

# SECURITY PROFILE FOR OPENADR

Prepared for:

The **UCAlug OpenADR  
Task Force, UCAlug SG  
Security Working Group &  
OpenADR Alliance**

Prepared by:

The **UCAlug OpenADR  
Task Force and SG  
Security Joint Task Force**

Managed by:

**UCAlug OpenADR Task  
Force**



Version  
0.03

SECURITY PROFILE FOR OPENADR	Version – 0.03	i
UCA International Users Group	March 30, 2012	

# Revision History

---

<b>Rev</b>	<b>Date</b>	<b>Summary</b>	<b>Marked</b>
0.01	2011-11-02	Initial draft for team review	N
0.01	2011-11-21	Revised for comments in 11/17/2011	N
0.01	2011-11-21	Revised for Ed Koch and Paul Lipkin comments	N
0.01	2011-12-12	Revised Controls section summary for scope definitions; remove section on Network Segmentation	N
0.02	2011-12-15	Created v0.02 for review cycle; accept changes, delete comments, remove issues log entries	N
0.03	03/30/2012	Applied changes based on comments submitted by Jeffrey J. Sweet (of American Electric Power; on behalf of Alan Rivaldo, Public Utilities Commission of Texas)	N

---

## Open Editorial Items and Issues Log

As open items and issues are addressed in new versions of this document, they are removed from this list.

<b>Item No.</b>	<b>Date</b>	<b>Provided By</b>	<b>Summary of the Issue</b>	<b>Status / Disposition</b>
			■	

# Executive Summary

---

This document presents the security profile for Open Automated Demand Response (OpenADR). The Security Profile identifies best practices for securing OpenADR functions in a smart grid environment.

This document defines a reference architecture, a set of use cases to define system functionality, and a set of security controls for systems and components that implement the use cases. The security controls in this document are inspired by and intended to cover the application of technical requirements found in *NIST Interagency Report (IR) 7628: Guidelines for Smart Grid Cyber Security* to OpenADR systems and technology. The underlying approach behind this document was therefore to (1) summarize OpenADR interactions based on the latest OpenADR 2.0 Specification, (2) define the function of these systems by presenting a reference architecture that defines abstract roles and use cases, (3) map the use cases and roles to real-world OpenADR systems, (4) define broad security objectives for OpenADR systems, (5) identify potential failures for each role in the context of the use cases, (6) define security controls to address the failures, and (7) assign controls to the roles.

The primary audience for this document is organizations that are developing or implementing solutions requiring or providing OpenADR functionality. This document is written for system owners, system implementers, and security engineers with at least a year of experience in securing electric utility field operations.

SECURITY PROFILE FOR OPENADR	Version – 0.03	iii
UCA International Users Group	March 30, 2012	

# Table of Contents

<b>INTRODUCTION</b> .....	<b>10</b>
1.1 SCOPE .....	11
1.1.1 <i>Explicit Exclusions</i> .....	12
1.2 APPROACH .....	12
1.3 AUDIENCE & RECOMMENDED USE .....	14
1.3.1 <i>Electric Utility and Demand Response Aggregators</i> .....	15
1.3.2 <i>OpenADR Vendors</i> .....	15
<b>2 FUNCTIONAL ANALYSIS</b> .....	<b>16</b>
2.1 LOGICAL ARCHITECTURE .....	17
2.2 ROLE DEFINITIONS .....	19
2.2.1 <i>Demand Response (DR) Controlling Entity</i> .....	19
2.2.2 <i>Demand Response (DR) Resource</i> .....	20
2.2.3 <i>Demand Response (DR) Asset</i> .....	20
2.3 ROLE MAPPINGS.....	21
2.4 USE CASES.....	21
<i>Use Case 1: Demand Response Resource Registers with a Demand Response Controlling Entity</i> .....	24
<i>Use Case 2: DR Controlling Entity Notifies DR Resource of DR Event (Point-to-point Push)</i> .....	26
<i>Use Case 3: DR Controlling Entity Notifies DR Resource of DR Event – (Broadcast)</i> .....	28
<i>Use Case 4: DR Resource Requests New DR Event from DR Controlling Entity (Point-to-point Pull)</i> .....	30
<i>Use Case 5: DR Resource Requests New DR Event from DR Controlling Entity (Anonymous Pull)</i> .....	32
<i>Use Case 6: DR Controlling Entity Schedules DR Resource for Periodic Feedback (Point-to-point Push)</i> .....	34
<i>Use Case 7: DR Resource Notifies DR Controlling Entity of Event Performance with Feedback by Request (Point-to-point Pull)</i> .....	36
<i>Use Case 8: DR Resource Notifies DR Controlling Entity of Event Performance with Feedback Self-Scheduled (Point-to-point Push)</i> .....	38
<b>3 FAILURE ANALYSIS</b> .....	<b>40</b>
3.1 FAILURE ANALYSIS PROCESS .....	40
3.2 SECURITY AND OPERATIONAL OBJECTIVES.....	41
3.2.1 <i>Contextual Assumptions</i> .....	42
3.2.2 <i>Security Principles</i> .....	43
3.3 FAILURES.....	45
<b>4 SECURITY CONTROLS</b> .....	<b>50</b>
4.1 SCOPE OF SECURITY CONTROLS.....	50
4.2 CONTROL DEFINITIONS.....	51
4.2.1 <i>Access Control</i> .....	53
4.2.2 <i>Audit and Accountability</i> .....	55
4.2.3 <i>Configuration Management</i> .....	56
4.2.4 <i>Continuity of Operation</i> .....	57
4.2.5 <i>Identification &amp; Authentication</i> .....	57
4.2.6 <i>Physical &amp; Environment Security</i> .....	59
4.2.7 <i>System &amp; Communications Protection</i> .....	59
4.2.8 <i>System &amp; Information Integrity</i> .....	61

4.2.9	<i>Controls Mapped to Roles</i> .....	62
<b>APPENDIX A:</b>	<b>RELATION TO THE NIST INTERAGENCY REPORT 7628</b> .....	<b>66</b>
A.1	TRACEABILITY .....	66
A.2	NIST IR 7628 ACTORS TO WAMPAC ROLES MAPPING.....	67
A.3	NIST IR 7628 SECURITY OBJECTIVES TO OPEN ADR SECURITY PRINCIPLES MAPPING .....	69
A.4	NIST IR 7628 TECHNICAL REQUIREMENTS MAPPED OPEN ADR CONTROLS.....	70
<b>APPENDIX B:</b>	<b>USE CASE NOTATION GUIDE</b> .....	<b>79</b>
<b>APPENDIX C:</b>	<b>USING THE SECURITY PROFILE TO EVALUATE AN OPENADR DEPLOYMENT</b> .....	<b>81</b>
<b>APPENDIX D:</b>	<b>GLOSSARY AND ACRONYMS</b> .....	<b>83</b>
<b>APPENDIX E:</b>	<b>REFERENCES</b> .....	<b>91</b>
<b>APPENDIX F:</b>	<b>OPENADR CRYPTOGRAPHIC SECURITY PROFILE</b> .....	<b>94</b>
F.1	METHOD.....	94
F.2	REFERENCES.....	95
F.3	HASH.....	96
	CONSIDERATIONS .....	96
	RECOMMENDATION.....	96
F.4	SYMMETRIC ENCRYPTION .....	96
	CONSIDERATIONS .....	96
	RECOMMENDATION.....	96
F.5	PUBLIC KEY/DIGITAL SIGNATURE .....	97
	CONSIDERATIONS .....	97
	RECOMMENDATIONS .....	97
	CIPHER SUITES.....	97

# Table of Figures

---

FIGURE 1 - OVERVIEW OF SECURITY PROFILE DEVELOPMENT APPROACH .....	12
FIGURE 3 – ARTIFACT RELATIONSHIPS .....	14
FIGURE 4 – ROLE INTERACTION DIAGRAM .....	17
FIGURE 5 – DR EVENT ACTIVITY DIAGRAM .....	18
FIGURE 6 - ROLE MAPPING.....	21
FIGURE 7 – SECURITY PROFILE WORKFLOW NIST-IR 7628 MAPPING .....	67
FIGURE 8 – UNIFIED LOGICAL ARCHITECTURE FOR OPENADR.....	68
FIGURE 9 – AN ANNOTATED SEQUENCE DIAGRAM .....	80
<i>Diagram: Use Case 1: Register DR Resource.....</i>	<i>25</i>
<i>Diagram: Use Case 2: DR Event Notification .....</i>	<i>27</i>
<i>Diagram: Use Case 3: DR Event Notification – Broadcast .....</i>	<i>29</i>
<i>Diagram: Use Case 4: DR Resource Requests DR Controlling Entity for New DR Event.....</i>	<i>31</i>
<i>Diagram: Use Case 5: Anonymous DR Resource Requests DR Controlling Entity for New DR Event.....</i>	<i>33</i>
<i>Diagram: Use Case 6: DR Controlling Entity Schedules DR Resource for Periodic Feedback .....</i>	<i>35</i>
<i>Diagram: Use Case 7: DR Resource Notifies DR Controlling Entity of Event Performance (Feedback).....</i>	<i>37</i>
<i>Diagram: Use Case 8: DR Resource Notifies DR Controlling Entity of Event Performance with Feedback Self-Scheduled.....</i>	<i>39</i>

# Table of Tables

---

TABLE 1 – CONTROLS: ACCESS CONTROL.....	53
TABLE 2 – CONTROLS: AUDIT AND ACCOUNTABILITY.....	55
TABLE 3 - CONTROLS: CONFIGURATION MANAGEMENT.....	56
TABLE 4 - CONTROLS: CONTINUITY OF OPERATIONS .....	57
TABLE 5 - CONTROLS: IDENTIFICATION & AUTHENTICATION .....	57
TABLE 6 - CONTROLS PHYSICAL & ENVIRONMENT SECURITY.....	59
TABLE 7 - CONTROLS: SYSTEM & COMMUNICATIONS PROTECTION.....	59
TABLE 8 - CONTROLS: SYSTEM & INFORMATION INTEGRITY.....	61
TABLE 9 - CONTROLS MAPPED TO ROLES.....	62
TABLE 10 – NIST IR 7628 ACTOR TO WAMPAC ROLE MAPPING.....	69
TABLE 11 - NIST IR 7628 USE CASE OBJECTIVES TO OPENADR SECURITY PRINCIPLES.....	69
TABLE 12 - NIST IR 7628 TECHNICAL REQUIREMENTS MAPPED TO OPENADR CONTROLS .....	70

# ***Acknowledgements***

---

SECURITY PROFILE FOR OPENADR	Version – 0.03	<b>viii</b>
UCA International Users Group	March 30, 2012	



# Authors

---

Bruce Bartell, Xtensible Solutions on behalf of SCE and PG&E

Darren Highfill, UtiliSec

Ed Koch, Akuacom/Honeywell

Phillip Lee, Honeywell

Tom Markham, Honeywell

Edited by: Bruce Bartell

SECURITY PROFILE FOR OPENADR	Version – 0.03	ix
UCA International Users Group	March 30, 2012	

# 1 **Introduction**

---

2 This document presents the security profile for Open Automatic Demand Response  
3 (OpenADR). System functions considered for OpenADR which includes standardized  
4 dispatch, control and pricing signals for Demand Response (DR) and Distributed  
5 Generation (DG) and related messages for monitoring the status and capabilities of the  
6 participating resources. The recommendations made herein are based on stated system  
7 architectural and functional assumptions, and offer a singular security baseline for overall  
8 use of OpenADR with tailored subsets of recommendations where variations in system  
9 deployment or usage occur.

10 This document defines a Reference Architecture, a set of use cases to define system  
11 functionality, and a set of security controls for systems and components that implement  
12 the use cases. The security controls in this document are inspired by and intended to  
13 cover the application of technical requirements found in *NIST Interagency Report (IR)*  
14 *7628: Guidelines for Smart Grid Cyber Security*<sup>1</sup> to OpenADR systems and technology.  
15 While NIST IR 7628 serves as an industry-wide reference that a utility or other  
16 OpenADR participants may use as a starting point to identify intersystem-level security  
17 requirements, this document provides the next level of detail by specifically addressing  
18 the use of OpenADR Signals and defining security controls. The controls presented  
19 herein may then, in turn, be satisfied by communications protocol definition-level  
20 standards and manufacturing specifications. The underlying approach for developing this  
21 document was (1) to draw on existing and developing OpenADR Standards and

---

<sup>1</sup> National Institute of Standards and Technology (NIST), Guidelines for Smart Grid Cyber Security, NIST Interagency Report 7628, August 2010. Available at: <http://csrc.nist.gov/publications/PubsNISTIRs.html>.

22 implementations, (2) define the function of these systems by presenting a reference  
23 architecture that defines abstract roles and use cases, (3) map the architecture's roles to  
24 OpenADR interactions, (4) define broad security objectives for OpenADR systems, (5)  
25 identify potential failures for each role in the context of the use cases, (6) define security  
26 controls to address the failures, and (7) assign controls to the roles.

27 Demand Response is defined as the temporary modification of customer energy usage for  
28 a defined duration which is triggered by some condition on the grid such as reliability or  
29 market conditions. These DR events result in the exchange of “DR signals” between  
30 service providers such as Utilities, Independent System Operators (ISO’s), Aggregators,  
31 Energy Service Providers (ESP’s), etc. and their customers. The information in the DR  
32 signals causes modifications to the end users load profiles. The temporary modifications  
33 to energy usage happen during “DR Events” when participants are called to perform  
34 according to the terms defined as part of enrollment in a DR Program.

35 An understanding of the concept of roles is essential to applying the security controls  
36 defined in this document. Roles have been designed abstractly to ensure applicability  
37 across a range of OpenADR deployment in different markets and with different actors  
38 with similar responsibilities. The parties are actors that can assume different roles  
39 depending on the type of interaction. The key roles for this document are Demand  
40 Response (DR) Controlling Entity, Demand Response (DR) Resource and Demand  
41 Response (DR) Asset. A DR Controlling Entity sends signals to DR Resources during  
42 DR Events in order to influence demand behavior. The roles and interactions mentioned  
43 above are elaborated in Section 2.

44 It is important to note that a single actor may implement multiple roles and that a role can  
45 be assumed by multiple actors. Moreover, each role may be implemented in different  
46 ways, using different technologies, and by different vendors. By assigning security  
47 controls to the abstract roles, no bias is expressed in any of these dimensions. This  
48 document addresses security concerns by requiring that products implementing the  
49 functionality of a given role satisfy all security controls associated with that role. If a  
50 product implements the functionality of multiple roles, it must implement all of the  
51 security controls associated with each of the roles.

## 52 **1.1 Scope**

53 This security profile addresses the security of functions involved in the deployment of  
54 OpenADR. The focus is on those aspects of DR management that is required to facilitate  
55 the exchange of DR signals between parties.

56 The types of DR interactions in scope are:

- 57 • Direct Load Control Signals
- 58 • Dispatching of Load Profiles
- 59 • DR Related Pricing Signals
- 60 • DR Resource Registration

- Response and Feedback from DR Resources for DR Signals

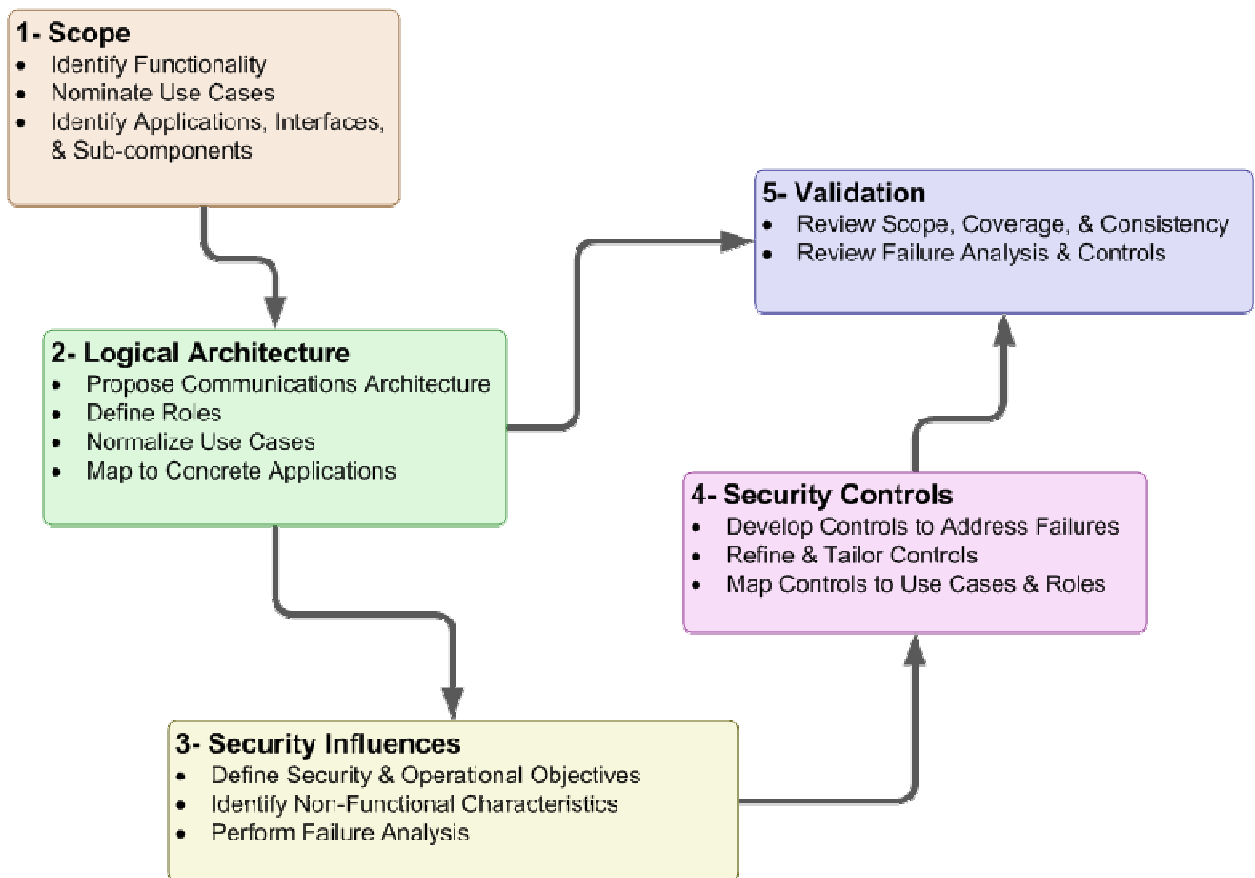
This document also recognizes that some organizations will only implement a subset of the functions defined herein, and is therefore designed to accommodate different configurations and choices.

### 1.1.1 Explicit Exclusions

Interactions to support many of the administrative aspects of managing a DR program such as Enrollment, Measurement and Verification (M&V), and Settlement are not in scope. The information and processes required for the Enrollment are still largely manual and vary depending on the participants and market structure. M&V and Settlement standards are defined elsewhere by Standards Setting Organizations such as NAESB and The IEC. The economic incentives used in DR Programs are supported by these settlement standards.

## 1.2 Approach

The procedure used to develop this security profile is shown in Figure 1 - Overview of Security Profile Development Approach. This procedure has five steps and, as illustrated below, these steps are not necessarily sequential and may in fact be iterative in nature.



77

78

**Figure 1 - Overview of Security Profile Development Approach**

SECURITY PROFILE FOR OPENADR	Version – 0.03	<b>12</b>
UCA International Users Group	March 30, 2012	

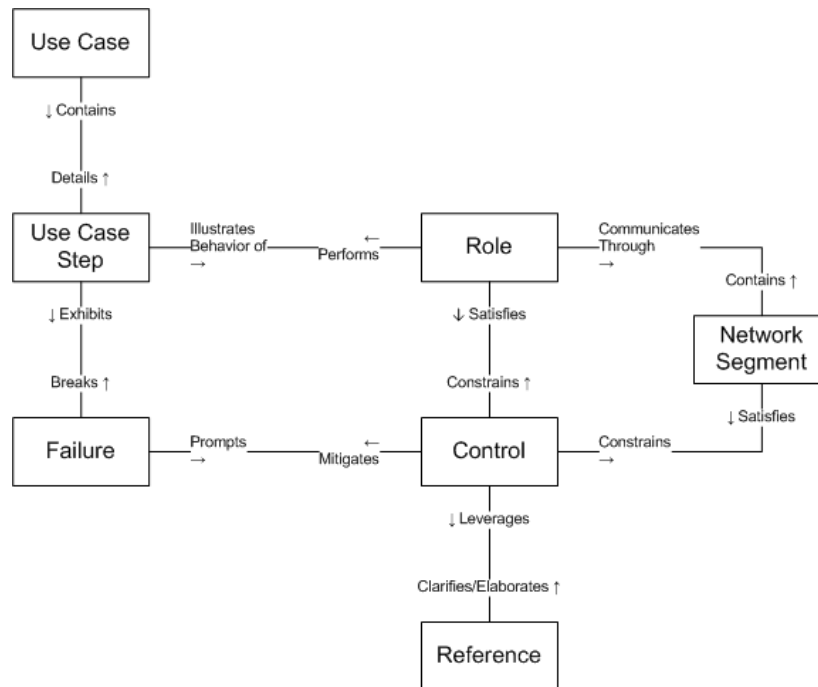
79 Steps 1 and 2, which are chiefly concerned with defining the scope of the profile, are  
 80 repeated several times as the development team works with stakeholders to understand  
 81 their needs. Steps 3 and 4 define the purpose of security in the system’s operation and  
 82 how security is realized. Steps 2 and 4 join in the final phases of the profile’s  
 83 development when the development team checks that the set of selected controls is  
 84 complete and relevant. Step 5, which is concerned with validating the convergence of  
 85 previous steps, proceeds in parallel with steps 3 and 4. The tasks within each step are  
 86 summarized below:<sup>2</sup>

- 87 1. *Define the scope of the security profile.* The first step is to decide what aspects of  
 88 the system are to be included in the security profile. This step requires discussion  
 89 with stakeholders, consideration of existing and planned systems that will fall  
 90 within the scope of the profile, and the construction of a conceptual model of  
 91 those systems that refines and clarifies the statement of scope. The conceptual  
 92 model includes use cases that define what uses of the system are addressed by the  
 93 security profile and identifies the roles within those use cases that are the targets  
 94 of the security guidance to be developed.
- 95 2. *Construct a logical architecture showing the relationships between roles in the*  
 96 *use cases.* The logical architecture ties the conceptual model developed in step 1  
 97 above to architectures and concrete applications familiar to stakeholders. The  
 98 logical architecture shows which roles and relationships fall within the scope of  
 99 the profile and which, though appearing in the use cases, may nonetheless fall  
 100 outside the scope of the profile.
- 101 3. *Identify security influences and objectives.* The specific aims of the security  
 102 profile are defined here in terms of the logical architecture from step 2. These  
 103 aims include high-level security guidance that the profile will refine, related  
 104 security guidance that will be tailored for the security profile, and characteristics  
 105 of the system that must be preserved as security controls are put into place. This  
 106 step also includes identification of security related failures that may inhibit the  
 107 operation of the system.
- 108 4. *Define the security controls.* New security controls are defined, existing controls  
 109 from other security documents are referenced, or both to meet the security  
 110 objectives defined in step 3. Each role is associated with the set of roles it is  
 111 expected to implement.
- 112 5. *Validation.* This step encompasses a collection of validation checks, such as  
 113 ensuring that the selected controls are complete with respect to the identified  
 114 failures (i.e., that there is at least one control for each failure) and that there are no  
 115 superfluous controls (i.e., for each recommended control, there is a failure that it  
 116 addresses).

