a number of electrical problems in their home that the
2178 electrician uncovered while fixing the loose wire in the panel. This is one example of a number
2179 of proactive actions that can be taken with the customer to help them be safe and know what is
2180 going on with their energy consumption. Similar work was undertaken on behalf of a water
2181 company and a number of beyond the meter leaks were identified with night time readings on
2182 homes with high water bill complaints.

2183 **B.5.1.4 Customer Energy Advisory**

2184 Some utilities have undertaken to provide a customer energy consumption advisory that allowed
2185 customers to indicate what they have for energy consuming devices and information about their
2186 home. In return, the utilities rank their consumption against similar homes and provide feedback
2187 on the equipment and appliances that were consuming significant energy.

2188
2189 This advisory can even suggest what should be replaced and the payback period on the
2190 replacement, based on energy usage. The comparison allows customers to see how they did
2191 against similar customers and where they ranked in energy consumption. This has been very
2192 useful in getting customers to pay more attention to their consumption.

2193 **B.5.1.5 Customer Price Display**

2194 To make a realistic decision about using or not using energy and water, customers need to know
2195 how much it will cost. As we have seen with Gasoline the global consumption decreased very
2196 little (in reality only the projection of growth in consumption declined, not the actual usage)
2197 when the price tripled at the pump in many countries. Electricity, gas and water today are in the
2198 noise of running a household for most families and for many businesses the cost does not enter
2199 the top five costs for the business. To this end, making a decision to consume energy and water is
2200 easy.

2201
2202 For a few businesses and a small percentage of residential customers this is not true and they
2203 have strong motivation to conserve power. With critical peak pricing or time of use pricing and
2204 rising prices for energy and water, the percentage of the average family income consumed by
2205 these utilities will no longer be noise and having information about pricing, will drive some
2206 conservation. Expect that customers will need to know the price to wash a load of clothes, not
2207 the price of a kilowatt hour.

2208 **B.5.2 Tariffs and Pricing Schemes**

2209 **B.5.2.1 Tariff Design**

2210 Today a sample of the customers is used to determine what the customer profile should be and
2211 how that profile should be priced. In many cases the classification of the customers is very broad
2212 and does not really take into account the different ways that customers actually consume power.
2213 For example, a young educated single male living in an apartment may have a lower usage than
2214 the young family across the hallway and they may both pay the same per kilowatt-hour of power.

2215
2216 However, the young male many actually cost the utility more to serve, since the load factor for
2217 that single male may be much lower than the load factor for the young family. By being able to
2218 provide accurate data, better tariffs can be designed and better segmentation done to support a
2219 fair power price.

2220 **B.5.2.2 Rate Case Support**

2221 Today to get almost any change in what can be charged to the customers or what is placed in the
2222 rate base, it requires a rate case. In some rate cases the documents filed fill rooms and rooms in a
2223 building, mostly because the issues can be handled in a black and white manner. Experts are

2224 required to testify on many aspects of the rate case using data from other locations, since the
2225 complete data set to answer the question does not exist at the utility. While experts will not go
2226 away, and there will still be a lot of estimating, it is important to realize that smart meters
2227 provide a large data set to assist with the rate cases.

2228 **B.5.2.3 Tariff Assessments**

2229 Do critical peak tariffs create the response expected, does it do it for all segments of customers,
2230 and does it impact some customer segments more harshly than others. Use of smart meter data
2231 allows a better review of how the customers are responding to the tariffs and how to re-work
2232 them to better fit the needs of the society.

2233 **B.5.2.4 Cross Subsidization**

2234 An issue that is raised over and over again is cross subsidization of customers, one group of
2235 customers paying part of the cost of another group of customers. With our example in Tariff
2236 Design, more than likely the young family is subsidizing the young male. Regulators want to
2237 know what the cross subsidization is, they do not always want to eliminate it (e.g. the long
2238 distance rates for the telephone companies for decades financed the ability of everyone to have a
2239 phone). By having complete data on each and every customer, subsidization arguments no longer
2240 fall on “I think” arguments, but fall into the “I know” allowing the regulator to only have
2241 intended subsidies.

2242 **B.5.2.5 Customer Segmentation**

2243 Customer segmentation has traditionally been done by industry or by business segment or by
2244 customer type, not by the actual needs or profile of the customers. Regulators have never had
2245 enough data to make segmentation decisions that really classify customers together by the way
2246 they consume power and their needs for power quality or their creation of power quality issues
2247 that the utility needs to fix. Smart metering can provide the data to make meaningful
2248 segmentation decisions.