117 The products of these steps are shown in Figure 2.

---

<sup>2</sup> For a more detailed description of this process, please see the ASAP-SG Security Profile Blueprint.  
[http://www.smartgridipedia.org/images/4/43/Security\\_Profile\\_Blueprint\\_-\\_v1\\_0\\_-\\_20101006.pdf](http://www.smartgridipedia.org/images/4/43/Security_Profile_Blueprint_-_v1_0_-_20101006.pdf)



**Figure 2 – Artifact Relationships**

118  
119

120 The individual use case steps within each use case provide a detailed view of the  
121 activities that are considered within the scope of the profile. Each step is carried out by a  
122 specific role, and that role is responsible for the security controls that mitigate potential  
123 failures of the step. These potential failures are identified in step 3 above by considering  
124 of how each step in these use cases may fail and, consequently, how the failure might  
125 prevent the system or role from successfully carrying out the use case. Each identified  
126 potential failure of a step in a use case prompts the development of one or more controls  
127 to mitigate it.

128 Though most controls are assigned to specific roles, some failures span two or more roles  
129 and therefore imply a failure of the communication network that is used by the roles to  
130 coordinate their actions. These failures are mitigated by network controls that focus  
131 specifically on protecting the movement of information within the use case. These  
132 controls take the form of recommended network segmentation (see Section 4.1).

133 Whenever a control is derived from sources identified in step 4, that source (e.g.,  
134 reference to a specific NIST IR 7628 requirement number) is noted.

### 135 **1.3 Audience & Recommended Use**

136 The primary audience of this document is organizations that are developing or  
137 implementing solutions requiring or providing OpenADR functionality. This document is  
138 written for system owners, system implementers, and security engineers with at least a  
139 year of experience in securing electric utility field operations. The user is assumed to be  
140 experienced at information asset risk estimation. The user is further assumed to be  
141 knowledgeable in applying security requirements and guidance. The user will ultimately

142 leverage this profile by reference as the specific set of security controls that must be  
143 implemented by OpenADR components and systems, above and beyond organizational-  
144 level requirements as specified in the NIST IR 7628 and other recommended best  
145 practice documents for cyber security as listed in Section 4.2 and Appendix  
146 E:References.

147 Additional sections below discuss how the document should be used by various  
148 stakeholders. The profile development approach (summarized in Section 1.2) guides the  
149 reader through the process used in this document for determining controls required for  
150 given failures (impacts) for roles and the functionality they implement (use cases),  
151 thereby providing traceability and justification for each of the controls selected.

### 152 ***1.3.1 Electric Utility and Demand Response Aggregators***

153 An electric utility may use this document to help achieve multiple security objectives for  
154 their organization through activities such as:

- 155 1. developing security requirements for OpenADR technology procurement  
156 activities
- 157 2. configuring and operating OpenADR systems
- 158 3. evaluating planned or deployed OpenADR solutions (see Appendix C: for more  
159 information)

160 In some cases, a utility will not make use of all functionality described in the included  
161 use cases, which may obviate the requirements for certain controls. The tables within the  
162 document can be used to determine security controls needed for a utility's environment  
163 and provide traceability and justification for the design requirements and control  
164 selection. In other cases, an organization may identify an alternative (mitigating) control  
165 that makes a required control unnecessary, but the utility should be sure it addresses all  
166 the same failures and should perform a risk analysis to confirm the adequacy of the  
167 alternative control.

### 168 ***1.3.2 OpenADR Vendors***

169 Vendors may use this document to incorporate security controls needed for the  
170 development of OpenADR products as well as solutions built upon or derived from  
171 OpenADR technology. This document provides enough requirement detail to allow a  
172 vendor to begin design activities, but avoids prescription that would thwart innovation or  
173 drive toward specific implementations. The reference architecture and use cases also  
174 offer tools for understanding OpenADR applications in an abstract sense.

175

## 2 Functional Analysis

---

177 The purpose of the functional analysis is to define a clear picture of the scope,  
178 architecture, and functionality of Open Automated Demand Control (OpenADR)  
179 systems, as addressed by this security profile. The implementation of OpenADR system  
180 functions varies in terms of function, scope, and technology from among different market  
181 and system offerings and deployments. However, this profile approaches the problem by  
182 defining a set of abstract roles that capture essential functionality that may be realized  
183 through a variety of implementations. This profile defines roles in such a way that the  
184 logical architecture and use case functionality may be used to represent a wide variety of  
185 real-world implementations.

186 By way of background, the following steps were performed in the functional analysis:

- 187 1. Review of the existing documents that define the overall OpenADR process,  
188 paradigm, and design (as defined in Appendix E References).
- 189 2. Define abstract roles that characterize elements of OpenADR Systems. Roles are  
190 neutral to implementation and vendor, and capture the essence of common  
191 functionality without the details of particular applications. The resulting roles are  
192 presented in Section 2. Their relationships with each other (topologically) are  
193 presented in Section 2.1.
- 194 3. Define use cases describing how the roles interact to implement OpenADR  
195 functionality. The use cases are modular in nature, which allows organizations to  
196 determine which use cases are relevant to their deployments. They also capture  
197 raw functionality, without the inclusion of security controls, which ensures that no  
198 pre-existing security controls are assumed and allows different controls to be  
199 applied without bias. The resulting use cases are presented in Section 2.4.

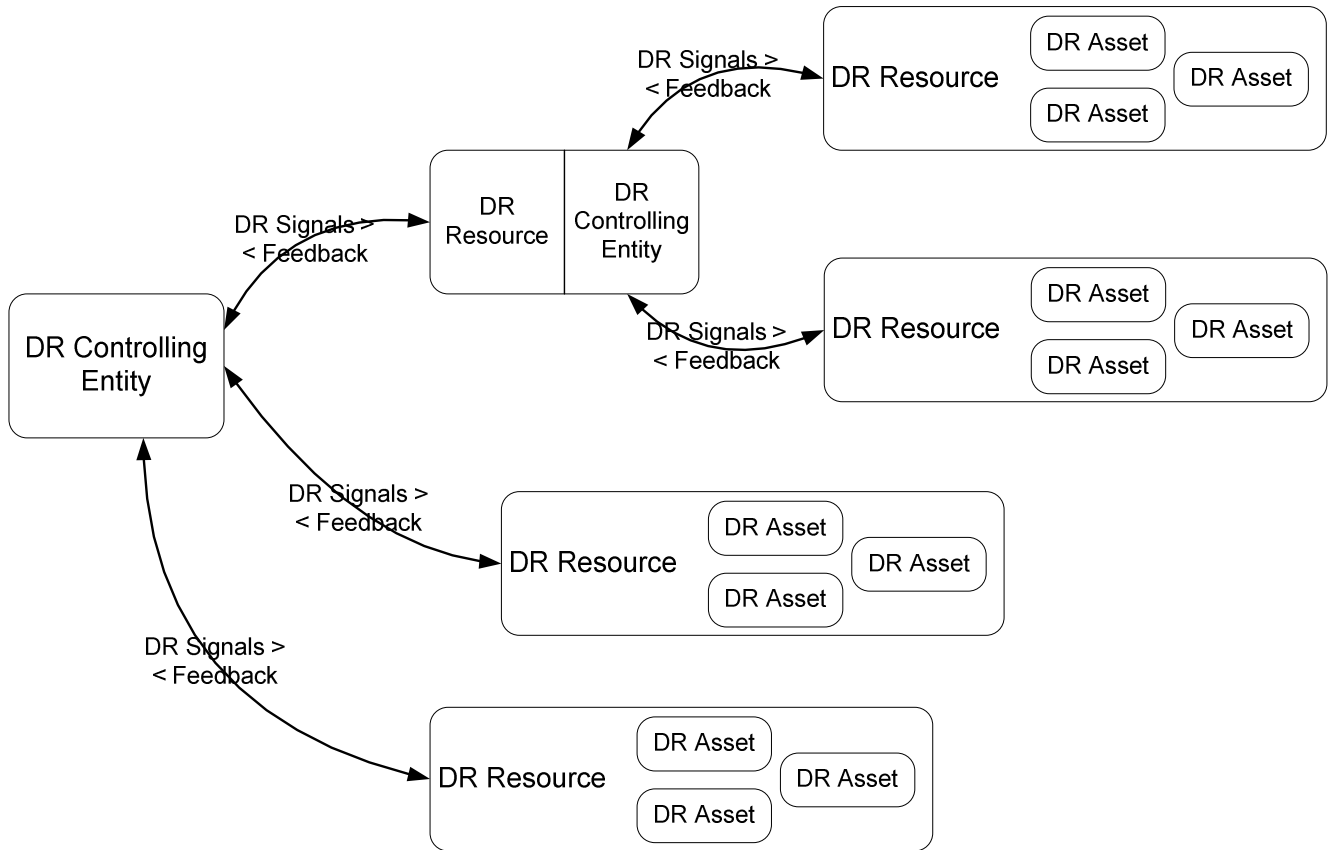


200 4. Validate the roles and use cases by ensuring that they are adequate to describe  
 201 common real-world implementations. The mapping between roles and real world  
 202 implementations are presented in Section 2.3 (this is presented before the use  
 203 cases to reinforce the meaning of the roles).

204 The security recommendations found in this document are defined in terms of the logical  
 205 architecture and its constituent roles, both of which are defined in this section. The  
 206 logical architecture includes some elements that are outside the scope of this profile;  
 207 however, each of these elements is important within the context of OpenADR and so are  
 208 included as context.

## 209 **2.1 Logical Architecture**

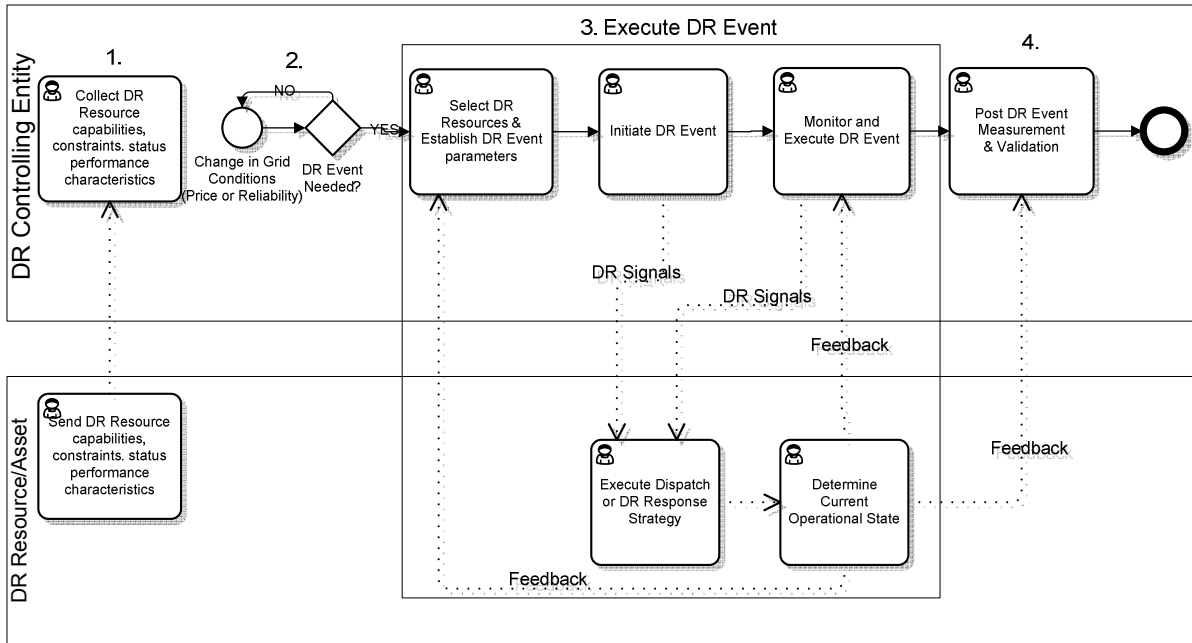
210 The roles defined in this profile are *abstract* or *logical* roles; that is, each role does not  
 211 necessarily map one-to-one with an actor, device, or system. It is possible for an actor to  
 212 implement the functionality of multiple roles. However, it is also possible for the  
 213 functionality of one role to be implemented by multiple actors. This document focuses on  
 214 defining the roles, their functionality, and ultimately the security controls each role must  
 215 implement at this abstract level and leaves the task of mapping roles to specific actors,  
 216 devices, or systems to those developing or procuring these elements.



217  
 218  
 219

**Figure 3 – Role Interaction Diagram**

220 The essential roles involved in OpenADR are shown in Figure 3 – Role Interaction  
 221 Diagram. This diagram represents the roles (defined in Section 2.2) as rounded  
 222 rectangles. Rectangles that include other rectangles indicate that a role is a composition  
 223 or aggregation of other roles. For example, a DR Resource is comprised of multiple  
 224 assets. A rectangle with multiple roles indicates that a single actor can act in multiple  
 225 roles in the OpenADR process. For example, the same actor can be a DR Resource for on  
 226 set of interactions, and a DR Controlling Entity for another set of interactions.



227  
 228

229 **Figure 4 – DR Event Activity Diagram**

230 A high level Activity Diagram of the OpenADR Event process is shown in Figure 4 – DR  
 231 Event Activity Diagram.

232 The detailed steps of all OpenADR processes in scope are defined in detailed Use Cases  
 233 in Section 2.4. The major steps are outlined as:

- 234 1. A DR Resource communicates capabilities, constraints, status and performance  
 235 characteristics to a DR Controlling Entity.(Register DR Resource)
- 236 2. A DR Controlling Entity decides to call an event (based on grid conditions)  
 237
  - Determine what objectives to meet during the Event schedule
- 238 3. Execution of the Event  
 239
  - Determine which DR Resources and participation schedules to apply to  
 240 meet those objectives
  - 241 ○ Send Signal(s) to the DR Resources
  - 242 ○ Monitor what is going on (Feedback from DR Resources)

243 4. Evaluation of what happened (out of scope for OpenADR)

244           ○ Measurement and Verification

245           ○ Reconciliation (Billing)

246

247 All roles are assumed to have some inherent communications ability (i.e., there is no need  
248 to model a distinct communications element associated with each role).

249

250

## 251 **2.2 Role Definitions**

252 All roles are defined in the following sub-sections.

### 253 **2.2.1 Demand Response (DR) Controlling Entity**

254 The Demand Response Controlling Entity role represents all of the different entities that  
255 may need to manage and interact with wholesale and/or retail DR resources and includes  
256 the following actors: Independent System Operator / Regional Transmission Operator  
257 (ISO/RTO), Distribution Company, Load Serving Entity, DR Aggregator and others.  
258 Different actors may function as the DR Controlling Entity at different points in the  
259 process of administering a DR Event. The DR Controlling Entity may represent a single  
260 actor, such as a Utility Distribution Company (UDC) in the business role of a Load  
261 Serving Entity.

262 A DR Controlling Entity may represent a hierarchy of entities such as the following  
263 example:

- 264           • An ISO/RTO dispatches DR instructions to a Transmission Operator.
- 265           • The Transmission Operator in turn assumes the DR Controlling entity role by  
266           sending the dispatch instructions on to a UDC.
- 267           • The UDC in turn assumes the DR Controlling Entity Role by sending instructions  
268           to a DR Aggregator.
- 269           • The DR Aggregator then assumes the DR Controlling Entity role by directing a  
270           specific DR Resource to execute the instruction.

271 This can be modeled as a recursive relationship with a DR Controlling Entity which  
272 represents each of these actors in an integration role. The goal is to minimize the number  
273 of different logical components and hence the number of different services and message  
274 payloads that need to be defined through reuse of the standard services and payload  
275 definitions.

276 This concept is elaborated more extensively in an EPRI report titled *Concepts to Enable*  
 277 *Advancement of Distributed Energy Resources*.<sup>3</sup> The terminology for the interaction  
 278 parties varies depending on the source<sup>4 5</sup>. For the purposes of this analysis, the roles and  
 279 definitions used are those defined in “OpenADR 1.0 System Requirements Specification  
 280 v1.0” developed by the OpenSG OpenADR Task Force.

### 281 **2.2.2 Demand Response (DR) Resource**

282 A DR resource is a virtual representation of one or more assets or physical devices  
 283 capable of shedding or managing load in response to a triggering event. A DR Resource  
 284 may consist of multiple assets or devices that have been aggregated to form a larger load  
 285 shedding capacity or energy resource.

286 As in the examples for a DR Controlling Entity, many of the same actors are also a DR Resource:

- 287 • An ISO/RTO dispatches DR instructions to a Transmission Operator. The Transmission Operator  
 288 is a DR Resource of the ISO/RTO.
- 289 • The Transmission Operator in turn assumes the DR Controlling entity role by sending the dispatch  
 290 instructions on to a UDC. The UDC is a DR Resource of the Transmission Operator.
- 291 • The UDC in turn assumes the DR Controlling Entity Role by sending instructions to a DR  
 292 Aggregator. The DR Aggregator is a DR Resource of the UDC.
- 293 • The DR Aggregator then assumes the DR Controlling Entity role by directing a specific DR  
 294 Resource to execute the instruction. The DR Resource in this example could be a manufacturing  
 295 facility. The facility has multiple types of machinery that is one large DR Resource composed of  
 296 the aggregated the total load shedding capacity of all the assets or devices in the plant. A DR  
 297 Resource may also consist of different types of generation assets such as a wind Turbine, battery,  
 298 and an electric motor that work in combination to meet DR program obligations.

### 299 **2.2.3 Demand Response (DR) Asset**

300 A DR Asset is an end device that is capable of shedding or managing load in response to  
 301 Demand Response Events, Energy or Ancillary Services, Price Signals or other system  
 302 events (e.g. under frequency detection). The DR Asset can be controlled by an end device  
 303 control through Direct Load Control or Demand Response Load Control.

---

<sup>3</sup> Concepts to Enable Advancement of Distributed Energy Resources: White Paper on DER. EPRI, Palo Alto, CA : 2010. 1020432

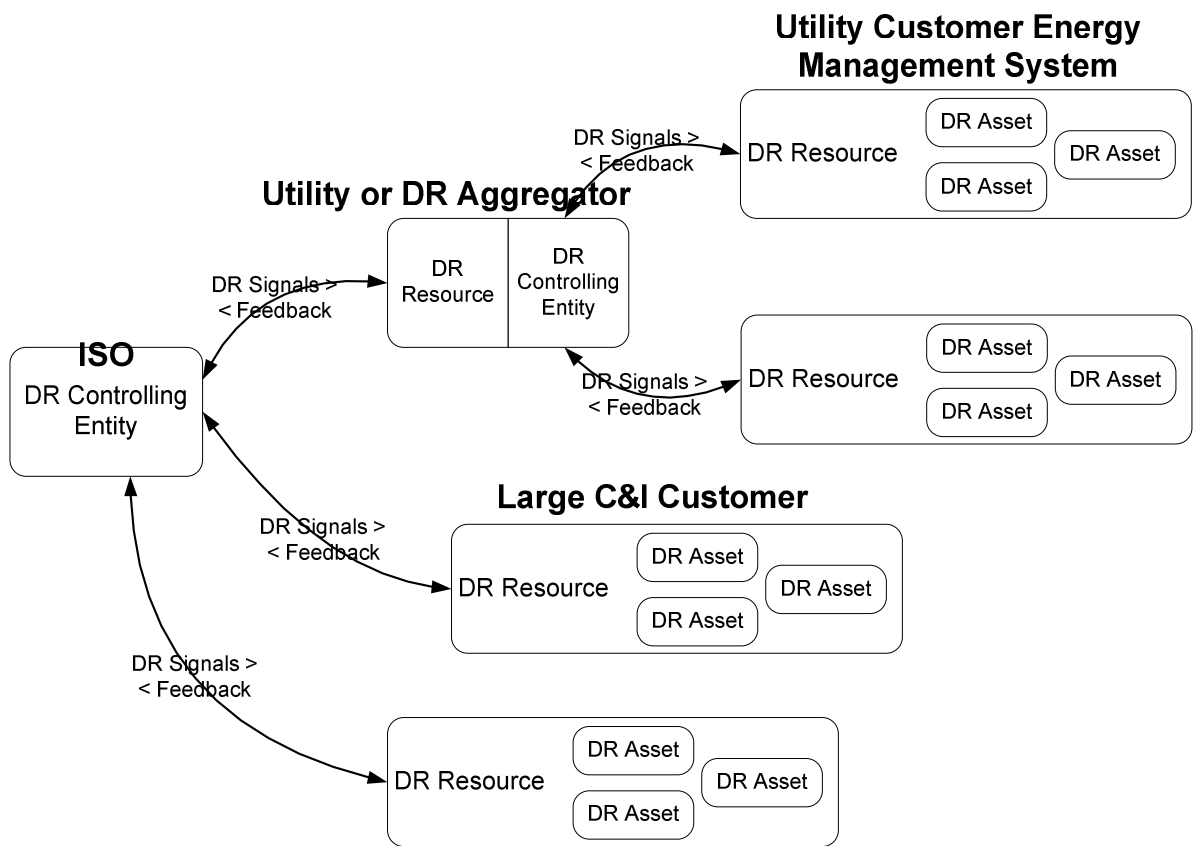
<sup>4</sup> The document referenced by 3 is also referenced by **[ENERGYINTEROP-v1.0]** *Energy Interoperation Version 1.0*. OASIS Committee Specification Draft 02 / Public Review Draft 02. 15 July 2011.  
<http://docs.oasis-open.org/energyinterop/ei/v1.0/csprd02/energyinterop-v1.0-csprd02.html>

<sup>5</sup> For the purposes of use case interactions defined in this document the role DR Controlling Entity is equivalent to Resource Energy Controller (REC) as used in 3 and Virtual Top Node (VTN) as used in 4. The role of DR Resource is equivalent to the role of Virtual End Node as used by 3 and 4.

304 **2.3 Role Mappings**

305 The logical architecture presented in the previous section can be realized in different  
 306 deployment settings. For example, The DR Controlling Entity that initiates a DR Event  
 307 can be a Market Operator, Independent System Operator (ISO), or a Utility depending on  
 308 location and market structure. The DR Resource that participates in the event under the  
 309 direction of a DR Controlling Entity could be a Utility, DR Aggregator, or any resource  
 310 at a customer location. At each level of interaction a DR Resource that receives a DR  
 311 Signal from a DR Controlling Entity can in turn act as a DR Controlling Entity to direct  
 312 other DR Resources. An example of one possible mapping to a single implementation  
 313 scenario is provided in Figure 3.

314



315  
 316  
 317

**Figure 5 - Role Mapping**

318 **2.4 Use Cases**

319 This section is a subset of all the interactions needed to implement OpenADR as a system  
 320 based on the scope defined in Section 2.1.

321 This Security Profile defines OpenADR functionality using the following use cases:

- 322 • Use Case 1 deals with the interactions initiated by a DR Resource to provide the  
 323 DR Controlling Entity with information on the capabilities and constraints of a  
 324 DR Resource to participate in DR Events. These include:
- 325 ○ Notice of capabilities and constraints and subsequent changes these  
 326 capabilities and constraints.
  - 327 ○ Notice of scheduling constraints based on temporary changes to  
 328 availability
- 329 • Use Cases 2-5 deal with the interactions used by a DR Controlling Entity to  
 330 manage the DR Resources during the execution of a DR Event. The DR Signals  
 331 used by a DR Controlling Entity can influence the behavior of a DR Resource  
 332 through the use of signal types for Objectives, Price, and Direct Load Control. For  
 333 the purposes of failure analysis the use cases are broken out based on the  
 334 interaction pattern<sup>6</sup>:
- 335 ○ Point to Point Push – Point to Point Push is an interaction initiated by the  
 336 producer or creator of the message. This pattern assumes that the  
 337 communications is point to point and between entities that are aware of  
 338 each others identity.
  - 339 ○ Point to Point Pull – Point to Point Pull is an interaction initiated by the  
 340 message consumer. It requires that a callback can be associated with a  
 341 request. This pattern assumes that the communications is point to point  
 342 and between entities that are aware of each others identity.
  - 343 ○ Broadcast – A Broadcast is a message sent to a set of parties where the  
 344 sender does not know who the recipients may be. Access to the broadcast  
 345 message could be through a message board, a message broker, or other  
 346 means. A Broadcast may also be considered an anonymous push.
  - 347 ○ Anonymous Pull – The Anonymous Pull pattern is similar to the point to  
 348 point pull except that the identity of the consumer is unknown to the  
 349 sender. It is also assumed that no reply from the consumer is required or  
 350 expected.
- 351 • Use Cases 6-8 deal with Feedback provided by a DR Resource to a DR  
 352 Controlling Entity during the execution of a DR Event. Feedback interactions use  
 353 Point-to-point Pull and Point-to-point Push as defined above. Use Cases 7-8 are  
 354 derivatives of Use Case 6.
- 355 These use cases do *not* include security controls, such as the use of authentication or  
 356 encryption. Security controls and their mapping to the roles performing these use cases  
 357 are found in Section 4.

---

<sup>6</sup> The terminology used for interaction patterns applies only to the pattern being described, and do not imply any specific routing or communication methodology.

358 The use cases include the depiction of “acknowledgements” in the interaction (sequence)  
359 diagrams for the purpose of completeness in the representation. Acknowledgements are  
360 considered a separate security control and are not included in the use case summary or  
361 addressed individually in context of a use case step. A “reply” to a message contains  
362 other information other than a simple acknowledgement that a message has been received  
363 (e.g. notice of non-performance, failure information, etc.). Reply messages are included  
364 are included in the use case analysis as security controls may vary by context.

365 Each use case contains the following elements:

- 366 • Use Case Description: This is a summary of the use case, describing the overall  
367 flow and steps.
- 368 • Preconditions: These are conditions that must be true for the use case to be  
369 successfully executed.
- 370 • Minimal Guarantees: These are properties that must remain true any time the use  
371 case is initiated, regardless of whether it terminates successfully.
- 372 • Success Guarantees: These are properties that will be true only if the use case  
373 terminates successfully. This requires that all preconditions and all condition  
374 checks (e.g., for validity of a request) be satisfied during execution of the use  
375 case.
- 376 • Trigger: This is the stimulus that initiates execution of the use case.
- 377 • Main Success Scenario: This defines the series of steps undertaken by each role  
378 during successful execution of the use case. The scenario is depicted graphically  
379 in an activity diagram (the notation used in these diagrams is explained in  
380 Appendix B) and each step is summarized in text.

381

382

383 ***Use Case 1: Demand Response Resource Registers with a Demand***  
384 ***Response Controlling Entity***

385 **Use Case Description:** A party with ownership, controlling interest or administrative  
386 responsibilities for a Resource communicates operational information about the Resource  
387 to a controlling entity. This includes information about the capabilities, availability, and  
388 constraints regarding the Resource’s ability to shed load or generate power.

389 The DR Resource initiates the process through a Registration Message and can  
390 subsequently change that information or remove any availability for performance in a DR  
391 Program using the same interaction pattern. A DR Resource can also declare itself  
392 unavailable to perform in a DR Program on a temporary basis using an Opt-out.

393

394 **Preconditions:**

- 395
- The DR Resource and DR Controlling Entity have all of the necessary network  
396 connections available.
  - The party with ownership, controlling interest or administrative responsibilities  
397 for the Resource has enrolled in a Demand Response Program that is administered  
398 by the DR Controlling Entity.  
399

400 **Minimal Guarantees:**

- 401
- The DR Resource does not reveal any information to another party that would  
402 allow that party to provide any false information to a DR Controlling Entity  
403 attributed to the DR Resource.
  - The DR Controlling Entity does not process any invalid data.  
404

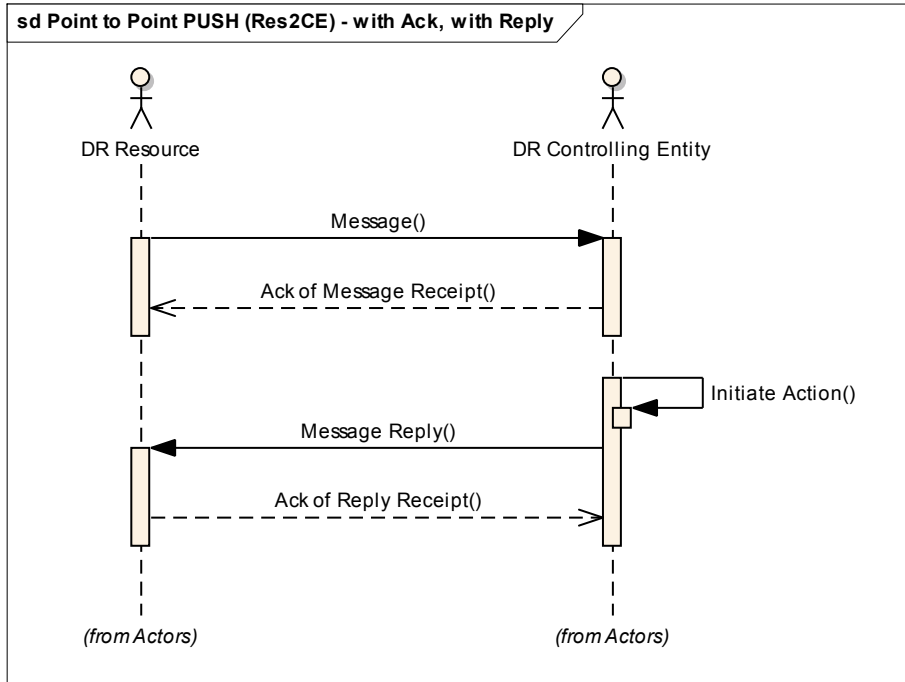
405 **Success Guarantees:**

- 406
- The DR Resource has registered with the DR Controlling Entity prior to a call for  
407 performance under the terms of the DR Program and provided all Resource  
408 information necessary to participate in a DR Event.

409 **Trigger:**

410 The trigger for this use case could be an operator initiated trigger or the result of a pre-  
411 configured device configured to participate in a DR Program.





412

413

**Diagram: Use Case 1: Register DR Resource**

414

**Main Success Scenario:**

416 1: The DR Resource sends a registration request to create, change, or remove a profile to  
 417 the DR Controlling Entity.

418 2: The DR Controlling Entity receives the registration.

419 3: The DR Controlling Entity assesses the validity of the Resource registration request.

420 4: The DR Controlling Entity sends a reply based on the results of the assessment.

421 ***Use Case 2: DR Controlling Entity Notifies DR Resource of DR Event***  
422 ***(Point-to-point Push)***

423 **Use Case Description:** This interaction is used to dispatch DR Resources. The initiator  
424 of the interaction is the DR Controlling Entity. The initiating event message is directed to  
425 a specific DR Resource. The dispatch can convey an objective, price or direct load  
426 control signal.

427 The objective is expressed as a load or generation value (e.g. shed 100kW) for the load  
428 profile of the DR Resource for a specific interval or series of intervals.

429 The price message expresses the price for an interval or intervals as an absolute real time  
430 price or a price relative to the current tariff price.

431 The direct load control message includes an on/off or set point (e.g. set thermostat to  
432 80 degrees).

433 The Event Notification message can contain one or more of the three signal types.

434 **Preconditions:**

- 435     • The DR Resource and DR Controlling Entity have all of the necessary network  
436 connections available.
- 437     • The party with ownership, controlling interest or administrative responsibilities  
438 for the Resource has enrolled in a Demand Response Program that is administered  
439 by the DR Controlling Entity.

440 **Minimal Guarantees:**

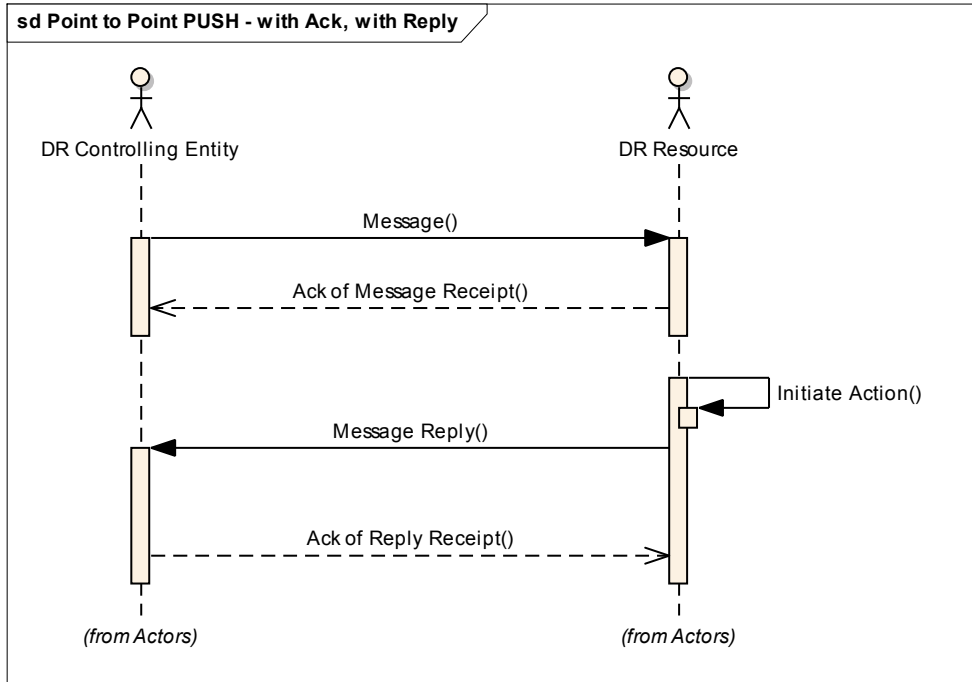
- 441     • The DR Controlling Entity does not reveal any information that could allow  
442 another party to present false identification, or intercept or alter future messages  
443 sent to the DR Resource.
- 444     • The DR Resource does not process any invalid data.

445 **Success Guarantees:**

- 446     • The DR Resource receives and replies to an Event notification.

447 **Trigger:**

448 The trigger for this use case could be from multiple sources depending on the span of  
449 control of the DR Controlling Entity and the DR Program definition. The originating  
450 Event message could be a manual response from a Market Operator based on forecasted  
451 or current conditions. The event could be a manual or automated response to a program  
452 rule regarding time of day and outside air temperature, or any number of options. If the  
453 DR Controlling Entity is a DR Aggregator, it could be a manual or automated response to  
454 an event signal from a Market Operator.



455

456

**Diagram: Use Case 2: DR Event Notification**

457

**458 Main Success Scenario:**

459 1: A DR Controlling Entity sends a DR Event Notification (a.k.a DR Dispatch) to the DR  
 460 Resource. [A DR Event Notification could be for a new DR Event, an update or  
 461 cancellation of a pending or current DR Event.]

462 2: The DR Resource receives the DR Event Notification and may or may not choose to  
 463 send an acknowledgement of receipt reply.

464 3: The DR Resource assesses the validity of the Event Notification and initiates action  
 465 necessary to send a valid reply.

466 4: The DR Resource sends a reply with an affirmative acknowledgement, notice to opt  
 467 out, or failure message.

468 5: The DR Controlling Entity receives the reply and may or may not choose to send an  
 469 acknowledgement of receipt reply.

470 **Use Case 3: DR Controlling Entity Notifies DR Resource of DR Event –**  
471 **(Broadcast)**

472 **Use Case Description:** This interaction is used to dispatch DR Resources. The initiator  
473 of the interaction is the DR Controlling Entity. The initiating event message is directed to  
474 multiple DR Resources. Identification of the applicable Resources could be one of  
475 several groups such as geographic location. The dispatch can convey an objective, price  
476 or direct load control signal.

477 The objective is expressed as a load or generation value (e.g. shed 100kW) for the load  
478 profile of the DR Resource for a specific interval or series of intervals.

479 The price message expresses the price for an interval or intervals as an absolute real time  
480 price or a price relative to the current tariff price.

481 The direct load control message includes an on/off or set point (e.g. set thermostat to  
482 80 degrees).

483 The Event Notification message can contain one or more of the three signal types.

484

485 **Preconditions:**

- 486 • The DR Resource and DR Controlling Entity have all of the necessary network  
487 connections available.

488 **Minimal Guarantees:**

- 489 • The DR Controlling Entity does not reveal any information that could allow  
490 another party to present false identification, or intercept or alter future messages  
491 sent to the DR Resource.
- 492 • The DR Resource does not process any invalid data.

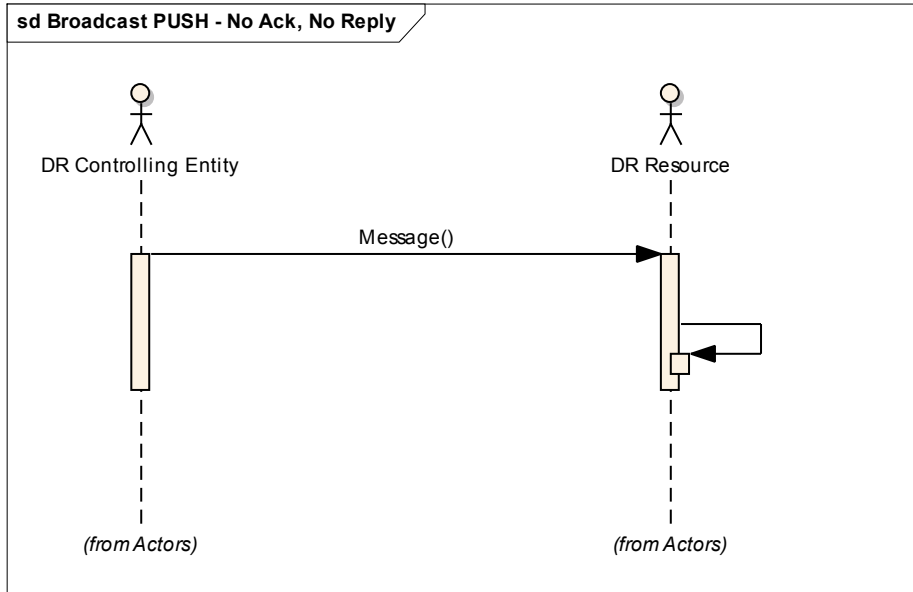
493 **Success Guarantees:**

- 494 • The DR Resource receives price notification and is able to respond and perform  
495 load-shed or generation based on the current price conditions and best economic  
496 interests of the DR Resource.

497

498 **Trigger:**

499 The trigger for this use case could be from multiple sources depending on the span of  
500 control of the DR Controlling Entity and the DR Program definition. It could be a manual  
501 or automated process.



502

503

**Diagram: Use Case 3: DR Event Notification – Broadcast**

504 **Main Success Scenario:**

505 1: A DR Controlling Entity broadcasts a DR Event message to multiple DR Resources.

506 2: The DR Resource receives the DR Event message.

507 3: The DR Resource initiates action to reduce load or generate power.

508

509

510

511 ***Use Case 4: DR Resource Requests New DR Event from DR Controlling***  
512 ***Entity (Point-to-point Pull)***

513 **Use Case Description:** This interaction is used to dispatch DR Resources based on a  
514 request from the DR Resource. The Event Notification message can contain one or more  
515 of the three signal types: objective, price or direct load control message.

516 The objective is expressed as a load or generation value (e.g. shed 100kW) for the load  
517 profile of the DR Resource for a specific interval or series of intervals.

518 The price message expresses the price for an interval or intervals as an absolute real time  
519 price or a price relative to the current tariff price.

520 The direct load control message includes an on/off or set point (e.g. set thermostat to 80  
521 degrees).

522 **Preconditions:**

- 523       • The DR Resource and DR Controlling Entity have all of the necessary network  
524 connections available.
- 525       • The party with ownership, controlling interest or administrative responsibilities  
526 for the Resource has enrolled in a Demand Response Program that is administered  
527 by the DR Controlling Entity.

528 **Minimal Guarantees:**

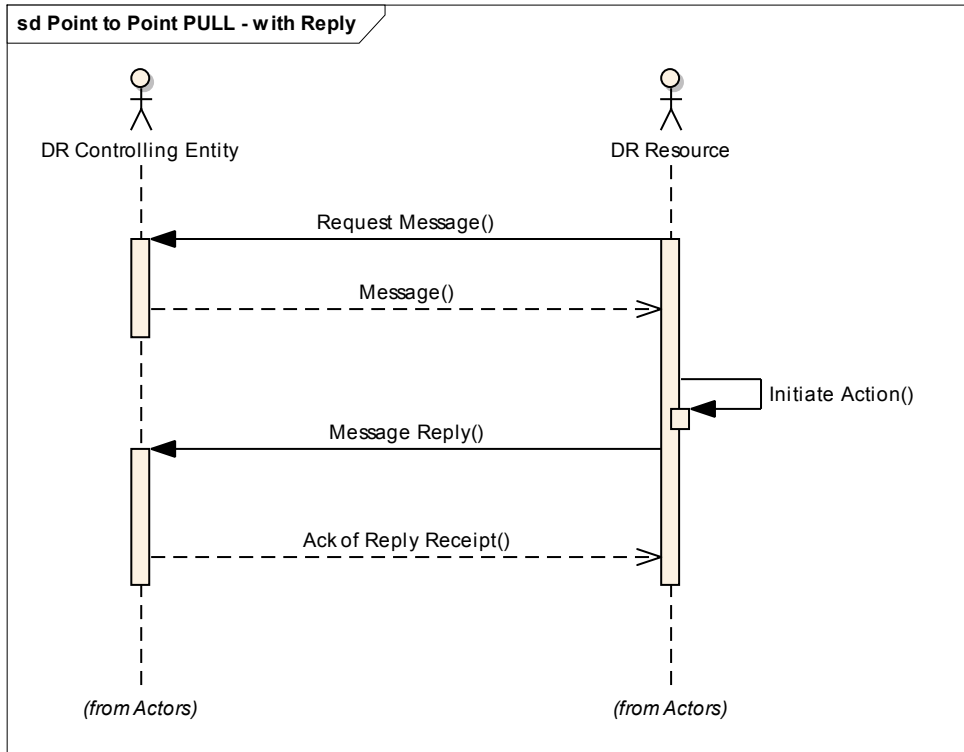
- 529       • The DR Resource does not reveal any information that would allow another party  
530 to present false identification or intercept messages as a DR Resource.
- 531       • The DR Controlling Entity does not process invalid requests.

532 **Success Guarantees:**

- 533       • The DR Resource receives an Event notification and is able to respond and  
534 attempt to perform based on the content and intentions of the DR Event signal and  
535 provide feedback to the DR Controlling Entity.

536 **Trigger:**

537 The trigger for this use case is a request from the DR Resource. The request is sent based  
538 on the temporal aspects of the specific Demand Response Program and enrollment  
539 agreements between the DR Controlling Entity and DR Resource. For example, for a  
540 day-ahead program the request is sent for the next day's event.



541

542 **Diagram: Use Case 4: DR Resource Requests DR Controlling Entity for New DR Event**

543 **Main Success Scenario:**

544 1: The DR Resource requests a DR Event Notification from the DR Controlling Entity.

545 2: The DR Controlling Entity receives a Request for a DR Event Notification.

546 3: The DR Controlling Entity responds with the Event Notification.

547 4: DR Resource receives the DR Event Notification.

548 5: The DR Resource assesses the validity of the Event Notification and initiates action  
549 necessary to send a valid reply.

550 6: The DR Resource replies to receipt of the DR Event Notification.

551 7: The DR Controlling Entity receives the reply and may or may not choose to send an  
552 acknowledgement of receipt reply.

553 **Use Case 5: DR Resource Requests New DR Event from DR Controlling**  
554 **Entity (Anonymous Pull)**

555 **Use Case Description:** This interaction is used to dispatch DR Resources based on a  
556 request from the DR Resource. The identity of the DR Resource is unknown to the DR  
557 Controlling Entity. The Event Notification message can contain one or more of the three  
558 signal types: objective, price or direct load control message.

559 The objective is expressed as a load or generation value (e.g. shed 100kW) for the load  
560 profile of the DR Resource for a specific interval or series of intervals.

561 The price message expresses the price for an interval or intervals as an absolute real time  
562 price or a price relative to the current tariff price.

563 The direct load control message includes an on/off or set point (e.g. set thermostat to 80  
564 degrees).

565 **Preconditions:**

- 566
  - The DR Resource and DR Controlling Entity have all of the necessary network  
567 connections available.

568 **Minimal Guarantees:**

- 569
  - The DR Resource does not reveal any information that would allow another party  
570 to present false identification or intercept messages as a DR Resource.

- 571
  - The DR Controlling Entity does not process invalid requests.