2249 **B.5.3 Demand Response**

2250 Demand response is a general capability that could be implemented in many different ways. The
2251 primary focus is to provide the customer with pricing information for current or future time
2252 periods so they may respond by modifying their demand. This may entail just decreasing load or
2253 may involve shifting load by increasing demand during lower priced time periods so that they
2254 can decrease demand during higher priced time periods. The pricing periods may be real-time
2255 based or may be tariff-based, while the prices may also be operationally-based or fixed or some
2256 combination. As noted below, real-time pricing inherently requires computer-based responses,
2257 while the fixed time-of-use pricing may be manually handled once the customer is aware of the
2258 time periods and the pricing.

2259
2260 Sub functions for demand response, which may or may not involve the AMI system directly,
2261 could include:

- 2262 • Enroll Customer
- 2263 • Enroll in Program
- 2264 • Enroll Device

- 2265 • Update Firmware in HAN Device
- 2266 • Send Pricing to device
- 2267 • Initiate Load Shedding event
- 2268 • Charge/Discharge PHEV – storage device
- 2269 • Commission HAN device
- 2270 • HAN Network attachment verification (e.g. which device belongs to which HAN)
- 2271 • Third Party enroll customer in program (similar to, but not the same as the customer enrolling directly)
- 2272 • Customer self-enrollment
- 2273 • Manage in home DG (e.g. MicroCHP)
- 2274 • Enroll building network (C&I – e.g. Modbus)
- 2275 • Decommission device
- 2276 • Update security keys
- 2277 • Validate device
- 2278 • Test operational status of device

2280 **B.5.3.1 Real Time Pricing (RTP)**

2281 Use of real time pricing for electricity is common for very large customers affording them an
 2282 ability to determine when to use power and minimize the costs of energy for their business, one
 2283 aluminum company cut the cost of power by more than 70% with real time pricing and flexible
 2284 scheduling. The extension of real time pricing to smaller customers and even residential
 2285 customers is possible with smart metering and in home displays. Most residential customers will
 2286 probably decline to participate individually because of the complexity of managing power
 2287 consumption, but may be quite willing to participate if they are part of a community whose
 2288 power usage is managed by an aggregator or energy service provider.

2289 **B.5.3.2 Time of Use (TOU) Pricing**

2290 Time of use pricing creates blocks of time and seasonal differences that allow smaller customers
 2291 with less time to manage power consumption to gain some of the benefits of real time pricing.
 2292 This is the favored regulatory method in most of the world for dealing with global warming.

2293
 2294 Although Real Time Pricing is more flexible than Time of Use, it is likely that TOU will still
 2295 provide many customers will all of the benefits that they can profitably use or manage.

2296 **B.5.3.3 Critical Peak Pricing**

2297 Critical Peak Pricing builds on Time of Use Pricing by selecting a small number of days each
 2298 year where the electric delivery system will be heavily stressed and increasing the peak (and
 2299 sometime shoulder peak) prices by up to 10 times the normal peak price. This is intended to
 2300 reduce the stress on the system during these days.

2301
 2302 California is the largest proponent of this tariff program at this time. Most of the California
 2303 utilities would prefer an incentive program instead to encourage the same behavior. There is
 2304 some question as to whether retailers in unregulated markets would have to pass thru the Critical
 2305 Peak Pricing to customers or if they could offer a flat price and hedge the risk of the critical peak
 2306 pricing.

2307 **B.6 External Parties Business Functions**

2308 **B.6.1 Gas and Water Metering**

2309 **B.6.1.1 Leak Detection**

2310 In the world of gas and water, non-revenue water and leaking gas pipes are important to track
2311 down. In the water industry, use of pressure transducers on smart meters has proven useful when
2312 doing minimum night flows to find unexpected pressure drops in the system. Normally the need
2313 is one pressure transducer meter per 500 to 1000 customers in an urban environment.

2314 **B.6.1.2 Water Meter Flood Prevention**

2315 With a disconnect in the water meter, it is possible if there is a sudden increase in flow and a
2316 drop in pressure that is sustained and unusual, that the disconnect can be activated and prevent
2317 flooding. Much work will have to be done in the control software algorithms to make this a
2318 useful benefit and not one the shuts off the water when the sprinkler system and the shower are
2319 both running.

2320 **B.6.1.3 Gas Leak Isolation**

2321 Similar to flood prevention, again the software needs to get much better or their needs to be a gas
2322 leak sensor in the structure that communicates with the meter.

2323 **B.6.1.4 Pressure Management**

2324 If there is a home area network, then shut off devices or throttling devices can be attached to
2325 specific water taps and the gas meter can communicate to thermostats and water heater controls
2326 to manage the rate of consumption in the location and help with pressure management on critical
2327 days.