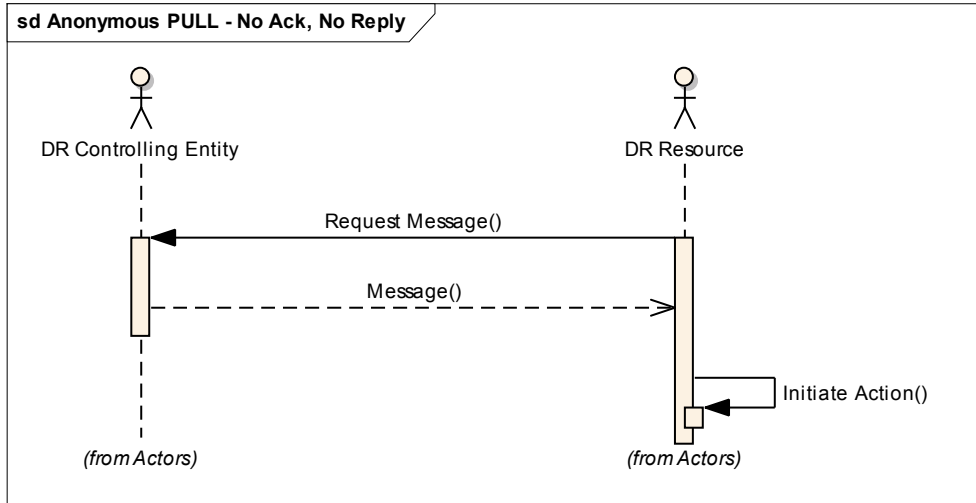
572 **Success Guarantees:**

- 573
  - The DR Resource receives an Event notification and is able to respond and  
574 perform based on the content and intentions of the DR Event signal and provide  
575 feedback to the DR Controlling Entity.

576 **Trigger:**

577 The trigger for this use case is a request from the DR Resource. The request is sent based  
578 on the temporal aspects of the specific Demand Response Program and enrollment  
579 agreements between the DR Controlling Entity and DR Resource. For example, for a  
580 day-ahead program the request is sent for the next day's event.





581

582

583

**Diagram: Use Case 5: Anonymous DR Resource Requests DR Controlling Entity for New DR Event**

584

**Main Success Scenario:**

585

1: The DR Resource requests a DR Event Notification from the DR Controlling Entity.

586

2: The DR Controlling Entity receives a Request for a DR Event Notification.

587

3: The DR Controlling Entity responds with the Event Notification.

588

4: DR Resource receives the DR Event Notification.

589

590 **Use Case 6: DR Controlling Entity Schedules DR Resource for Periodic**  
591 **Feedback (Point-to-point Push)**

592 **Use Case Description:** This interaction is used by the DR Resource to notify the DR  
593 Controlling Entity of the Resource's status or state of the Resource during the event. The  
594 feedback is provided continuously during the event in intervals agreed upon by the  
595 parties. The performance feedback contains information such as the load profile response  
596 characterization of the DR Resource in response to getting the DR signal and information  
597 about the near real time electricity usage of the DR Resource.

598 This use case is comprised of three interaction patterns:

- 599 ○ Initiate periodic feedback.
- 600 ○ Provide periodic feedback.
- 601 ○ Change (terminate is a type of change) feedback request.

602 **Preconditions:**

- 603 ● The DR Resource and DR Controlling Entity have all of the necessary network  
604 connections available.
- 605 ● The party with ownership, controlling interest or administrative responsibilities  
606 for the Resource has enrolled in a Demand Response Program that is administered  
607 by the DR Controlling Entity.

608 **Minimal Guarantees:**

- 609 ● The DR Resource does not reveal any information that could allow another party  
610 to present false identification, or intercept or alter future messages sent to the DR  
611 Controlling Entity.
- 612 ● The DR Controlling Entity does not process any invalid data.

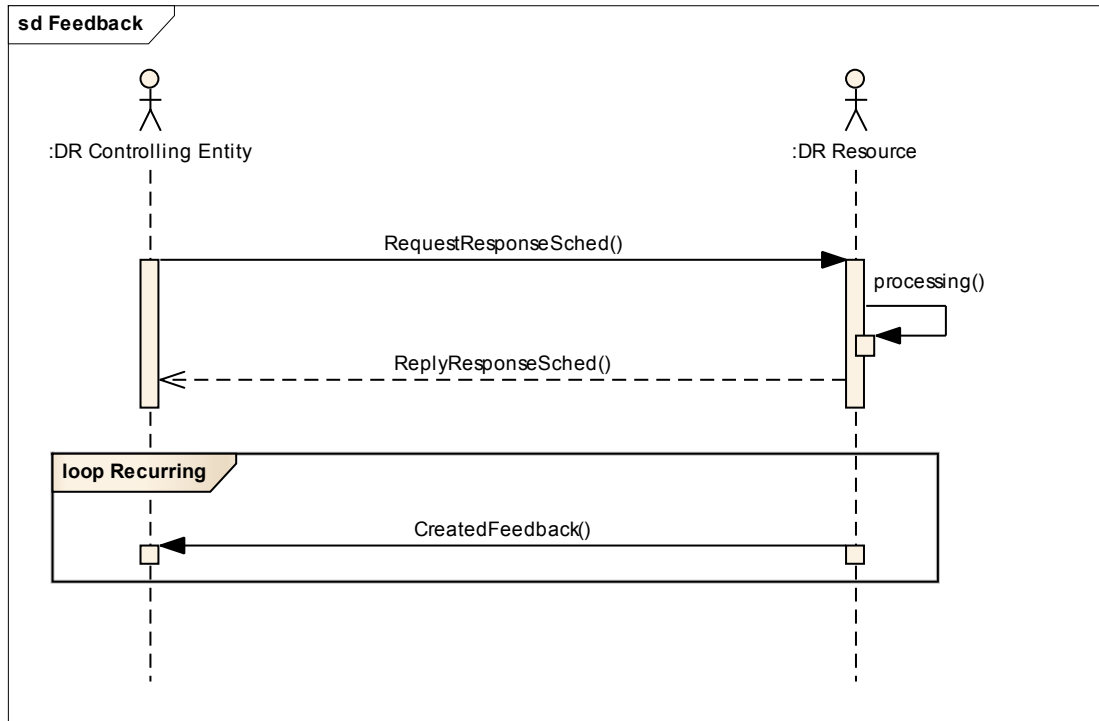
613 **Success Guarantees:**

- 614 ● The DR Controlling Entity receives continuous and timely (real time or near real  
615 time) feedback from the DR Resource during the entire Event performance  
616 window.

617 **Trigger:**

618 The trigger for this use case is based on an agreed upon reporting interval associated with  
619 a DR Event. Generally, the DR Controlling Entity will initiate the feedback interactions  
620 at the start of an Event.

621



622

623

624

**Diagram: Use Case 6: DR Controlling Entity Schedules DR Resource for Periodic Feedback**

625

**Main Success Scenario:**

626

**1. Initiate or terminate periodic feedback:**

627

1.1: A DR Controlling Entity sends a Feedback schedule request to a DR Resource.

628

1.2: A DR Resource receives a Feedback schedule request from a DR Controlling Entity.

629

1.3: A DR Resource assesses the request and initiates action to provide a reply and

630

subsequent feedback messages.

631

**2. Provide periodic feedback**

632

2.1: A DR Resource periodically summarizes performance status using an interval

633

defined in the Feedback schedule request.

634

2.3: A DR Resource sends a Feedback message to a DR Controlling Entity containing the

635

information assembled in the previous step.

636

2.4: The DR Controlling Entity Receives a Feedback message from a DR Resource.

637 ***Use Case 7: DR Resource Notifies DR Controlling Entity of Event***  
638 ***Performance with Feedback by Request (Point-to-point Pull)***

639

640 **Use Case Description:** This interaction is used by the DR Resource to notify the DR  
641 Controlling Entity of the Resource’s status or state of the Resource during the event. The  
642 feedback is provided as requested by the DR Controlling Entity. The performance  
643 feedback contains information such as the load profile response characterization of the  
644 DR Resource in response to getting the DR signal and information about the near real  
645 time electricity usage of the DR Resource. This case differs from the prior use case in  
646 that the request from the DR Controlling Entity is for a single reply without a recurring  
647 schedule.

648 **Preconditions:**

- 649       • The DR Resource and DR Controlling Entity have all of the necessary network  
650 connections available.
- 651       • The party with ownership, controlling interest or administrative responsibilities  
652 for the Resource has enrolled in a Demand Response Program that is administered  
653 by the DR Controlling Entity.

654 **Minimal Guarantees:**

- 655       • The DR Resource does not reveal any information that could allow another party  
656 to present false identification, or intercept or alter future messages sent to the DR  
657 Controlling Entity.
- 658       • The DR Controlling Entity does not process any invalid data.

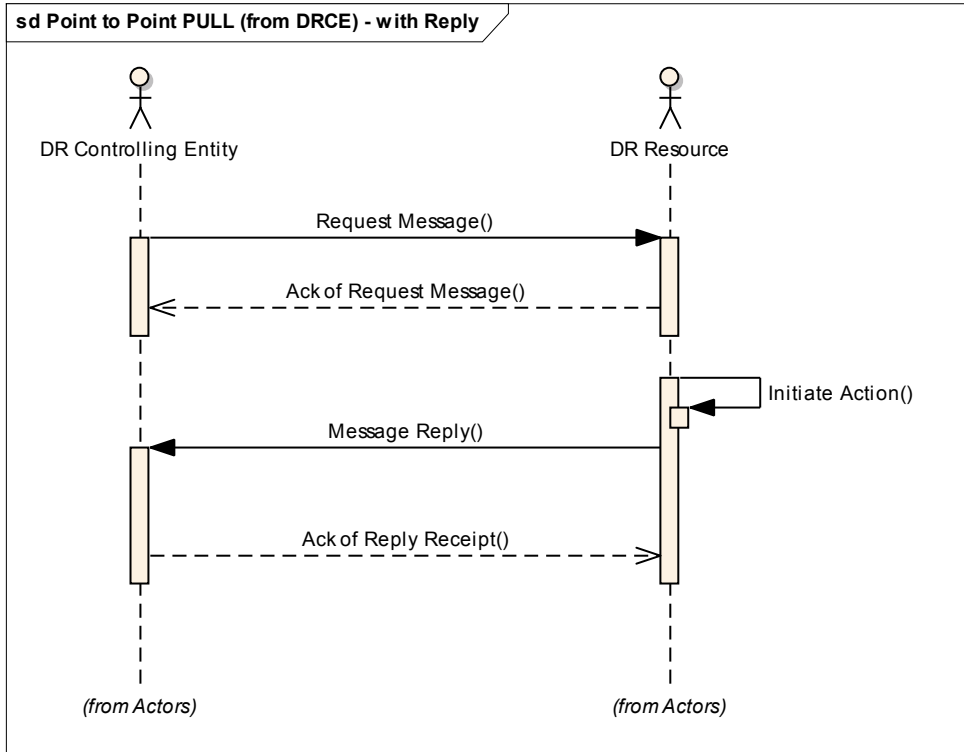
659 **Success Guarantees:**

- 660       • The DR Controlling Entity receives timely (real time or near real time) feedback  
661 from the DR Resource.

662 **Trigger:**

663 The trigger for this use case is based on an agreed upon reporting interval.

664



665

666

667

**Diagram: Use Case 7: DR Resource Notifies DR Controlling Entity of Event Performance (Feedback)**

668

**Main Success Scenario:**

669

1: A DR Controlling Entity sends a Feedback request to a DR Resource.

670

2: A DR Resource receives a Feedback request from a DR Resource.

671

3: A DR Resource retrieves feedback information.

672

4: A DR Resource sends a Feedback message to a DR Controlling Entity.

673

5: The DR Controlling Entity Receives a Feedback message from a DR Resource.

674 **Use Case 8: DR Resource Notifies DR Controlling Entity of Event**  
675 **Performance with Feedback Self-Scheduled (Point-to-point Push)**

676 **Use Case Description:** This interaction is used by the DR Resource to notify the DR  
677 Controlling Entity of the Resources status or state of the Resource during the event. The  
678 feedback is provided as scheduled by the DR Resource without scheduling influences  
679 from the DR Controlling Entity. The performance feedback contains information such as  
680 the load profile response characterization of the DR Resource in response to getting the  
681 DR signal and information about the near real time electricity usage of the DR Resource.

682 **Preconditions:**

- 683 • The DR Resource and DR Controlling Entity have all of the necessary network  
684 connections available.
- 685 • The party with ownership, controlling interest or administrative responsibilities  
686 for the Resource has enrolled in a Demand Response Program that is administered  
687 by the DR Controlling Entity.
- 688 • The DR Resource is a self-scheduled Resource.

689 **Minimal Guarantees:**

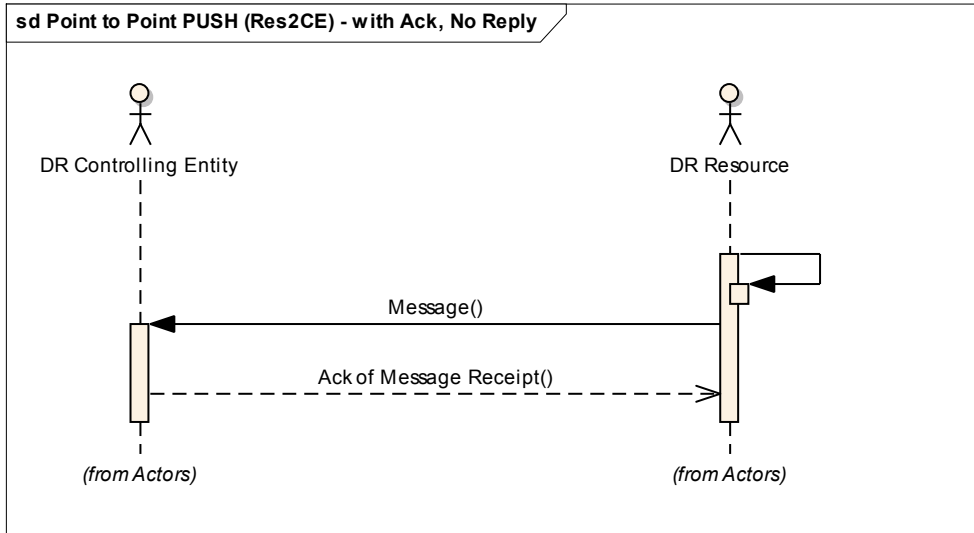
- 690 • The DR Resource does not reveal any information that could allow another party  
691 to present false identification, or intercept or alter future messages sent to the DR  
692 Controlling Entity.
- 693 • The DR Controlling Entity does not process any invalid data.

694 **Success Guarantees:**

- 695 • The DR Controlling Entity receives timely (real time or near real time) feedback  
696 from the DR Resource.

697 **Trigger:**

698 The trigger for this use case is based on an agreed upon reporting interval.  
699



700

701

702

**Diagram: Use Case 8: DR Resource Notifies DR Controlling Entity of Event Performance with Feedback Self-Scheduled**

703

**Main Success Scenario:**

704

1. DR Resource accumulates Feedback information.

705

2. DR Resource sends Feedback to DR Controlling Entity.

706

3. DR Controlling Entity receives Feedback message from DR Resource.

707

## 3 Failure Analysis

---

709 The approach used to create this security profile defines the functions of OpenADR  
710 systems based on defined abstract roles and use cases. The development of the use cases  
711 and the definition of roles take into account a foundational set of security and operational  
712 objectives that is also used in the failure analysis. The failure analysis begins with a  
713 description of the process for identifying failures in Section 3.1 below. A brief overview  
714 of the foundational security and operational objectives is presented in Section 3.2 and a  
715 more detailed view of the identified failures is presented in Section 3.3.

### 716 3.1 Failure Analysis Process

717 The failure identification and analysis process is loosely based on conducting a Failure  
718 Modes and Effects Analysis (FMEA) on the OpenADR logical architecture presented in  
719 Section 2.1, however the analysis was performed with a security bias to failure  
720 identification. A FMEA is a qualitative procedure for analyzing potential system failures  
721 and their associated modes as a function of assemblies, subassemblies, components,  
722 subcomponents, and so forth. This process leads to a quantification of the number and  
723 severity of failures and to an understanding of their impact on system stability and  
724 operations. With this information, a cost-benefits analysis can then be conducted to  
725 eliminate those risks that are considered catastrophic and accept those risks that are  
726 considered acceptable/manageable during operations. In general, the protocol for  
727 conducting a FMEA includes:

- 728 1. Establish a comprehensive understanding of the enterprise/system/process under  
729 consideration by gathering all relevant information and invoking a proper review  
730 process.



- 731 2. Based on (1), develop a functional hierarchy of roles and responsibilities.
- 732 3. At an appropriate level of abstraction, identify all failures, effects, consequences,
- 733 and initiating events associated with each role.
- 734 4. Identify and analyze controls for each failure, its effects and consequences, or
- 735 both.
- 736 5. Qualitatively assign a risk for each failure pairing through a Risk Priority Number
- 737 (RPN) calculation.
- 738 6. Perform a cost-benefit evaluation for controls (with respect to risk reduction) and
- 739 provide a balanced decision process for corrective action implementation.

740 For the OpenADR security profile, the failure analysis process centers on steps 1-4. Steps  
 741 5-6 must account for the specific needs of the organization that owns or operates the  
 742 system, so the outcome of these steps is necessarily specific to that organization and is  
 743 not covered by this profile.

744

745 Given the system elements and their roles (Section 2) and relationships (Section 2.3), the  
 746 set of role/failure pairings are applied to a finite set of use cases (Section 2.4) to provide a  
 747 descriptive analysis of how the OpenADR system may fail. The resulting list of failures  
 748 serves as a basis for (1) justifying the set of selected controls, as each control must  
 749 address an identified failure, and (2) identifying and remediating gaps in the selected  
 750 controls, as each failure must be addressed by at least one control.

751 For this security profile, failure analysis centers on the roles and use cases defined in  
 752 Sections 2 and 2.4 and the impact of potential failures on an OpenADR system. This  
 753 process is used to identify OpenADR system issues, which are in turn used as inputs to  
 754 assign failure incidents for the pairing of each role with each step of each use case. Each  
 755 step of each use case is examined for potential failures against the security and  
 756 operational objectives with respect to each role. All of the identified failures are then  
 757 aggregated and generalized across all use cases.

### 758 **3.2 Security and Operational Objectives**

759 The goal of this document is to establish a cyber environment in which an OpenADR  
 760 system can successfully and securely operate. Meeting this goal requires that a number of  
 761 security and operational objectives that support that goal are achieved. This section  
 762 defines the assumptions made regarding the operational context for OpenADR systems  
 763 and how the systems will be operated in the context of a security analysis, and then  
 764 presents a set of security objectives around which the remainder of the document  
 765 revolves.

766 **3.2.1 Contextual Assumptions**

767 This document assumes that the following conditions, largely or wholly outside of the  
768 organization’s control, apply to the environment in which Open ADR systems will be  
769 deployed:

- 770 1. Load shedding/Generation capacity and ramp rate vary from DR Asset to  
771 DR Asset. Risks associated with the compromise of each DR Asset will be  
772 different depending on the compromised DR Asset’s capabilities.
- 773 2. DR Resource/Asset’s response to DR Event(s) is uncertain due to DR  
774 Resource/Asset’s ability to opt-out of DR Event(s) at any time. Open ADR  
775 is not intended to be part of critical grid operations unless DR  
776 Resource/Asset gives full commitment to accurately follow DR  
777 instructions.
- 778 3. All participants will act to maximize their own profits. For example,  
779 possible behaviors such as bidder collusion or the use of grid reliability  
780 information in the bidding process, unless such behaviors are specifically  
781 prohibited by the organization.
- 782 4. DR Resource can be used to enhance grid reliability or to facilitate market  
783 operations. However, regulation and legal agreements require a separation  
784 between electric system operations and market functions.
- 785 5. DR Controlling Entity has little to no control over the physical  
786 environment in which DR Assets reside in.

787

788 **3.2.2 Core Operational Assumptions**

789 This document assumes that organizations will operate Open ADR systems in the  
790 following manner:

- 791 1. Open ADR services shall be provided via existing, well established IP  
792 based communication protocols.
- 793 2. The DRCE shall provide messaging standards that will be used to  
794 exchange all DR related information. In addition, all participants will  
795 adhere to these standards.
- 796 3. Open ADR systems will operate in such a way as to minimize the need for  
797 human intervention as much as possible.
- 798 4. DR Resources are responsible for physical control of assets under their  
799 purview.
- 800 5. The triggers for DR Event(s) may not be predictable or may even lie  
801 outside the DRCE’s control. It is presumed that DRCE will receive  
802 instructions from authoritative entities at unpredictable times (e.g. during

803 oscillations in the grid due to external causes such as transmission line  
804 faults).

805

### 806 **3.2.2 Security Principles**

807 These objectives served as the “ground rules” for the Open ADR systems and helped with  
808 use case development and failure identification. The 13 objectives are as follows:

- 809 1. Security controls should have minimal impact on the primary mission of  
810 the Open ADR.
- 811 2. DR Resource/Asset should only accept and respond to authorized and  
812 valid DR messages in a timely manner.
- 813 3. Open ADR participants should only perform as intended.
- 814 4. Open ADR should employ different types of security measures depending  
815 on the risks associated with different types of DR events in order to  
816 facilitate efficient operations of Open ADR applications (see Figure 1  
817 below).
  - 818 a. if personally identifiable information (PII) is introduced to the  
819 signal, confidentiality becomes increasingly important.
  - 820 b. if Direct Load Control is introduced to the signal, integrity  
821 becomes increasingly important.
  - 822 c. if faster response times are required, availability and low latency  
823 become increasingly important.
- 824 5. No unauthorized or unauthenticated download of software (firmware,  
825 configuration, etc.) shall be accepted by Open ADR system components.
- 826 6. Open ADR systems should be able to determine the source of DR event  
827 messages and its intended recipients at all times.
- 828 7. All control activity (configuration changes, access requests, etc.) on the  
829 Open ADR system shall be auditable.
- 830 8. The integration of Open ADR systems should not expose other utility  
831 systems to unauthorized access or attack.
- 832 9. Only the authorized personnel should have physical access to Open ADR  
833 system devices.
- 834 10. Open ADR systems should support non-repudiation of all transactions  
835 between the DR controlling entity and DR Resource/Asset.
- 836 11. Asset owners must not rely on security measures outside their direct  
837 observation and control for protection from unauthorized access.

- 838 12. Users shall not be allowed to perform any action that falls outside of their  
839 assigned role.
- 840 13. Open ADR applications should not reveal sensitive, personally identifiable  
841 information.

842 **3.3 Failures**

843 Generic Failures defined in the Generic Failures Table are mapped to each uses case step  
 844 below.

845 **Table 1 - Generic Failures Mapped to Use Case Step**

-	Indicates the failure does NOT apply to this Use Case step
x	Indicates the failure DOES apply to this Use Case step

Failure #	UC1				UC2					UC3			UC4							UC5				UC6.1			UC6.2			UC7					UC8			
	S1	S2	S3	S4	S1	S2	S3	S4	S5	S1	S2	S3	S1	S2	S3	S4	S5	S6	S7	S1	S2	S3	S4	S1	S2	S3	S1	S2	S3	S1	S2	S3	S4	S5	S1	S2		
GF1	x	-	-	x	x	-	-	x	-	x	-	-	x	-	x	-	-	x	-	x	-	x	-	x	-	-	x	-	x	-	-	x	-	-	x	-	-	
GF2	-	x	-	-	-	x	-	-	x	-	x	-	-	x	-	x	-	-	x	-	x	-	x	-	-	-	x	-	x	-	-	x	-	-	x	-	x	
GF3	-	x	-	-	-	x	-	-	x	-	x	-	-	x	-	x	-	-	x	-	x	-	x	-	-	-	x	-	x	-	-	x	-	-	x	-	x	
GF4	-	-	x	-	-	-	x	-	-	-	-	x	-	-	-	-	x	-	-	-	-	-	-	-	-	x	x	-	-	-	-	x	-	-	-	-		
GF5	x	-	-	x	x	-	-	x	-	x	-	-	x	-	x	-	-	x	-	x	-	x	-	-	-	x	-	x	-	-	x	-	-	x	-	x		
GF6	x	-	-	x	x	-	-	x	-	x	-	-	x	-	x	-	-	x	-	x	-	x	-	-	-	x	-	x	-	-	x	-	-	x	-	x		
GF7	-	-	x	x	-	-	x	x	-	-	-	x	-	-	x	-	-	x	-	-	x	-	-	-	x	-	-	-	-	-	x	x	-	-	-	-		
GF8	x	-	-	x	x	-	-	x	-	x	-	-	x	-	x	-	-	x	-	x	-	x	-	-	-	x	-	x	-	-	x	-	-	x	-	x		
GF9	-	-	x	x	-	-	x	x	-	-	-	x	-	-	x	-	-	x	-	-	-	-	-	-	x	-	-	-	-	-	x	x	-	-	-	-		
GF10	x	-	-	x	x	-	-	x	-	x	-	-	x	-	x	-	-	x	-	x	-	x	-	-	-	x	-	x	-	-	x	-	-	x	-	x		
GF11	-	-	x	x	-	-	x	x	-	-	-	x	-	-	x	-	-	x	-	-	x	-	-	-	x	-	-	-	-	-	x	x	-	-	-	-		
GF12	x	-	-	x	x	-	-	x	-	x	-	-	x	-	x	-	-	x	-	x	-	x	-	-	-	x	-	x	-	-	x	-	-	x	-	x		
GF13	-	-	x	x	-	-	x	x	-	-	-	x	-	-	x	-	-	x	-	-	x	-	-	-	x	-	-	-	-	-	x	x	-	-	-	-		
GF14	-	-	x	x	-	-	x	x	-	-	-	x	-	-	x	-	-	x	-	-	x	-	-	-	x	-	-	-	-	-	x	x	-	-	-	-		
GF15																																						
GF16																																						
GF17	-	-	x	-	-	-	x	-	-	-	-	x	-	-	x	-	-	-	-	x	-	-	-	-	x	-	-	x	-	-	x	-	-	x	-	-		
GF18																																						
GF19	-	-	-	-	-	-	x	-	-	-	-	x	-	-	-	-	x	-	-	-	-	-	-	-	-	x	-	-	-	-	x	-	-	-	-	-		

846

847

848 **Generic Failures**

849 Generic failures apply to all the roles with in OpenADR.

850

851

**Table 2 Generic Failures**

Failure ID	Definition	Explanation	Examples
F1	<Role> does not send a message in a timely manner.	The transmission of a message must occur within a particular span of time but the role fails to start the transmission within that span.	DRCE fails to notify DR Asset of upcoming DR Event(s) during the notification period.
F2	<Role> does not receive a message in a timely manner due to flooding or jamming attacks (Denial of Service attacks) on the	The reception of a message must occur within a particular span of time, but the role fails to initiate reception of the message in that time due to	1) DR Asset fails to receive information regarding upcoming DR Event(s) due to DoS attack on owner's

	communications channel.	DoS attacks.	other assets. 2) DRCE fails to receive registration request due to DoS attack on DRCE server.
<b>F3</b>	<Role> does not receive a message in a timely manner due to internal errors.	The reception of a message must occur within a particular span of time, but the role fails to initiate reception of the message in that time due to internal errors such as receive buffer overflow.	1) DR Asset fails to receive information regarding upcoming DR Event(s) due to a compromised NIC. 2) DRCE fails to receive registration request due to compromised software/configuration.
<b>F4</b>	<Role> fails to execute action in a timely fashion after receiving a legitimate message	The role fails to execute a command within the required span of time.	DR Asset fails to respond to DR Event(s) after acknowledgment and commitment.
<b>F5</b>	<Role> sends a message to an incorrect recipient	The role addresses a message to recipients that do not require the message or are incapable of processing the message.	1) DRCE sends a DR Event notification to a DR Asset who is not enrolled in that DR Event. 2) DR Asset sends registration request to a destination other than the DRCE.
<b>F6</b>	<Role> sends an unauthorized message	The role transmits a message in spite of a prohibition against doing so or in violation of limits on the sender's use of network resources.	1) DR Asset sends a DR Event notification message to another DR Asset. 2) DRCE sends a DR Event to a DR Asset that is not enrolled in the corresponding program.
<b>F7</b>	<Role> receives and responds to a message from an unauthorized source	The role accepts a message that comes from a source that is not authorized to send information to the role.	1) DR Asset responds to a DR Event which was initiated by another DR Asset. 2) DR Asset responds to a DR Event for a program in which it is not enrolled. 3) DRCE registers a faulty (i.e., imposter) DR Asset.

<b>F8</b>	<Role> sends an incorrect type of message	The role sends a message containing information other than what is required by the recipient.	1) DR Asset sends acknowledgement instead of registration request. 2) DRCE sends Objective Event instead of Load Control Event.
<b>F9</b>	<Role> receives and processes an incorrect type of message	The role receives a message other than the type that is expected, but processes that message regardless.	DR Asset receives and processes a Load Control Event, when it should only respond to Pricing Events.
<b>F10</b>	<Role> sends an incorrectly formatted message	The role transmits a message using a protocol or message format that is not understood by the recipient and therefore cannot be processed by the recipient.	DRCE sends a DR Event notification message which violates the messaging standards defined by the organization. Such messages cannot be processed by the recipient.
<b>F11</b>	<Role> receives and processes a corrupted/wrong message.	The role processes a message with an expected type from a legitimate source but that is ill formed or has been manipulated in transit (e.g. Man-In-the-middle attack).	DR Asset responds to a DR Event message that has been modified in transit by an unauthorized third party.
<b>F12</b>	<Role> sends a spurious message	The role transmits a message that is not required or expected by a legitimate recipient.	.DR Asset sends an acknowledgement for an unpublished DR Event.
<b>F13</b>	<Role> receives and processes a spurious message	The role receives a message that is not expected but processes the message regardless.	DRCE receives affirmative acknowledgement for an unpublished Event and incorporates it into performance calculations.
<b>F14</b>	<Role> accepts and applies corrupted configuration file	The role applies new configuration settings regardless of their integrity or appropriateness in the context of the device's mission.	DR Asset is configured to independently generate and transmit DR Event(s) to other DR Assets.
<b>F15</b>	<Role> fails to protect data storage from being	<Role> fails to protect against data being modified or	The List of scheduled DR Events is

	corrupted	destroyed and the modification or destruction is not detected, is irreversible, or both	corrupted by a misconfigured process, resulting in an unusable schedule.
<b>F16</b>	<Role> fails to protect information or resources against unauthorized access and manipulation	The role allows a user or device to read or modify data without regard for their credential and access rights.	An unauthorized entity is able to access and modify the list of scheduled DR Events.
<b>F17</b>	<Role> fails to accept authorized and valid message	The role fails to recognize the credentials of a device or individual, improperly marks the message as erroneous, or both, and thereby improperly disregards messages from that device or individual.	DR Resource rejects a valid DR Event message due to authentication software errors.
<b>F18</b>	<Role> fails to prevent exhaustion of storage space.	The role fails to provide sufficient resources to storing data and the exhaustion of storage goes unnoticed.	The list of scheduled DR Events exceeds storage space, causing unpredictable loss of data.
<b>F19</b>	<Role> executes wrong action based on changes to its operational parameters, its data, or its internal state	The role is made to take action or inaction that is inappropriate to its mission or operation state. This can occur when software is corrupted prior to being placed into a particular device.	DR Asset is instructed to increase its power consumption during high price periods or to decrease its power consumption during low price periods, or both.

852

853

854

855 ***Specific Failures***

856 Specific Failures are failures associated with specific OpenADR roles that are critical to  
 857 the mission or operational state of the system.

858

Failure ID	Definition	Explanation
------------	------------	-------------



<b>SF1</b>	DR Resource is physically unable to receive or respond to DR event signals	DR Resource is physically removed or damaged due to equipment failures or malicious activities and cannot respond to DR Event(s).
<b>SF2</b>	Communication and storage devices of DRCE are physically compromised	A malicious user gains physical access to communication and storage devices.
<b>SF3</b>	<Role> is synchronized to a wrong time source	Either DRCE or DR Resource is synchronized to a wrong time source
<b>SF4</b>	DR Resource responds to DR Event(s) that has already ended	This may happen due to poor configuration settings or as the result of replay attacks.
<b>SF5</b>	DR Resource denies receiving DR event information	DR Resource/Asset does not respond to scheduled DR Event(s) and then denies receiving the related information.
<b>SF6</b>	Sensitive, personally identifiable information is revealed while DR messages are in transit.	A malicious attacker gains sensitive information by eavesdropping on DR related messages in transit.
<b>SF7</b>	DR Resource enrolls in a DR program multiple times assuming multiple identities.	Same DR Resource/Asset enrolls in a DR program multiple times pretending as if they are different physical entities attempting to gain financial profit.

859

## 860 **4 Security Controls**

---

861

862 This section defines the set of recommended security controls for OpenADR systems and  
863 components as that satisfy the functionality of the roles and use cases delineated earlier in  
864 this document. Many of the security controls in this document are inspired by and  
865 intended to cover the technical requirements found in NIST IR 7628 as applied to  
866 Demand Response technology and related systems. The controls presented herein may  
867 then, in turn, be satisfied by communications protocol definition-level standards and  
868 manufacturing specifications. This section defines the controls, and assigns the controls  
869 to roles.

### 870 **4.1 Scope of Security Controls**

871 The scope of network topology of OpenADR systems defined in this document is limited  
872 to the interactions between a paired DR Controlling Entity and DR Resource over a  
873 public (Internet) or private network. The Network Architecture at these points should  
874 follow best practices for securing internal systems. The specific practices are out of scope  
875 of this document. Numerous documents on best practices are available on the NIST  
876 Computer Security Resource Center (<http://csrc.nist.gov/publications/index.html>), and are  
877 summarized in “Generally Accepted Principles and Practices for Securing Information  
878 Technology Systems” (<http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf>).

879 Securing internal systems is also addressed by corporate or other organizational policies  
880 that are also out of scope. The process for tailoring security controls to an organization

881 are outlined in Section 3.3 of “NIST SP 800-53 – Recommended Security Controls for  
882 Federal Information Systems and Organizations”<sup>7</sup> This includes “Specifying  
883 organization-defined parameters in the security controls via explicit assignment and  
884 selection statements to complete the definition of the tailored baseline”<sup>7</sup>. An example of  
885 an organization defined parameter as used in a control is:

886 “SC-5 DENIAL OF SERVICE PROTECTION

887 Control: The information system protects against or limits the effects of the following  
888 types of denial of service attacks: [Assignment: organization-defined list of types of  
889 denial of service attacks or reference to source for current list].”<sup>7</sup>

890 **4.2 Control Definitions**

891 The process for defining the controls in this document is based on an analysis of the  
892 roles, use cases, and failures defined in this profile along with careful examination of the  
893 NIST IR 7628, the WAMPAC Security Profile, Distribution Management Security  
894 Profile, and other collections of security standards and best practices. The process for  
895 deriving the controls includes the following steps (with natural iteration and review):

- 896 1. Examine the failures and associated controls from the WAMPAC Security Profile  
897 for similarities to the failures as defined in this document and for potential re-use  
898 of control material.
- 899 2. Re-write selected controls from the WAMPAC Security Profile to apply to  
900 OpenADR systems. Verify, augment, or correct the mapping of each re-written  
901 control to the OpenADR failures.
- 902 3. Examine the list of OpenADR failures for complete coverage. Compose new  
903 controls as needed to ensure all OpenADR failures are addressed.
- 904 4. Explicitly document the applicability of each control to roles or network  
905 segments. Tailor and/or split controls where necessary to accommodate  
906 implementation and environmental constraints for each role or network segment.
- 907 5. Map each OpenADR control against the technical requirements in the NIST IR  
908 7628. Assess coverage of technical requirements in the NIST IR 7628 by  
909 OpenADR controls.
- 910 6. Modify OpenADR controls to complete coverage of individual NIST IR 7628  
911 requirements where appropriate. Document NIST IR 7628 requirements not  
912 completely covered along with reasoning.

913 This document does not attempt to cover general information technology cyber security,  
914 cyber security best practices for other control systems, or organizational-level cyber

---

<sup>7</sup> “NIST SP 800-53 – Recommended Security Controls for Federal Information Systems and Organizations” ([http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final\\_updated-errata\\_05-01-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf))

915 security requirements that would apply to all or multiple smart grid systems. Substantial  
916 guidance is already available on these subjects, and may be found in such documents as:

- 917 • COBIT – the Control Objectives for Information and related Technology is an IT  
918 governance framework and supporting toolset that allows managers to bridge the  
919 gap between control requirements, technical issues and business risks. COBIT  
920 enables clear policy development and good practice for IT control throughout  
921 organizations. COBIT emphasizes regulatory compliance, helps organizations to  
922 increase the value attained from IT, enables alignment and simplifies  
923 implementation of the COBIT framework. ([http://www.isaca.org/Knowledge-  
924 Center/COBIT/Pages/Overview.aspx](http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx))
- 925 • ISO 27000 series – consists of several parts numbering from 27001 – 27006 that  
926 provide a specification for an information security management system (ISMS).  
927 This work supersedes the BS7799 standard.  
928 ([http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnum  
929 ber=41933](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41933))
- 930 • ITIL (Information Technology Infrastructure Library) – ITIL is a widely adopted  
931 approach for IT Service Management. It provides a practical, no-nonsense  
932 framework for identifying, planning, delivering and supporting IT services to the  
933 business. (<http://www.itil-officialsite.com>)
- 934 • NIST SP 800-53 – Recommended Security Controls for Federal Information  
935 Systems and Organizations – provides guidelines for selecting and specifying  
936 security controls for information systems supporting the executive agencies of the  
937 federal government to meet the requirements of FIPS 200, Minimum Security  
938 Requirements for Federal Information and Information Systems. The guidelines  
939 apply to all components of an information system that process, store, or transmit  
940 federal information. ([http://csrc.nist.gov/publications/nistpubs/800-53-  
941 Rev3/sp800-53-rev3-final\\_updated\\_errata\\_05-01-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated_errata_05-01-2010.pdf))

942 This document’s primary point of reference for broader cyber security guidance is the  
943 NIST IR 7628, and as such, these controls do not address the requirements in the NIST  
944 IR 7628 that apply to organizational policy. The controls herein are strictly focused on  
945 detailed recommendations for building and implementing OpenADR systems and  
946 technology where guidance may not be found in other broadly accepted reference  
947 material.

948 The following tables define technical security controls that, if followed, will improve the  
949 security of an OpenADR system. The elements of each control include:

- 950 • Control ID: This ID is composed of the control's category and a sequence number  
951 within that category.
- 952 • Short Name: This is a unique string that concisely references the intent of the  
953 control.
- 954 • Definition: This is the text that defines the control itself.

955 • Reference(s): These are the requirements from the NIST IR 7628 that are  
 956 partially or fully satisfied by the control. Requirements listed in parenthesis are  
 957 not required by the NIST IR 7628, but are included here for completeness.

958 • Failure(s): These are the failures from Section 3.3 addressed by the control.

959  
 960

961 **4.2.1 Access Control**

962

**Table 3 – Controls: Access Control**

Control ID	Short Name	Definition	Reference(s)	Failure(s)
Access Control.01	Automated Account Management	<p>The system shall provide the means to authorize, establish, activate, modify, disable or remove accounts. These processes can be managed through a pre-established directory structure as long as the system is fully integrated with the directory structure; otherwise the system must utilize a self contained standards based structure that provides all of the abilities previously listed. In either case the method used must provide the ability to automatically log any activities performed on accounts.</p> <p>The organization shall review all access on a recurring basis in accordance with a frequency determined by the organization.</p> <p>The system shall notify role when users are terminated, modified, or transferred to ensure the system is also is appropriately updated.</p>	SG.AC-3 SG.AU-15	F6 F16
Access Control.02	Least Privilege	<p>The organization shall grant each user, process, or service within a system the most restrictive set of privileges needed for the performance of authorized tasks.</p> <p>The system must allow for the ability to manage access and authorization based on roles established in accordance with the organizations policies and standards.</p> <p>Each role must have the ability to be individually managed and controlled.</p> <p>All access and authorization shall be based on the role to which an identity is associated.</p> <p>A separate and distinct security role shall be provided by the system for the purpose of managing security administration of the solution.</p> <p>A separate and distinct administrator role shall be established for the system.</p>	SG.AC-6 SG.AC-7 SG.SC-19 SG.SC-29	F16
Access Control.03	Unsuccessful Access Attempts	<p>The system: 1. Enforces a limit of organization-defined number of consecutive invalid login attempts by a user during an organization-defined time period.</p> <p>2. When the maximum number of unsuccessful attempts is exceeded, automatically locks the account/node for an organization-defined, exponentially increasing time period or until released by an administrator with appropriate safety</p>	SG.AC-8	F16

Control ID	Short Name	Definition	Reference(s)	Failure(s)
		<p>considerations (e.g., emergency override).</p> <p>3. When automatic locks are triggered, alerts shall be raised to the administrator.</p>		
<b>Access Control.04</b>	Concurrent Session Management	The system shall limit the number of concurrent connections DR Resource may establish with DRCE. The number of concurrent sessions shall be limited to the minimum necessary for proper operation of the Open ADR system. (More than 1 concurrent session requires justification.)	SG.AC-11	F1 F4
<b>Access Control.05</b>	Session Duration	<p>The system:</p> <ol style="list-style-type: none"> <li>Prevents further user access to the system by expiring or terminating the session after no more than <b>organization determined period</b> of inactivity with appropriate safety considerations.</li> <li>Sessions must be reestablished using appropriate identification and authentication procedures.</li> <li>Terminates a remote session after disconnect or an organization specified period of inactivity.</li> <li>The existing information on the display shall be obfuscated during session lock..</li> </ol>	SG.AC-12 SG.AC-13	F1 F4
<b>Access Control.06</b>	Portable Device Attachment	<p>The organization shall establish processes to</p> <ol style="list-style-type: none"> <li>Control the use of writeable removable media in Smart Grid information systems;</li> <li>Control the use of personally owned, removable media in Smart Grid systems;</li> <li>Issue specially configured mobile devices to individuals traveling to locations the organization determined to be a significant risk</li> <li>Applies specified measures to mobile devices returning from locations the the organization determines to be of significant risk.</li> </ol>	SG.AC-17	F16
<b>Access Control.07</b>	Remote Access Restrictions	<p>The organization authenticates remote access, and uses cryptography to protect the confidentiality and integrity of remote access sessions;</p> <p>The Smart Grid information system protects wireless access to the system using authentication and encryption.</p> <p>The organization monitors for unauthorized remote connections, including unauthorized wireless access points on an organization-defined frequency.</p>	SG.AC-15	F6 F7
<b>Access Control.08</b>	Password Management	<p>&lt;Role&gt; enforces the use of strong user passwords, in accordance with FIPS 112, and protects user passwords from potential exposure. This includes:</p> <ol style="list-style-type: none"> <li>Ensuring that passwords never cross component boundaries (i.e. in a message) in the clear.</li> <li>Ensuring that plaintext passwords are never stored and that stored password hashes use a cryptographic one-way hash function in accordance with the FIPS 180 series per applicable dates specified in SP800-131A.</li> </ol>	SG.AC-21 SG.SC-12	F16

Control ID	Short Name	Definition	Reference(s)	Failure(s)
		3. Ensuring that passwords are never included in or allowed to be embedded in tools, source code, scripts, URLs, aliases, or shortcuts. 4. Enforcing password complexity policies (minimum length of at least 10 characters with a combination of lower/upper case letters, numerals, and special characters). 5. Changing passwords at defined intervals and minimizing reuse. 6. Expiring passwords after defined intervals. 7. Protecting the password store from unauthorized modification.		