2328 **B.6.2 Third Party Access**

2329 **B.6.2.1 Third Party Access for Outsourced Utility Functions**

2330 For some utilities, many of the business functions listed in the previous sections may be provided
2331 by third parties, rather than by the utility. In these situations, messaging will come through the
2332 "external party access" avenue, rather than an internally-driven messaging. The business
2333 processes will be fundamentally the same, but the security requirements could be significantly
2334 different and probably requiring stronger authentication at each system handoff.

2335

2336 Some of the business functions provided by third parties could include:

- 2337 • Prepaid metering
- 2338 • Remote connect/disconnect
- 2339 • Load management
- 2340 • Emergency control
- 2341 • Distribution automation
- 2342 • Customer usage information
- 2343 • HAN management

2344 **B.6.2.2 Third Party Security Management of HAN Applications**
2345 Customers will need access to HAN application accounts through a secure web portal where they
2346 can upload device and software security keys. Those keys will need to be sent through the AMI
2347 network to the meter to allow the HAN devices to provision and join with the meter.
2348

2349 Future functionality may include extraction of security keys out of the meter for storage in the
2350 utility's database. This will allow the keys to be downloaded back to a meter if it ever has to be
2351 replaced. This functionality will be required to eliminate the need to re-provision all the HAN
2352 devices in the house in the event of a meter replacement.

2353 **B.6.2.3 Appliance Monitoring**

2354 Appliances seldom last as long in the home as they do in the lab, part of this is that home owners
2355 do not do maintenance when they should, and part of it is that when small problems occur that
2356 are not handled, so they become big and expensive problems. Smart meters are a key part of an
2357 appliance monitoring solution, even for appliances that were installed long ago.

2358 **B.6.2.4 Home Security Monitoring**

2359 Today's security monitoring industry uses phone lines and other communications methods to
2360 monitor homes. The ability to hook security monitoring devices into a home area network and
2361 provide alerts and alarms over the smart metering network could lower the cost of home security
2362 monitoring making it more affordable to the people who live in areas most likely to need it.

2363 **B.6.2.5 Home Control Gateway**

2364 Home owners may want to control their home devices themselves or they may want a third party
2365 to do so, in either case, the smart metering system can be a method of providing that home area
2366 network gateway and allowing that control to be done.

2367 **B.6.2.6 Medical Equipment Monitoring**

2368 More and more medical equipment is being installed in homes as nursing homes and hospitals
2369 are getting too expensive to live in and more life support equipment is required for people who
2370 still can live at home unassisted most of the time. Today that equipment is only monitored by
2371 specialized companies and this seldom happens. It is a growing need especially for the elderly
2372 customers of the utility. While utilities may not wish to step into this role, the smart metering
2373 infrastructure can provide a way for authorized third parties to do so.

2374 **B.6.3 External Party Information**

2375 **B.6.3.1 Regulatory Issues**

2376 There are a number of issues that regulators need to judge the performance of a utility and the
2377 fairness of a utility to its customers. Smart metering has a role to play in providing facts to the
2378 regulator to help them manage these issues.

2379 **B.6.3.2 Investment Decision Support**

2380 When a utility goes to the regulator for a major capital expense there is a need for proof that the
2381 expense is required. Today like other regulator interactions, the data is typically made up of

2382 sampled data and expert opinions. With smart metering the complete data set is available to
2383 support the decisions.

2384 **B.6.4 Education**

2385 **B.6.4.1 Customer Education**

2386 Customers today call the call center and receive bills. They have little interaction with their
2387 utilities, less than 40% of the customer base interacts with the utility annually. The majority of
2388 the call volume is related to outage or other power quality issues. The second highest interaction
2389 reason is billing issues. If the industry is to be successful in changing people's habits and helping
2390 to reduce consumption, then there will need to be more interaction with customers, some on
2391 billing issues, some on power quality, but more on the way they consume power and what they
2392 have for appliances.

2393

2394 AMI systems will provide a means of interacting more with the customer, but only if the
2395 customer understands the capabilities – as well as being assured that AMI systems are not “Big
2396 Brother” watching over them.

2397 **B.6.4.2 Utility Worker Education**

2398 Utility workers will need significant education to learn not only their own roles in a utility with
2399 AMI, but also the issues of security and privacy that will become far more critical with the
2400 widespread scope of AMI systems.

2401 **B.6.5 Third Party Access for Certain Utility Functions**

2402 For some utilities, many of the business functions listed in the previous sections may be provided
2403 by third parties, rather than by the utility. In these situations, messaging will come through the
2404 "external party access" avenue, rather than an internally-driven messaging. The business
2405 processes will be fundamentally the same, but the security requirements could be significantly
2406 different and probably requiring stronger authentication at each system handoff.