963

964 **4.2.2 Audit and Accountability**

965

**Table 4 – Controls: Audit and Accountability**

Control ID	Short Name	Definition	Reference(s)	Failure(s)
<b>Audit and Accountability.01</b>	Inappropriate User Activity	Each role shall monitor all user activity and report indications of inappropriate or unusual activity as defined by the organization.	SG.AU-6	F14 F16 F19 SF7
<b>Audit and Accountability.02</b>	Contents of Audit Records for DR Resource	DR Resource shall produce audit records for each DR event notification. The content of the audit records shall include the DR Controlling Entity Identity, date and time of the event, identity of the DR Resource where the event occurred and the state of DR Resource.	SG.AU-15	F14 F16 F17 F19 SF3 SF4 SF5
<b>Audit and Accountability.03</b>	Contents of Audit Records for DRCE	DRCE shall produce audit records for each DR event that has occurred. The content of the audit records shall include date and time of the event, type of the DR signal, identity of the user who issued the DR event, identity of the DR Resource where the event occurred and the state of DR Resources as a result of the event.	SG.AU-3 SG.AU-15	F14 F16 F17 F19 SF3 SF4 SF5 SF7
<b>Audit and</b>	Electronic Log	The system shall make all physical access logs to facilities containing communication and storage	SG.AU-2	SF2

Control ID	Short Name	Definition	Reference(s)	Failure(s)
<b>Accountability.04</b>	Format	devices of DRCE (e.g., DRAS) available in electronic form suitable for long term storage and retrieval.	SG.AU-3 SG.AU-4 SG.AU-15	
<b>Audit &amp; Accountability.05</b>	Local and Central Logging	<role> shall maintain a local log of all local authority actions at the highest level of detail available for the longest period of time that local storage space permits which shall be at least <Organizationally defined per role>. <role> shall forward all log entries to a dedicated logging server via its management server or directly to the log server . Retain centrally stored logs for at least <Organizationally defined>, with a minimum of <Organizationally defined> immediately available for analysis.	SG.AU-2 SG.AU-3 SG.AU-4 SG.AU-7 SG.AU-10 SG.AU-15	F14 F16 F19
<b>Audit &amp; Accountability.06</b>	User Access Monitoring/Logging	The system shall monitor and log all user interactive sessions to <role> including all administrative and maintenance activities.	SG.AU-2 SG.AU-14 SG.AU-15	F16 F19

966

967 **4.2.3 Configuration Management**

968

**Table 5 - Controls: Configuration Management**

Control ID	Short Name	Definition	Reference(s)	Failure(s)
<b>Configuration Management.01</b>	Access Restrictions for Configuration Change	Each role shall accept and apply configuration changes only from authenticated and authorized users. In addition, each role shall document all configuration changes.	SG.CM-1 SG.CM-3 SG.CM-4 SG.CM-5 SG.CM-6 SG.CM-11	F7 F14
<b>Configuration Management.02</b>	Factory Default Credentials	The system shall force a change of all factory default access and authentication credentials on DR Resource upon installation.	SG.CM-10	F14 F19
<b>Configuration Management.03</b>	Systems Inventory	The system shall create and maintain (on at least a daily basis) an inventory of Open ADR systems and devices that includes information that uniquely identifies each component, such as manufacturer, type, serial number, version number, and location (logical and physical).	SG.CM-8	F16 F19
<b>Configuration Management.04</b>	Current Configuration	A designated system or systems shall daily or on request obtain current version numbers, installation date, configuration settings, and patch level on <role>; validate the sender's cryptographic signature; and compare this	SG.CM-2 SG.CM-4	F14 F19



Control ID	Short Name	Definition	Reference(s)	Failure(s)
		information with recorded values in the inventory and configuration databases. All discrepancies shall be logged and alerts shall be generated where appropriate.	SG.CM-6 SG.SI-7	
<b>Configuration Management.05</b>	Disabling Unnecessary Communication Services	All networking and communication capabilities not required for the operation or maintenance of the system shall be disabled. This includes VOIP, instant messaging, ftp, HTTP, file sharing. Vendor defaults for all wireless options should be initially set "off". Any unused ports must be disabled. FTP, HTTP, Telnet shall be disabled and secure versions of these protocols, Secure FTP, Secure Copy Protocol, HTTP over TLS, and Secure Shell, must be used instead. Modems should be disabled by default. Every modem port and LAN port should be disabled by default.	SG.CM-2 SG.CM-7 SG.CM-10 SG.SC-17	F7 F12 F13

969

970 **4.2.4 Continuity of Operation**

971

**Table 6 - Controls: Continuity of Operations**

Control ID	Short Name	Definition	Reference(s)	Failure(s)
<b>Continuity of Operation.01</b>	Alternate Storage	DRCE shall provide alternate storage for essential configuration settings (e.g., participants and DR programs they are enrolled in).	SG.CP-2 SG.CP-7	F15 F16 F18
<b>Continuity of Operation.02</b>	Alternate Telecommunication Services	The system shall provide alternate telecommunication channel between DRCE and DR Resource when the primary channel becomes unavailable.	SG.CP-8	F2
<b>Continuity of Operations.03</b>	Operations Continuity	The system shall provide means to compensate for loss of a single component implementing DRCE without loss of system functionality.	SG.CP-2 SG.PM-5	SF2
<b>Continuity of Operations.04</b>	System Restoration	The system shall have the ability to recover DRCE from securely maintained backups, images, and configurations in the event of compromised device(s) or network (exception: hardware changes).	SG.CP-10	SF2
<b>Continuity of Operations.05</b>	Alternative Time Source	The <role> shall support alternative time source for redundancy and consistency checking.	SG.CM-6	SF3 SF4

972

973 **4.2.5 Identification & Authentication**

974

**Table 7 - Controls: Identification & Authentication**

Control ID	Short Name	Definition	Reference(s)	Failure(s)
------------	------------	------------	--------------	------------

<b>Identification &amp; Authentication.01</b>	Identifier Management	The system shall assign (globally) unique identifiers to each individual and device. Within the context of this specification global refers to the system as a whole and does not include identifiers with respect to other systems.	SG.IA-2	F5 F6 F7 F16 F19 SF7
<b>Identification &amp; Authentication.02</b>	Authenticator Feedback	The system shall obscure the feedback of authentication information during the authentication process (e.g., displaying asterisks when a user types in a password).	SG.IA-6	F16 F19
<b>Identification &amp; Authorization.03</b>	Credential Management	The system shall provide a single point of initiation to distribute, manage, and revoke all logical and physical access credentials for all OPEN ADR systems and components. Revocation shall be carried out on all systems within 24 hours.	SG.IA-3	F16 F19
<b>Identification &amp; Authorization.04</b>	Digital Certificates	DRCE shall provide cryptographically strong authentication credentials such as digital certificates signed by the organization (to which the DRCE belongs) or other trusted party (i.e., a trusted identity provider or vendor). Certificate issuance and signing must conform to a secure process such as NIST SP 800-53: FPKI Security Controls for PKI Systems and NIST SP 800-53A: Assessment Guidance for Security Controls in PKI Systems. The proof of authenticity must be generated by an organizational process that supports independent review, and credentials must be independently verifiable by external (to the organization) audit.	SG.AC-1 SG.AU-2 SG.AU-16 SG.IA-4 SG.SC-15	F7 F11
<b>Identification &amp; Authorization.05</b>	Message Identities	<Role> shall include in every message the identity of the sender and the intended recipient(s). The mechanisms used to meet the requirement of this control are intended to be applied within the message payload.	SG.IA-5 SG.AU-2 SG.AU-3	F5 F6 F7
<b>Identification &amp; Authorization.06</b>	Self Identification	Software shall be able to report identifying and configuration information on request. This should include version number, installation date, configuration settings, patch level.	SG.SI-7	F14 F19

975

976 **4.2.6 Physical & Environment Security**

977

**Table 8 - Controls Physical & Environment Security**

Control ID	Short Name	Definition	Reference(s)	Failure(s)
<b>Physical &amp; Environmental. 01</b>	Physical Access Authentication of DRCE	The system shall implement a minimum of two factor (TBD) authentication for physical access to facilities containing communication and storage devices of DRCE (e.g., DRAS).	SG.PE-2	SF2
<b>Physical &amp; Environmental. 02</b>	Facility Access Monitoring/Logging of DRCE	Physical Access to facilities containing communication and storage devices of DRCE (e.g., DRAS) shall be monitored and logged at all times.	SG.PE-4	SF2
<b>Physical &amp; Environmental.03</b>	Limited Access - Interactive Resources	Supporting systems shall limit physical access to <role> to only those personnel responsible for operating, maintaining, or managing the <role>.	(SG.PE-3)	SF1 SF2
<b>Physical &amp; Environmental.04</b>	Component Location for DRCE	The physical location of DRCE shall minimize potential damage from physical and environmental hazards and minimize the opportunity for unauthorized access.	(SG.PE-12)	SF2
<b>Physical &amp; Environmental.05</b>	Fire Detection	All facilities housing DRCE shall implement fire detection devices/systems. These devices/systems shall activate automatically and notify the organization and emergency responders in the event of a fire. All activations of the system shall be logged.	NONE	SF2

978

979 **4.2.7 System & Communications Protection**

980

**Table 9 - Controls: System & Communications Protection**

Control ID	Short Name	Definition	Reference(s)	Failure(s)
<b>System &amp; Communications Protection.01</b>	Communication Integrity	DRCE employs FIPS 180 compliant hashing mechanisms and FIPS 186 compliant digital signature mechanisms.	SG.SC-8 SG.SC-12 SG.SC-20	F7 F11
<b>System &amp; Communication Protection.02</b>	Communication Confidentiality	Each role employs FIPS 140-2 compliant cryptographic mechanisms on messages that contain of private information (e.g., password, cryptographic keys) to prevent unauthorized disclosure.	SG.SC-9 SG.IA-6	SF6
<b>System &amp; Communication Protection.03</b>	Cryptographic Key Implementation and Management	The system shall provide a mechanism to generate cryptographic keys with sufficient randomness. In addition, the system shall provide efficient mechanism to revoke and refresh cryptographic keys.	SG.SC-11	F6 F7

Control ID	Short Name	Definition	Reference(s)	Failure(s)
<b>System &amp; Communication Protection.04</b>	Multiple verification	The DRCE must provide alternate channels of notification in order to allow humans to verify and authorize interactions with the DRCE in scenarios where it is operationally required to have multiple levels of verification and authorization before any actions be taken in response to a message from the DRCE. (Not applicable to FastDR – See Glossary for definition)	None	F7 F9 F11 F13
<b>System &amp; Communication Protection.05</b>	Information Flow Enforcement	The system shall provide dynamic control of DR event information flow based on changes of user accounts and authorized roles.	SG.AC-5 SG.AC-15 SG.SC-5 SG.SC-7	F3 F5 F6 F7 F12 F13
<b>System &amp; Communication Protection.07</b>	No Shared Accounts	The system shall associate each individual account (no shared accounts) with an account group/user group for proper auditing, management, and tracking. Wherever possible, globally privileged accounts (e.g., SuperUser accounts, Administrator, or Root) shall be disabled and/or removed.	SG.SC-19	F14 F16 F19
<b>System &amp; Communication Protection.08</b>	Emergency Network Segmentation	If an attack is detected, the system shall label all traffic from compromised Open ADR network segments as potentially malicious, and provide tools to isolate the compromised segment from network segments that are confirmed as trustworthy and defensible.	NONE	F5 F6 F7 F12 F13
<b>System &amp; Communication Protection.09</b>	Remote Interactive Sessions	All remote user-interactive sessions to <role> shall be encrypted using FIPS 140-2 compliant mechanisms, including all administrative and maintenance activities.	SG.AC-15 SG.SC-9 SG.SC-12	F6 F7
<b>System &amp; Communication Protection.10</b>	Resource Consumption	The <role> shall implement resource monitoring and control mechanisms for all devices/processes to identify and mitigate excessive resource consumption (e.g., runaway processes).	SG.SC-6	F4
<b>System &amp; Communication Protection.11</b>	Quality of Service - Specification	DRCE shall use a QoS or other resource reservation control mechanism on all outgoing communications. Relative priority for traffic related to Open ADR systems shall be from highest to lowest: 1) DR Event messages, 2) configuration and management,	SG.SC-6	F1 F4
<b>System &amp; Communication Protection.12</b>	Quality of Service - Enforcement	The network shall process all traffic in accordance with the QoS or other resource reservation control identifier.	SG.SC-6	F1 F3

981

982 **4.2.8 System & Information Integrity**

983

**Table 10 - Controls: System & Information Integrity**

Control ID	Short Name	Definition	Reference(s)	Failure(s)
<b>System &amp; Information Integrity.01</b>	Intrusion Detection	The system shall implement intrusion detection systems to monitor and detect malicious traffic passing between the network segments.	SG.AC-15	F6 F12
<b>System &amp; Information Integrity.02</b>	Clock Record	DR Resource's clock record shall indicate time source used for synchronization and when last synchronized.	NONE	SF 3
<b>System &amp; Information Integrity.03</b>	End Point Security	<Roles> using a general purpose operating system shall implement end point security mechanisms to scan software for malicious code.	SG.SI-3	F19
<b>System &amp; Information Integrity.04</b>	End Point Isolation	The system shall provide the capability to isolate compromised devices from the rest of the Open ADR system upon detection of compromise. This includes the capability to physically disconnect DR Resource from the grid by collaborating with authoritative entities if such actions are deemed necessary.	NONE	F6 F7
<b>System &amp; Information Integrity.05</b>	Software Integrity Check	The system shall maintain a complete image of all currently deployed component software. All components shall maintain a hash of installed software, including patches. Any update to component software shall require a recalculation of the hash. A periodic integrity check of all component software shall be performed by comparing the hash on the component to the hash in the repository. This check shall be performed at least once every (TBD) days. Acceptable technologies shall be specified by FIPS 186.	SG.SC-12 SG.SI-7	F19
<b>System &amp; Information Integrity.06</b>	Storage Integrity Check	<Role> shall perform automated checks (e.g., file system checks, database integrity checks, and checksum comparisons) to validate the integrity of the logical and physical media on a periodic basis as defined by the organization, in no cases exceeding (TBD) week between checks. Integrity checks shall verify the media is in adequate condition to perform the functions assigned to <role>, and shall immediately report any abnormalities or problems discovered during the scan to the administrator of <role>.	NONE	F15
<b>System &amp; Information Integrity.07</b>	Network Quality Monitoring	The system periodically interrogates and validates current connectivity by observing communication from DRCE on at least a daily basis. All results shall be recorded in an associated log file. Any results indicating an error (as determined by preset conditions) shall alert the system manager.	NONE	F2
<b>System &amp; Information Integrity.08</b>	Message Validation	<Role> shall validate all application protocol fields that it uses for logical and expected values including source, destination, time stamps, and state indicators. <Role> shall use its context and history when assessing the validity of the message. For example, DR Resource should check the type of DR Program it is enrolled in before processing the	SG.SI-8	F9 F11 F8 F10

Control ID	Short Name	Definition	Reference(s)	Failure(s)
		DR Event Notification Message.		
<b>System &amp; Information Integrity.09</b>	Minimal Error Message Content	<Role> shall not reveal potentially harmful (e.g., exploitable) information in error messages.	SG.SI-9	F16
<b>System &amp; Information Integrity.10</b>	Message Time stamping	<Role> shall time stamp all configuration and management messages that it sends.	NONE	SF4
<b>System &amp; Information Integrity.11</b>	Configuration File Authenticity	<Role> shall not accept any message payload containing configuration files that is not cryptographically signed. Acceptable technologies shall be specified by FIPS 186.	SG.AU-16 SG.SC-12 SG.SI-7	F3 F11 F14
<b>System &amp; Information Integrity.12</b>	Configuration File and Sensitive Data Integrity Check	Configuration files and other sensitive data should include cryptographic integrity checks (e.g., cryptographic hashes) and the integrity of the file should be checked whenever it is read by an application.	SG.SI-7	F3 F14
<b>System &amp; Information Integrity.13</b>	Software and Firmware Authenticity	<Role> shall not accept software or firmware updates that do not have cryptographically signed message payloads, nor shall a system execute any software or firmware before validating its cryptographic signature. Acceptable technologies shall be specified by FIPS 186.	SG.AU-16 SG.SC-12 SG.SI-7	F11 F19

984 **4.2.9 Controls Mapped to Roles**

985

**Table 11 - Controls Mapped to Roles**

Control ID	Short Name	DR Controlling Entity	DR Resource
<b>Access Control.01</b>	Automated Account Management	X	X
<b>Access Control.02</b>	Least Privilege	X	X
<b>Access Control.03</b>	Unsuccessful Access Attempts	X	X
<b>Access Control.04</b>	Concurrent Session Management		X
<b>Access Control.05</b>	Session Duration	X	X
<b>Access Control.06</b>	Portable Device Attachment	X	X

Control ID	Short Name	DR Controlling Entity	DR Resource
Access Control.07	Remote Access Restrictions	X	X
Access Control.08	Password Management	X	X
Audit and Accountability.01	Inappropriate User Activity	X	X
Audit and Accountability.02	Contents of Audit Records for DR Resource		X
Audit and Accountability.03	Contents of Audit Records for DRCE	X	
Audit and Accountability.04	Electronic Log Format	X	
Audit & Accountability.05	Local and Central Logging	X	X
Audit & Accountability.06	User Access Monitoring/Logging	X	X
Configuration Management.01	Access Restrictions for Configuration Change	X	X
Configuration Management.02	Factory Default Credentials		
Configuration Management.03	Systems Inventory	X	X
Configuration Management.04	Current Configuration	X	X
Configuration Management.05	Disabling Unnecessary Communication Services	X	X
Continuity of Operation.01	Alternate Storage	X	
Continuity of Operation.02	Alternate Telecommunication Services	X	X
Continuity of Operations.03	Operations Continuity	X	X
Continuity of Operations.04	System Restoration	X	
Continuity of Operations.05	Alternative Time Source		X
Identification & Authentication.01	Identifier Management	X	X
Identification & Authentication.02	Authenticator Feedback	X	X

Control ID	Short Name	DR Controlling Entity	DR Resource
Identification & Authorization.03	Credential Management	X	X
Identification & Authorization.04	Digital Certificates	X	
Identification & Authorization.05	Message Identities	X	X
Identification & Authorization.06	Self Identification	X	X
Physical & Environmental. 01	Physical Access Authentication of DRCE	X	
Physical & Environmental. 02	Facility Access Monitoring/Logging of DRCE	X	
Physical & Environmental.03	Limited Access - Interactive Resources	X	X
Physical & Environmental.04	Component Location for DRCE	X	
Physical & Environmental.05	Fire Detection	X	
System & Communications Protection.01	Communication Integrity	X	X
System & Communication Protection.02	Communication Confidentiality	X	X
System & Communication Protection.03	Cryptographic Key Implementation and Management	X	X
System & Communication Protection.04	Multiple verification		X
System & Communication Protection.05	Information Flow Enforcement	X	X
System & Communication Protection.07	No Shared Accounts	X	X
System & Communication Protection.08	Emergency Network Segmentation	X	X
System & Communication Protection.09	Remote Interactive Sessions	X	X



Control ID	Short Name	DR Controlling Entity	DR Resource
System & Communication Protection.10	Resource Consumption	X	
System & Communication Protection.11	Quality of Service Specification	X	
System & Communication Protection.12	Quality of Service Enforcement	X	X
System & Information Integrity.01	Intrusion Detection	X	X
System & Information Integrity.02	Clock Record		X
System & Information Integrity.03	End Point Security	X	X
System & Information Integrity.04	End Point Isolation	X	X
System & Information Integrity.05	Software Integrity Check	X	X
System & Information Integrity.06	Storage Integrity Check	X	X
System & Information Integrity.07	Network Quality Monitoring	X	
System & Information Integrity.08	Message Validation		X
System & Information Integrity.09	Minimal Error Message Content	X	X
System & Information Integrity.10	Message Time stamping	X	X
System & Information Integrity.11	Configuration File Authenticity	X	X
System & Information Integrity.12	Configuration File and Sensitive Data Integrity Check	X	X
System & Information Integrity.13	Software and Firmware Authenticity	X	X

986

987 **Appendix A: Relation to the NIST**  
988 **Interagency Report 7628**

---

989 A goal of the OpenADR security profile is to support and align with the NIST IR 7628.  
990 This document approaches analyzing each interface at each process step in regard to  
991 failure analysis and control development (refer to Figure 6).

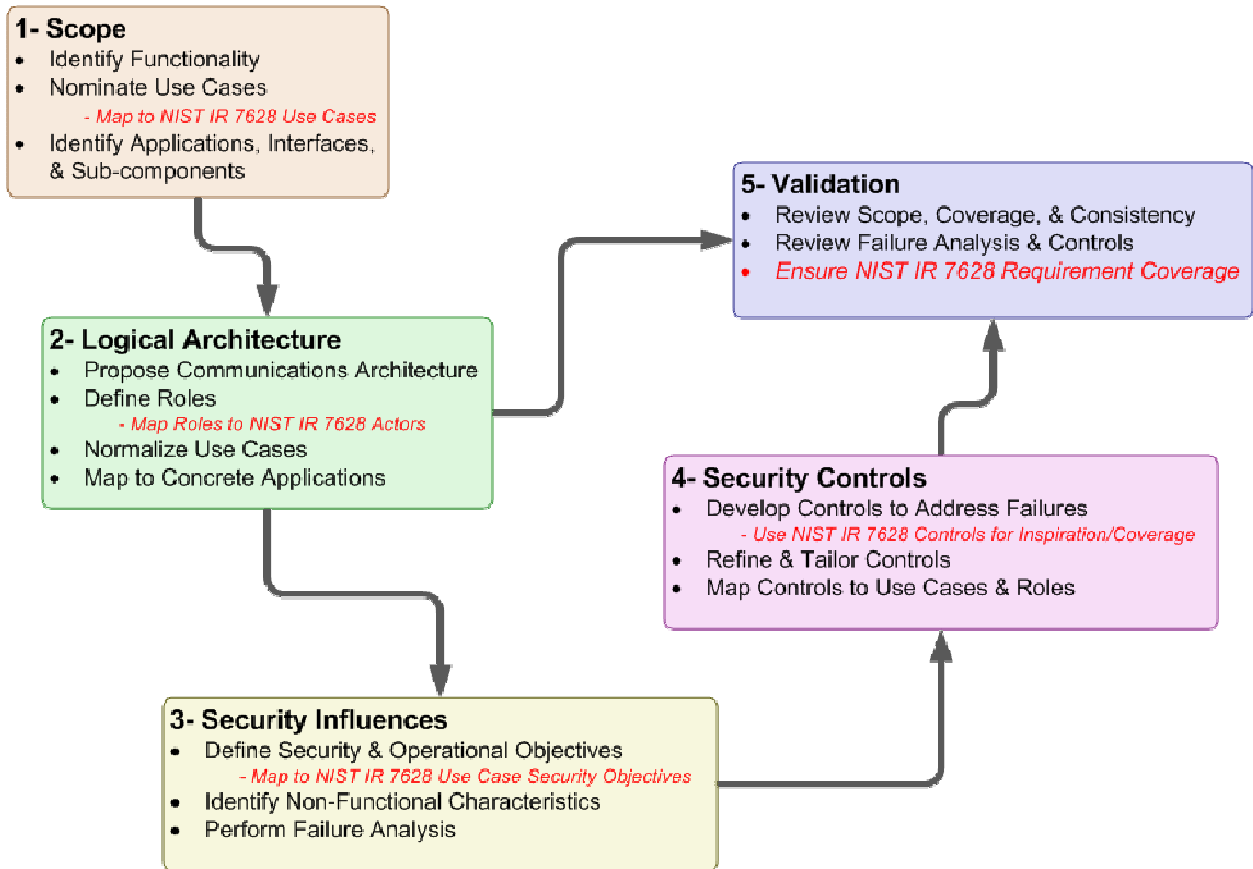
992 **A.1 Traceability**

993 This section documents the traceability found between the NIST IR 7628 and the  
994 OpenADR Security Profile. The OpenADR Security Profile incorporates the NIST IR  
995 7628 in each of the five major phases of the security profile development.

- 996 1. Scope – This document incorporates a review and analysis of NIST IR 7628 use  
997 cases to guide the development of OpenADR scope.
- 998 2. Logical Architecture – This document incorporates a review and analysis of  
999 relevant architectural elements from the NIST IR 7628 in the OpenADR logical  
1000 architecture development, re-using actors where possible and further  
1001 decomposing the architecture where needed.
- 1002 3. Security Influences – This document incorporates an analysis of the security  
1003 objectives defined in the NIST IR 7628 use cases in developing and expanding  
1004 security principles for OpenADR.
- 1005 4. Security Controls – This document used the relevant technical requirements from  
1006 NIST IR 7628 as a source of inspiration for the development of the controls for  
1007 this security profile. The NIST IR 7628 controls were also used as a means to

1008 verify coverage by way of identifying controls that this document might not have  
 1009 otherwise considered.

1010 5. Validation – the validation step is an iterative process in the development of a  
 1011 security profile. This document incorporates a review of the NIST IR 7628  
 1012 controls and actor-to-control mappings as a means to ensure completeness in the  
 1013 OpenADR Security Profile.



1014  
 1015 **Figure 6 – Security Profile Workflow NIST-IR 7628 Mapping**

1016 **A.2 NIST IR 7628 Actors to WAMPAC Roles Mapping**

1017 This section documents the mapping from NIST IR 7628 actors to WAMPAC Security  
 1018 Profile roles. This document uses the term “Role” to denote the function performed by  
 1019 the object within the use cases since a given device may perform more than one function.  
 1020 This approach supported the understanding of security failures and controls at the lowest  
 1021 level practical.

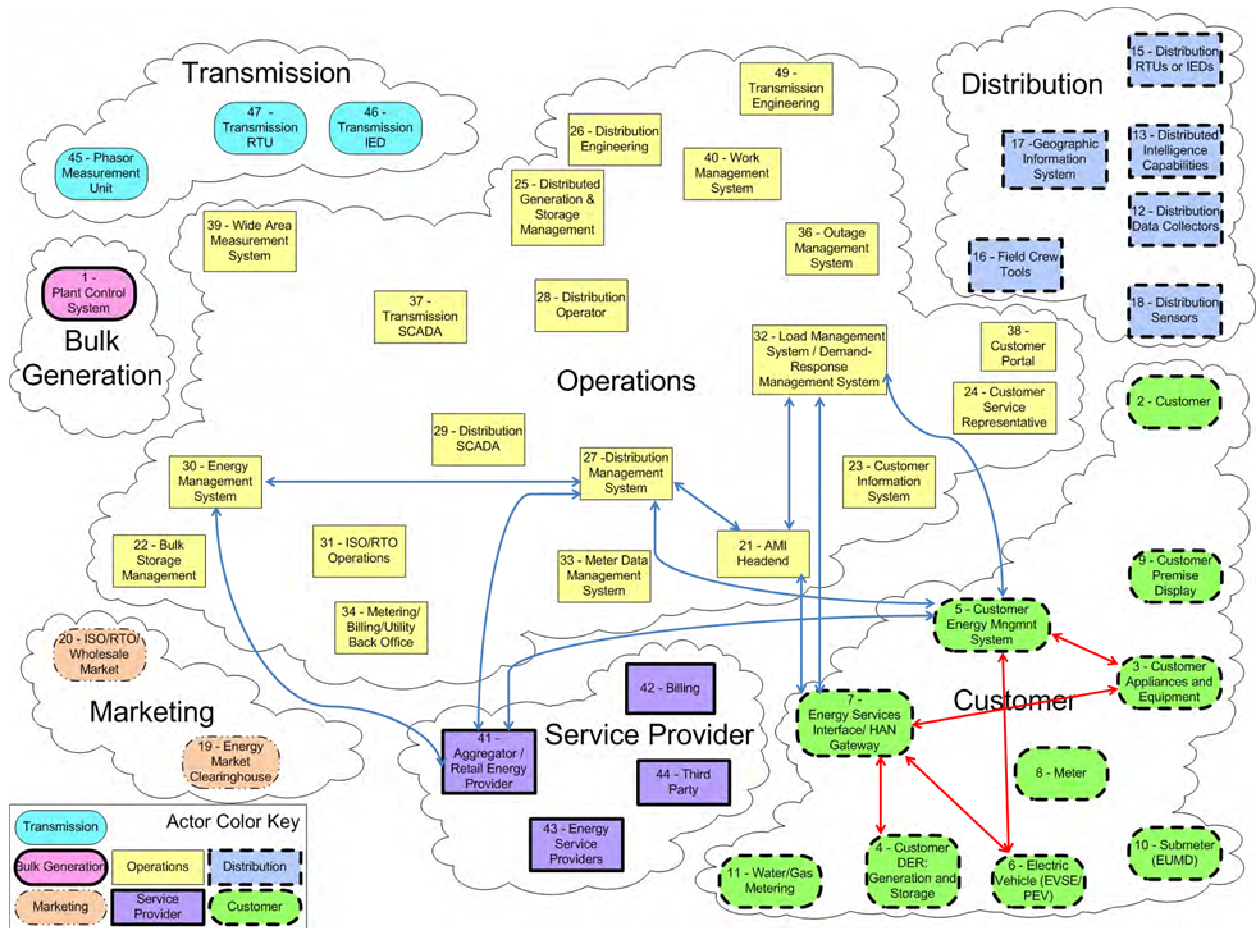
1022 By comparison, although subtle, an “Actor” as defined by the OMG for unified modeling  
 1023 language is:

1024 *A type of role played by an entity that interacts with the subject, but which is*  
 1025 *external to the subject. Actors may represent roles played by human users,*  
 1026 *external hardware, or other subjects. Note that an actor does not necessarily*  
 1027 *represent a specific physical entity but merely a particular facet (i.e., “role”) of*  
 1028 *some entity that is relevant to the specification of its associated use cases. Thus, a*  
 1029 *single physical instance may play the role of several different actors and,*  
 1030 *conversely, a given actor may be played by multiple different instances. (p.604-5,*  
 1031 *OMG Unified Modeling Language (OMG UML), Superstructure Version 2.3)*

1032 Briefly, NIST IR 7628 actors are entities that may perform many OpenADR roles. NIST  
 1033 IR 7628 actors are derived from Figure F-6, Volume 3 page F-21.

1034 The NIST IR 7628 actors that are omitted are out of scope for this security profile.

1035 Figure 7 – Unified Logical Architecture for OpenADR depicts the areas of the Unified  
 1036 Logical Architecture potentially impacted by OpenADR interactions. The blue lines are  
 1037 communication links. The red lines are the communications from a DR Resource point-  
 1038 of-view.



1039  
 1040

**Figure 7 – Unified Logical Architecture for OpenADR**

1041

1042

1043

**Table 12 – NIST IR 7628 Actor to WAMPAC Role Mapping**

<b>NIST IR 7628 Actor Number</b>	<b>NIST IR 7628 Actor</b>	<b>Open ADR Role</b>
27	Distribution Management System	DR Controlling Entity
41	Aggregator/Retail Energy Provider	DR Controlling Entity/DR Resource
32	Load Management Systems/Demand Response Management System	DR Controlling Entity
30	Energy Management System (EMS)	DR Controlling Entity
5	Customer Energy Management System	DR Resource
3	Customer Appliances and Equipment	DR Asset
4	Customer Distributed Energy Resources: Generation and Storage (DER)	DR Asset

1044

1045

### ***A.3 NIST IR 7628 Security Objectives to Open ADR Security Principles Mapping***

1046

1047

**Table 13 - NIST IR 7628 Use Case Objectives to OpenADR Security Principles**

<b>NIST IR 7628 Scenario</b>	<b>Cyber Security Objective / Requirements</b>	<b>Open ADR Security Principle</b>
<b>Real-Time Pricing (RTP) for Customer Load and DER/PEV</b>	<p>Integrity, including non-repudiation, of pricing information is critical, since there could be large financial and possibly legal implications</p> <p>Availability, including non-repudiation, for pricing signals is critical because of the large financial and possibly legal implications</p> <p>Confidentiality is important mostly for the responses that any customer might make to the pricing signals</p>	<p>Transactive pricing signals are not in scope for OpenADR.</p>

NIST IR 7628 Scenario	Cyber Security Objective / Requirements	Open ADR Security Principle
<b>Time of Use (TOU) Pricing</b>	Integrity is not critical since TOU pricing is fixed for long periods and is not generally transmitted electronically  Availability is not an issue  Confidentiality is not an issue, except with respect to meter reading	1, 13
<b>Net Metering for DER and PEV</b>	Integrity is not very critical since net metering pricing is fixed for long periods and is not generally transmitted electronically  Availability is not an issue  Confidentiality is not an issue, except with respect to meter reading	1,13
<b>Feed-In Tariff Pricing for DER and PEV</b>	Integrity is not critical, since feed-in tariff pricing is fixed for long periods and is generally not transmitted electronically  Availability is not an issue  Confidentiality is not an issue, except with respect to meter reading	1,13
<b>Critical Peak Pricing</b>	Critical Peak Pricing builds on TOU pricing by selecting a small number of days each year where the electric delivery system will be heavily stressed and increasing the peak (and sometime shoulder peak) prices by up to 10 times the normal peak price. This is intended to reduce the stress on the system during these days.	1,13
<b>Load Management</b>	Integrity of load control commands is critical to avoid unwarranted outages  Availability for load control is important – in aggregate (e.g. > 300 MW), it can be critical  Confidentiality is not very important	1,2,3,4,6,7,8,10,11

1048

1049

1050 **A.4 NIST IR 7628 Technical Requirements Mapped**  
 1051 **Open ADR Controls**

1052 **Table 14 - NIST IR 7628 Technical Requirements Mapped to OpenADR Controls**

<b>NIST IR 7628 Requirement</b>	<b>NIST IR 7628 Short Name</b>	<b>Open ADR Control</b>	<b>Coverage</b>
<b>SG.AC-5</b>	Information Flow Enforcement	System & Communication Protection.12	fully covered
<b>SG.AC-6</b>	Separation of Duties	Access Control.2 Access Control.3	covers non-organizational portions
<b>SG.AC-7</b>	Least Privilege	Access Control.2 Access Control.3	fully covered
<b>SG.AC-8</b>	Unsuccessful Login Attempts	Access Control.4	fully covered
<b>SG.AC-11</b>	Concurrent Session Control	Access Control.6	fully covered
<b>SG.AC-12</b>	Session Lock	Access Control.7	fully covered
<b>SG.AC-13</b>	Remote Session Termination	Access Control.7	fully covered
<b>SG.AC-14</b>	Permitted Actions without Identification or Authentication	Access Control.5	NIST IR 7628 is organizational, but supported by our control

NIST IR 7628 Requirement	NIST IR 7628 Short Name	Open ADR Control	Coverage
<b>SG.AC-15</b>	Remote Access	Access Control.3 Access Control.9 Access Control.10 Access Control.11 Identification & Authorization.3 Identification & Authorization.4 Identification & Authorization.5 Identification & Authorization.6 Network.2 System & Information Integrity.6 System & Communication Protection.10 System & Communication Protection.11 System & Communication Protection.12 System & Communication Protection.14 System & Communication Protection.17	fully covered
<b>SG.AC-16</b>	Wireless Access Restrictions	Access Control.10 Access Control.11	fully covered
<b>SG.AC-17</b>	Access Control for Portable and Mobile Devices	Access Control.8	fully covered
<b>SG.AC-21</b>	Passwords	Access Control.12	fully covered
<b>SG.AU-2</b>	Auditable Events	Access Control.1 Access Control.5 Audit & Accountability.1 Audit & Accountability.3 Identification & Authorization.3	covers non-organizational portions
<b>SG.AU-3</b>	Content of Audit Records	Audit & Accountability.5	fully covered



<b>NIST IR 7628 Requirement</b>	<b>NIST IR 7628 Short Name</b>	<b>Open ADR Control</b>	<b>Coverage</b>
<b>SG.AU-4</b>	Audit Storage Capacity	Audit & Accountability.3 Audit & Accountability.4 System & Information Integrity.24 System & Information Integrity.25	fully covered
<b>SG.AU-15</b>	Audit Generation	Audit & Accountability.5	fully covered
<b>SG.AU-16</b>	Non-Repudiation	Audit & Accountability.2 Audit & Accountability.3 Identification & Authorization.3 System & Communication Protection.10 System & Information Integrity.7 System & Information Integrity.9	fully covered
<b>SG.CM-7</b>	Configuration for Least Functionality	Configuration Management.3 Configuration Management.4	fully covered
<b>SG.CM-8</b>	Component Inventory	Configuration Management.1	fully covered
<b>SG.IA-4</b>	User Identification and Authentication	Identification & Authorization.4	fully covered
<b>SG.IA-5</b>	Device Identification and Authentication	Identification & Authorization.5 Identification & Authorization7	fully covered
<b>SG.IA-6</b>	Authenticator Feedback	Identification & Authorization.8	fully covered
<b>SG.SC-2</b>	Communications Partitioning	System & Communication Protection.1	fully covered
<b>SG.SC-3</b>	Security Function Isolation	System & Communication Protection.2	fully covered
<b>SG.SC-4</b>	Information Remnants	System & Communication Protection.3	partially covered; object reuse is not addressed by our control.

NIST IR 7628 Requirement	NIST IR 7628 Short Name	Open ADR Control	Coverage
<b>SG.SC-5</b>	Denial-of-Service Protection	System & Communication Protection.12 Continuity of Operations.2 Continuity of Operations.3 Continuity of Operations.6	partially covered – NIST IR 7628 does not give specific guidance on how to meet requirement.
<b>SG.SC-6</b>	Resource Priority	System & Communication Protection.6 System & Communication Protection.7 System & Communication Protection.8	
<b>SG.SC-7</b>	Boundary Protection	Network.2 Network.4 Network.6 Network.8 Identification & Authorization.5 Identification & Authorization.6 System & Communication Protection.10 System & Communication Protection.11 System & Communication Protection.12 System & Communication Protection.13 System & Communication Protection.14	fully covered
<b>SG.SC-8</b>	Communication Integrity	Access Control.10 System & Communication Protection.10 System & Information Integrity.9	fully covered
<b>SG.SC-9</b>	Communication Confidentiality	System & Communication Protection.11 System & Communication Protection.16 System & Communication Protection.17 System & Communication Protection.18	fully covered

NIST IR 7628 Requirement	NIST IR 7628 Short Name	Open ADR Control	Coverage
SG.SC-10	Trusted Path	Access Control.3 Access Control.7 Access Control.10 Configuration Management.4 Identification & Authorization.1 Identification & Authorization.3 Identification & Authorization.4 Identification & Authorization.6 Identification & Authorization.7 Network.2 Network.4 Network.6 Network.8 Physical & Environmental.2 Physical & Environmental.3 Physical & Environmental.14 System & Communication Protection.4 System & Communication Protection.5 System & Communication Protection.10 System & Communication Protection.11 System & Communication Protection.12 System & Communication Protection.13 System & Communication Protection.14 System & Communication Protection.17 System & Communication Protection.20 System & Communication Protection.21 System & Communication Protection.22 System & Information Integrity.4 System & Information Integrity.6 System & Information Integrity.14 System & Information Integrity.17	fully covered

<b>NIST IR 7628 Requirement</b>	<b>NIST IR 7628 Short Name</b>	<b>Open ADR Control</b>	<b>Coverage</b>
<b>SG.SC-11</b>	Cryptographic Key Establishment and Management	System & Communication Protection.18	fully covered
<b>SG.SC-12</b>	Use of Validated Cryptography	Access Control.10 Access Control.12 Identification & Authorization.9 System & Communication Protection.10 System & Communication Protection.11 System & Communication Protection.17 System & Information Integrity.7 System & Information Integrity.9 System & Information Integrity.10	fully covered
<b>SG.SC-15</b>	Public Key Infrastructure Certificates	Identification & Authorization.3	covers non-organizational portions
<b>SG.SC-16</b>	Mobile Code	System & Communication Protection.19	fully covered
<b>SG.SC-17</b>	Voice-Over Internet Protocol	Configuration Management.4 System & Communication Protection.9	fully covered
<b>SG.SC-18</b>	System Connections	Access Control.9 System & Communication Protection.20	fully covered
<b>SG.SC-19</b>	Security Roles	Access Control.2 Access Control.3 System & Communication Protection.21	covers non-organizational portions
<b>SG.SC-20</b>	Message Authenticity	Identification & Authorization.5 System & Communication Protection.20	fully covered
<b>SG.SC-21</b>	Secure Name/Address Resolution Service	System & Communication Protection.22	fully covered

<b>NIST IR 7628 Requirement</b>	<b>NIST IR 7628 Short Name</b>	<b>Open ADR Control</b>	<b>Coverage</b>
<b>SG.SC-29</b>	Application Partitioning	Access Control.2 and Access Control.3	seems redundant with NIST IR 7628 least privilege controls
<b>SG.SC-30</b>	Smart Grid Information System Partitioning	Network.1 - Network.8	fully covered
<b>SG.SI-2</b>	Flaw Remediation	Configuration Management.2 System & Information Integrity.1 System & Information Integrity.2	fully covered
<b>SG.SI-7</b>	Software and Information Integrity	Configuration Management.2 Identification & Authorization.9 System & Information Integrity.7 System & Information Integrity.8 System & Information Integrity.9 System & Information Integrity.10	fully covered
<b>SG.SI-8</b>	Information Input Validation	System & Information Integrity.13 System & Information Integrity.14	fully covered
<b>SG.SI-9</b>	Error Handling	System & Information Integrity.15 System & Information Integrity.16	fully covered

1053  
1054  
1055  
1056  
1057  
1058  
1059  
1060  
1061  
1062  
1063  
1064

1065

1066

<i>SECURITY PROFILE FOR OPENADR</i>	<i>Version – 0.03</i>	<b>78</b>
UCA International Users Group	March 30, 2012	

1067

## Appendix B: Use Case Notation Guide

1068

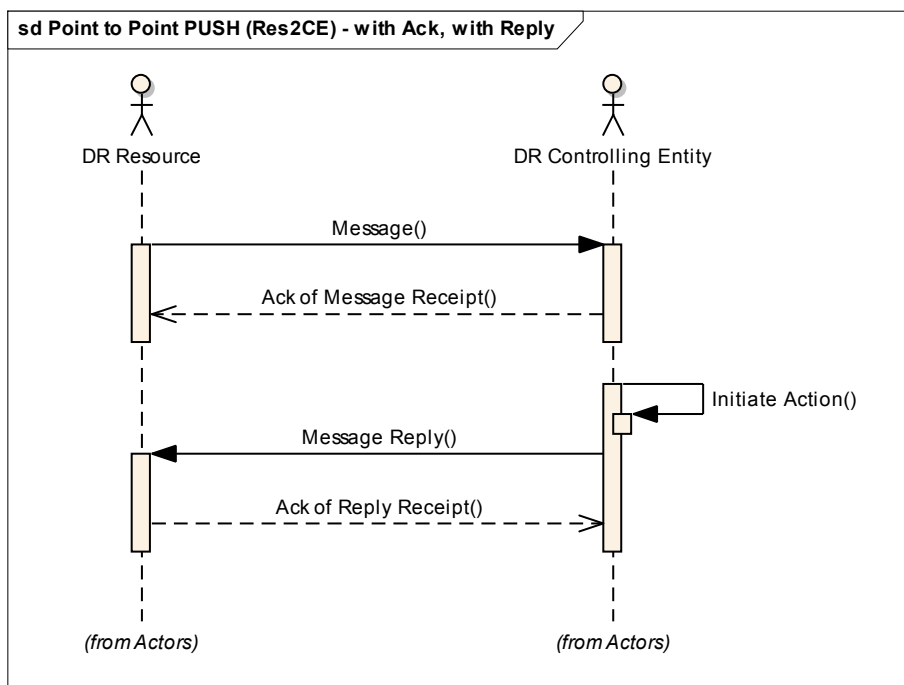
1069

The use cases presented in Section 2.4 of this document include sequence diagrams that graphically depict the flow of information/data and activities performed by roles in order to complete the use case. A sequence diagram represents role or actor behavior as a series of sequential steps. An example is shown in Figure 8 below.

1070

1071

1072



1073

1074

### Figure 8 – An Annotated Sequence Diagram

1075 This example is annotated to illustrate key features of the notation.

- 1076 1. Sequence Diagrams represent behavior of actors/roles as parallel vertical lines  
1077 with the messages exchanged between them presented as parallel horizontal lines  
1078 in the sequence that they occur.
- 1079 2. The role name is presented at the top of each vertical line. The lines vertical line  
1080 represents a timeline that flows from top to bottom
- 1081 3. Messages are presented as a series of horizontal lines with the message name  
1082 above the line. Dashed lines indicate a return message.
- 1083 4. Message lines that begin and terminate with the same role indicate a message or  
1084 action internal to the role.
- 1085 5. A use case ends when all of its steps have been completed and the vertical lines  
1086 end.



1087 **Appendix C: Using the Security**  
1088 **Profile to Evaluate an OpenADR**  
1089 **Deployment**

---

1090 This document can be used to evaluate the security of a proposed OpenADR deployment<sup>8</sup>.  
1091 The security controls and the failure analysis in this security profile are based on the  
1092 definition of uses cases and roles. In different OpenADR deployments, the use cases and  
1093 roles will be mapped to different elements of the actual deployment. An architectural analysis  
1094 of a proposed deployment against this document has the following steps.  
1095

- 1096 1. Map the proposed deployment to the roles in Section 2.
- 1097 2. For each use case, use the mapping generated in step 2 and Failures mapped to Use Cases  
1098 in Table xx (Section 3.2) to determine which elements are involved in the use case.
- 1099 3. For each instance of each use case, determine the possible failures, per role and per step.  
1100 This information comes from the three failure tables in Section 3.3. Then determine the  
1101 controls that mitigate each possible failure using the mappings in Section 0.
- 1102 4. For each element of the proposed OpenADR deployment, determine the recommended  
1103 controls for that element. This involves mapping each element to the appropriate use

---

<sup>8</sup> For more advice on how to use a Security Profile for the system lifecycle see : HOW A UTILITY CAN USE ASAP-SG SECURITY PROFILES by theAdvanced Security Acceleration Project for the Smart Grid (ASAP-SG)

- 1104 cases and use case steps, proceeding through possible failures and determining the  
 1105 recommended controls. This is the information gathered in steps 1-4 above.
- 1106 5. For each element of the proposed OpenADR deployment, and each recommended control  
 1107 for that element, determine how the control is implemented. If the control is not  
 1108 implemented, ensure that all the failures that would be mitigated by the recommended  
 1109 control are being mitigated by one or more alternate controls. Perform a risk analysis to  
 1110 determine the adequacy of the alternate control(s).
- 1111 6. For each possible failure that is not mitigated, perform a risk analysis that determines the  
 1112 probability of the failure occurring and the cost if the failure does occur.  
 1113
- 1114

1115 **Appendix D: Glossary and**  
1116 **Acronyms**

---

1117 Many of the definitions in this section have been adapted or directly quoted from Smart  
1118 Grid Today's Glossary of Terms and Abbreviations.<sup>9</sup>

1119

1120 **ASAP-SG:** Advanced Security Acceleration Project for the Smart Grid. This group has  
1121 been tasked with developing security profiles for the smart grid to accelerate the  
1122 development of security requirements & standards, requiring vendor products with built-  
1123 in security, and provide tools for understanding failure mitigation and RFP language.

1124 **Authentication:** The process of verifying the identity that an entity (e.g., person, or a  
1125 computer system) is what it represents itself to be.

1126 **Authorization:** Specifying access rights to IT or electric power system resources.

1127 **COBIT:** Control Objectives for Information and related Technologies

1128 **CSWG:** Cyber Security Working Group. A sub-group formed under the Smart Grid  
1129 Interoperability Panel to address the cyber security aspects of the Smart Grid  
1130 Interoperability Framework.<sup>10</sup>

---

<sup>9</sup> <http://www.smartgridtoday.com/public/department40.cfm>

<sup>10</sup> <http://collaborate.nist.gov/wiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG>

1131 **Demand Response:** Demand Response, where "demand" is the utility term for the draw  
 1132 of electricity from the electric distribution system and "response" refers to actions taken  
 1133 by utility customers to reduce their demand. This term refers to a type of arrangement  
 1134 between utilities and customers that can take various forms but always refers to the  
 1135 agreement by customers to cut their use of electricity when the utility asks them to, or in  
 1136 some cases customers give the utility permission to remotely change the use of power  
 1137 within the customer's premises. Many DR arrangements are with big industrial  
 1138 consumers that agree to shut down some or all of their power use when the utility alerts  
 1139 them -- often via a phone call -- to a peak demand condition, and often with a financial  
 1140 consideration to mitigate the impact on the business of the customer. Programs for  
 1141 residential customers often use remote controls of thermostats, water heaters, swimming  
 1142 pool pumps and other appliances. Some DR programs offer financial incentives to the  
 1143 customer to have their power use reduced temporarily and others use variable power  
 1144 rates, boosting the cost of power to create an incentive for the customer to reduce power  
 1145 use as peak use times.<sup>9</sup>

1146 **Demand Response Event:** A DR Event consists of the time periods, deadlines, and  
 1147 transitions during which DR Resources perform. A DR Event Schedule consists of a  
 1148 Notification Period, Active Event Period, Ramp Period and Recovery Period. The Ramp  
 1149 Period is considered part of the Active Event Period. A DR Event can be partitioned into  
 1150 a continuous block of consecutive time periods called intervals. Events can also be open-  
 1151 ended. i.e. a Start Time without duration or end-time.<sup>11</sup>

1152 **DG:** Distributed Generation

1153 **DHS:** Department of Homeland Security

1154 **Distributed Generation:** Power generation that is on the premises of the end user.

1155 **DOD:** Department of Defense

1156 **DMZ:** Demilitarized Zone

1157 **DNMTT:** Data and Network Management Task Team

1158 **DNSSec:** Domain Name System Security Extensions

1159 **DR:** Demand Response

1160 **DSL:** Digital Subscriber Line

1161 **EMS:** Energy Management System

1162 **External Application:** Applications that reside outside of the physical infrastructure of  
 1163 the demand response system.

---

<sup>11</sup> A more detailed definition of DR Event can be found in section "3.4.1 Temporal Model of a DR Event" in UCAIug OpenSG OpenADR Task Force, OpenADR 1.0 System Requirements Specification v1.0, <http://osgug.ucaiug.org/sghsystems/OpenADR/Shared%20Documents/SRS/OpenSG%20OpenADR%201.0%20SRS%20v1.0.pdf>

1164 **External Data Source:** A source of data that does not originate with the electric utility

1165 **Fast Demand Response (FastDR)** is characterized by support of fast dispatch  
 1166 frequencies ranging from 4 seconds to several minutes. One of the intended uses is to  
 1167 support some types of ancillary services that require a response in the 4 second to 10  
 1168 minute range. These services may include:

- 1169 • Regulating Reserve
- 1170 • Load Following or Fast Energy Markets
- 1171 • Spinning Reserve
- 1172 • Non-Spinning Reserve
- 1173 • Replacement or Supplemental Reserve

1174 **FERC:** The Federal Energy Regulatory Commission. An independent agency that  
 1175 regulates the interstate transmission of natural gas, oil, and electricity. FERC also  
 1176 regulates natural gas and hydropower projects.<sup>12</sup>

1177 **FIPS:** Federal Information Processing Standard. Publicly announced standards developed  
 1178 by the United States government.

1179 **Firewall:** A network device designed to block or allow packets based on a pre-  
 1180 determined set of rules.

1181 **Firmware:** Software embedded in a hardware device including in computer chips.

1182 **FMEA:** Failure Modes and Effects Analysis

1183 **FPKI:** Federal Public Key Infrastructure

1184 **FTP:** File Transfer Protocol

1185 **FTPS:** File Transfer Protocol over SSL. FTPS is an extension to the FTP protocol that  
 1186 adds application layer encryption via TLS and SSL. For “Secure FTP” or “SSH File  
 1187 Transfer Protocol”, please see SFTP.

1188 **Gateway:** A network management device that functions as the entry and exit point for a  
 1189 network segment.

1190 **GF:** General Failure

1191 **GPS:** Global Positioning System

1192 **GUID:** Globally Unique Identifier

1193 **HSM:** Hardware Security Module. An external physical type of secure crypto-processor  
 1194 targeted at managing digital keys, accelerating crypto-processes such as digital signings,  
 1195 and for providing strong authentication to access critical keys for server applications.

1196 **HTTP:** Hyper Text Transmission Protocol

---

<sup>12</sup> <http://www.ferc.gov/about/about.asp>

- 1197 **IDS:** Intrusion Detection System. A passive monitoring system used to monitor network  
1198 and/or system activity for malicious activity or policy violations.
- 1199 **IEC:** International Electrotechnical Commission. A non-profit, non-governmental  
1200 international standards organization that prepares and publishes International Standards  
1201 for all electrical, electronic and related technologies – collectively known as  
1202 "electrotechnology."
- 1203 **IED:** Intelligent Electronic Device.
- 1204 **IEEE:** Institute of Electrical and Electronics Engineers. An international non-profit,  
1205 professional organization for the advancement of technology related to electricity.
- 1206 **Information Repository:** Any location where the DM system stores data.
- 1207 **IP:** Internet Protocol. The primary protocol used for network communications in packet-  
1208 switched networks. This protocol is specifically used for node addressing and packet  
1209 routing.
- 1210 **IPS:** Intrusion Prevention System. An active monitoring system, similar to an IDS, used  
1211 to monitor network and/or system activity for malicious activity or policy violations.  
1212 Additionally, an IPS can terminate a connection upon detecting suspicious activity.
- 1213 **IPv4, IPv6:** IP (above) version 4 is the fourth revision of IP based on RFC 791. IPv4  
1214 uses 32-bit addressing with a total of 4,294,967,296 ( $2^{32}$ ) unique addresses. IPv6 is  
1215 designed to supersede IPv4 and uses 128-bit addressing for a total of  $2^{128}$  unique  
1216 addresses.
- 1217 **IR:** Interagency Report
- 1218 **ISO:** International Organization for Standardization
- 1219 **ISO:** Independent System Operator
- 1220 **IT:** Information Technology.
- 1221 **ITIL:** Information Technology Infrastructure Library
- 1222 **LAN:** Local Area Network. A network covering a small physical area.
- 1223 **LIC:** Logical Interface Category
- 1224 **Link:** is a step labeled with the name of some other use case. A link indicates that the  
1225 activity of this use case is followed by the activity of the linked use case.
- 1226 **Load:** Electric utility term for the infrastructure that uses the power the utility distributes  
1227 -- such as homes, businesses, industry and in-the-field equipment -- thus, locating a  
1228 power generation or storage device near load, for example, means putting it close to  
1229 where the power will be used.
- 1230 **Mesh network:** A network technology where each node or end-device can communicate  
1231 with any nearby devices to create "smart" data routing that finds the most efficient path  
1232 for data and can change the path when a node stops working.
- 1233 **MPLS:** Multiprotocol Label Switching

- 1234 **Multi-factor Authentication:** Similar to two-factor authentication, using two or more  
 1235 independent methods, something you have (token or smart card), something you know  
 1236 (password or passcode), and something you are (biometric), for authentication.
- 1237 **NDA:** Non-Disclosure Agreement.
- 1238 **NERC:** North American Electric Reliability Corporation. A self-regulatory, non-  
 1239 government organization which has statutory responsibility to regulate bulk power  
 1240 system users, owners, and operators through the adoption and enforcement of standards  
 1241 for fair, ethical and efficient practices.<sup>13</sup>
- 1242 **Network Equipment:** Equipment implementing any intermediary function specifically  
 1243 aimed at facilitating or brokering exchange of synchrophasor data between organizations  
 1244 is in scope.
- 1245 **Network Segment:** In networking, this is a network segment where all devices  
 1246 communicate using the same physical layer. Within WAMPAC, some switching devices  
 1247 may be used to extend the segment which is defined by the role of the devices in that  
 1248 segment.
- 1249 **NIST:** National Institute of Standards & Technology. An office of the US Dept of  
 1250 Commerce, it handles standards and technology issued for the federal government  
 1251 including being tasked in the Energy Independence & Security Act of 2007 with heading  
 1252 up an effort to set interoperability standards for the smart grid industry.(www.nist.gov)
- 1253 **NOAA:** National Oceanic and Atmospheric Administration
- 1254 **Non-WAMPAC Application:** This is a utility operated application that does not rely  
 1255 critically on time-synchronized phasor measurements for its primary task.
- 1256 **NTP:** Network Time Protocol
- 1257 **Open SG:** Open Smart Grid users group – part of the UCA International users group.<sup>14</sup>
- 1258 **OMG UML:** Object Management Group
- 1259 **Operations Center Equipment:** Equipment in the Operations or Control Center that  
 1260 internalizes and processes phasor data in the course of performing synchrophasor  
 1261 application functionality is in scope.
- 1262 **Optional flows:** An optional flow indicates a flow that may or may not always happen in  
 1263 a use case.
- 1264 **OWASP:** Open Web Application Security Project
- 1265 **Phasor Gateway:** This is software that bridges one or more utility networks for the  
 1266 purpose of exchanging phasor measurement data.
- 1267 **PKI:** Public Key Infrastructure

<sup>13</sup> <http://www.nerc.com/page.php?cid=1>

<sup>14</sup> <http://osgug.ucaiug.org/org/default.aspx>

1268 **Private Network:** In networking this refers to networks using private IP space as defined  
1269 by RFC 1918. Within electric power systems this refers to networks owned, operated or  
1270 controlled by the utility or retail electric provider.

1271 **Public Network:** In networking this refers to networks using publicly-addressable IP  
1272 space which can be routed via the Internet. Within electric power systems this refers to  
1273 networks not owned, operated, or controlled by the utility or retail electric provider.

1274 **QoS:** Quality of Service. In an IP network QoS provides guaranteed resource reservation  
1275 to provide different priorities to different applications, users, or data flows, or to  
1276 guarantee a certain level of performance to a data flow.

1277 **Reference Architecture:** Abstraction of solution architectures have been successfully  
1278 used to address similar requirements.

1279 **RF:** Radio Frequency. Used as a generic term in many industries to describe radio  
1280 signals used for networking and even those signals that cause interference.

1281 **RFC:** Request for Comments

1282 **RPN:** Risk Priority Number. A measurement used when assessing risk in the FMEA  
1283 process, which equals (Severity x Occurrence x Detection).

1284 **RFP:** Request for Proposal.

1285 **RTO:** Regional Transmission Organization

1286 **RTU:** Remote Terminal Unit. A unit that collects data from electrical devices, such as  
1287 meters, in real time.

1288 **SAMATE:** Software Assurance Metrics and Tool Evaluation

1289 **SCADA:** Supervisory Control and Data Acquisition. A system used by power utilities to  
1290 gather data from and issue commands to devices in the field.

1291 **SCP:** Secure Copy. SCP is an extension to the SSH protocol to implement a secure  
1292 replacement for Remote Copy (RCP).

1293 **SCL:** Substation Configuration Language<sup>15</sup>

1294 **SFTP:** SSH File Transfer Protocol, also known as Secure FTP. SFTP is an IETF  
1295 extension to the Secure Shell (SSH) protocol to implement a secure replacement for FTP.  
1296 For “FTP over SSL”, please see FTPS.

1297 **SG Security:** Smart Grid Security working group within Open SG.

1298 **SGIP:** Smart Grid Interoperability Panel<sup>16</sup>

1299 **Sensor:** A sensor is a device that collects information such as voltage, temperature, or  
1300 device status.

---

<sup>15</sup> As defined in IEC 61850

<sup>16</sup> <http://www.nist.gov/smartgrid/>



- 1301 **Smart grid:** The utility power distribution grid enabled with computer technology and  
 1302 two-way digital communications networking. The term encompasses the ever-widening  
 1303 palette of utility applications that enhance and automate the monitoring and control of  
 1304 electrical distribution networks for added reliability, efficiency and cost effective  
 1305 operations.
- 1306 **SOC:** Security Operations Center. Often incorporated with the network operations center,  
 1307 but designed to monitor security logging and security-related events.
- 1308 **Step:** indicates the activities performed by a role during a use case
- 1309 **Substation:** An electrical substation is a subsidiary station of an electricity generation,  
 1310 transmission and distribution system where voltage is transformed from high to low or  
 1311 the reverse using transformers. Electric power may flow through several substations  
 1312 between generating plant and consumer, and may be changed in voltage in several  
 1313 steps.<sup>17</sup>
- 1314 **TCP, TCP/IP:** Transmission Control Protocol. Usually written with internet protocol as  
 1315 TCP/IP and the two make up the suite of protocols that are used to communicate via the  
 1316 Internet.
- 1317 **TLS:** Transport Layer Security
- 1318 **TO:** Transmission Owner, as defined by NERC
- 1319 **TPM:** Trusted Platform Module. The name of a published specification detailing a secure  
 1320 crypto-processor that can store cryptographic keys that protect information, as well as the  
 1321 general name of implementations of that specification, often called the "TPM chip" or  
 1322 "TPM Security Device"
- 1323 **Two-Factor Authentication:** The act of using two independent authorization methods.  
 1324 Examples are mixing something you have (token or smart card), something you know  
 1325 (password or passcode), and something you are (biometric).
- 1326 **UCAIug:** UCA International Users Group. A not-for-profit corporation focused  
 1327 on assisting users and vendors in the deployment of standards for real-time applications  
 1328 for several industries with related requirements. The Users Group does not write  
 1329 standards, however works closely with those bodies that have primary responsibility for  
 1330 the completion of standards (notably IEC TC 57: Power Systems Management and  
 1331 Associated Information Exchange).<sup>18</sup>
- 1332 **UML:** Universal Modeling Language
- 1333 **UPS:** Universal Power Supply
- 1334 **URL:** Universal Resource Locator

<sup>17</sup> [http://en.wikipedia.org/wiki/Electrical\\_substation](http://en.wikipedia.org/wiki/Electrical_substation)

<sup>18</sup> <http://www.ucaiug.org/default.aspx>

- 1335 **USB:** Universal serial bus, a cable system with rectangular plugs used to connect a wide  
 1336 variety of devices to computers and computer peripherals.
- 1337 **VLAN:** Virtual Local Area Network. A method of segmenting and routing traffic  
 1338 between devices on an IP network so that they communicate as if they were attached to  
 1339 the same broadcast domain, regardless of their physical location.
- 1340 **VOIP:** Voice over Internet Protocol.
- 1341 **VPN:** Virtual Private Network. A VPN encapsulates data transfers between two or more  
 1342 networked devices not on the same private network so as to protect the transferred data  
 1343 from other devices on one or more intervening local or wide area networks.
- 1344 **WAMPAC:** Wide-Area Monitoring, Protection, and Control
- 1345 **WAN:** Wide Area Network. A computer network that covers a broad geographic area.
- 1346 **WASA:** Wide-area Situational Awareness
- 1347 **WECC:** Western Electricity Coordinating Council
- 1348 **WiFi:** Wireless Fidelity -- a standard for sending and receiving data -- such as in a home  
 1349 or small office network or LAN (or even an entire city). The standard includes a number  
 1350 of sub-standards under the IEEE's 802.11 standards.

1351

## **Appendix E: References**

---

- 1352 Mary Ann Piette, Girish Ghatikar, Sila Kiliccote, Ed Koch, Dan Hennage, Peter  
1353 Palensky, and Charles McParland. 2009. *Open Automated Demand Response*  
1354 *Communications Specification (Version 1.0)*. California Energy Commission, PIER  
1355 Program. CEC-500-2009-063. <http://openadr.lbl.gov/index.html>
- 1356 UCAIug OpenSG OpenADR Task Force, *OpenADR 1.0 System Requirements*  
1357 *Specification v1.0*,  
1358 [http://osgug.ucaiug.org/sgsystems/OpenADR/Shared%20Documents/SRS/OpenSG%20](http://osgug.ucaiug.org/sgsystems/OpenADR/Shared%20Documents/SRS/OpenSG%20OpenADR%201.0%20SRS%20v1.0.pdf)  
1359 [penADR%201.0%20SRS%20v1.0.pdf](http://osgug.ucaiug.org/sgsystems/OpenADR/Shared%20Documents/SRS/OpenSG%20OpenADR%201.0%20SRS%20v1.0.pdf)
- 1360 UCAIug OpenSG Service Definition Team, *OpenADR 1.0 Service Definition - Common*  
1361 *Version :R0.91*,  
1362 [http://osgug.ucaiug.org/sgsystems/OpenADR/Shared%20Documents/Services/OpenSG%](http://osgug.ucaiug.org/sgsystems/OpenADR/Shared%20Documents/Services/OpenSG%20OpenADR%20SD%20-%20Common%20r0.91.doc)  
1363 [20OpenADR%20SD%20-%20Common%20r0.91.doc](http://osgug.ucaiug.org/sgsystems/OpenADR/Shared%20Documents/Services/OpenSG%20OpenADR%20SD%20-%20Common%20r0.91.doc)
- 1364 UCAIug OpenSG Service Definitions Team, *OpenADR 1.0 Service Definition – Web*  
1365 *Services Implementation Profile Version: v0.91*  
1366 [http://osgug.ucaiug.org/sgsystems/OpenADR/Shared%20Documents/Services/OpenSG%](http://osgug.ucaiug.org/sgsystems/OpenADR/Shared%20Documents/Services/OpenSG%20OpenADR%20SD%20-%20WS%20r0.91.doc)  
1367 [20OpenADR%20SD%20-%20WS%20r0.91.doc](http://osgug.ucaiug.org/sgsystems/OpenADR/Shared%20Documents/Services/OpenSG%20OpenADR%20SD%20-%20WS%20r0.91.doc)
- 1368 OASIS, *Energy Interoperation Version 1.0 Working Draft 2*[working draft – convert  
1369 reference to latest specification when available]
- 1370 ASAP-SG. (2009, December 14). Security Profile Blueprint. Knoxville, Tennessee,  
1371 United States of America. Retrieved 1 28, 2010, from Open Smart Grid - OpenSG > SG  
1372 Security: <http://osgug.ucaiug.org/utilisec>

1373 U.S. Department of Homeland Security. (2010, March). *Catalog of Control Systems*  
1374 *Security: Recommendations for Standards Developers*. Arlington, Virginia, United States  
1375 of America. [http://www.us-](http://www.us-cert.gov/control_systems/pdf/Catalog%20of%20Control%20Systems%20Security%20-%20Recommendations%20for%20Standards%20Developers%20June-2010.pdf)  
1376 [cert.gov/control\\_systems/pdf/Catalog%20of%20Control%20Systems%20Security%20-](http://www.us-cert.gov/control_systems/pdf/Catalog%20of%20Control%20Systems%20Security%20-%20Recommendations%20for%20Standards%20Developers%20June-2010.pdf)  
1377 [%20Recommendations%20for%20Standards%20Developers%20June-2010.pdf](http://www.us-cert.gov/control_systems/pdf/Catalog%20of%20Control%20Systems%20Security%20-%20Recommendations%20for%20Standards%20Developers%20June-2010.pdf)

1378 BSI Group, Department of Trade and Industry, United Kingdom. *BS 7799 Best practices*  
1379 *for Information Security Management (1998) and BS 7799 Part 2: Information Security*  
1380 *management Systems – Specification with Guidance for use*.

1381 Control Objectives for Information and related Technologies:  
1382 <http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx>

1383 Hinden, R. and Haberman, B. (2005). *RFC 4193: Unique Local IPv6 Unicast Addresses*

1384 Institute of Electrical and Electronics Engineers, Inc. (2003). Standards [as listed below],  
1385 New York, New York.

1386 *IEEE Std 1613-2003, Standard Environmental and Testing Requirements for*  
1387 *Communications Networking Devices in Electric Power Substations*

1388 *IEEE C37.118 Synchrophasor Protocol*

1389 International Electrotechnical Commission. Standards [as listed below]. Geneva,  
1390 Switzerland

1391 *IEC 61850 “Communication Networks and Systems in Substations”*

1392 *IEC 61850-90-5 “Use of IEC 61850 to transmit synchrophasor information according to*  
1393 *IEEE C37.118” (Draft Technical Specification)*

1394 *IEC 62351 “Information Security for Power System Control Operations”*

1395 International Standard Organization *ISO/IEC 27000:2009. Information technology –*  
1396 *Security Techniques – Information Security Management Systems – Overview and*  
1397 *Vocabulary*. Geneva, Switzerland

1398 Quanta Technology LLC, *Phasor Gateway Technical Specification for North American*  
1399 *Synchro-Phasor Initiative Network (NASPInet)*, May 29, 2009, page 1-4 (PDF page 11).  
1400 Available at: <http://www.naspi.org/naspinet.stm>

1401 Quanta Technology LLC, *Data Bus Technical Specification for North American Synchro-*  
1402 *Phasor Initiative Network (NASPInet)*, May 29, 2009, page 1-4 (PDF page 11).  
1403 Available at: <http://www.naspi.org/naspinet.stm>

1404 Seacord, Robert C., (2008, October). *The CERT C Secure Coding Standard*. Addison-  
1405 Wesley.

1406 National Institute of Standards and Technology, Department of Commerce, United States  
1407 of America. *Interagency Report 7628: Guidelines for Smart Grid Cyber Security*.  
1408 Gaithersburg, Maryland.

1409 National Institute of Standards and Technology, Department of Commerce, United States  
1410 of America. *Special Publication SP 800-53: FPKI Security Controls for PKI Systems and*

1411 *SP 800-53A: Assessment Guidance for Security Controls in PKI Systems*. Gaithersburg,  
 1412 Maryland.

1413 National Institute of Standards and Technology, Department of Commerce, United States  
 1414 of America. Federal Information Processing Standards (FIPS) [as listed below, available  
 1415 at <http://csrc.nist.gov/publications/PubsFIPS.html>]. Gaithersburg, Maryland.

1416 OMG Unified Modeling Language (OMG UML), UML Superstructure Specification,  
 1417 Version 2.3. Online at <http://www.omg.org/spec/UML/2.3/Superstructure/PDF/>

1418 *FIPS 140-2 Security Requirements for Cryptographic Modules, May 2001*

1419 *FIPS 186-3 Digital Signature Standard (DSS), June 2009*

1420 *FIPS 112 Password Usage, May 1985*

1421 *FIPS 180 Secure Hash Standard, October 2008*

1422 North American SynchroPhasor Initiative. Data and Network Management Task Team.  
 1423 <http://www.naspi.org/resources/dnmtt/dnmttresources.stm>

1424 OWASP: Open Web Application Security Project Development Guide.  
 1425 [https://www.owasp.org/index.php/Guide\\_Table\\_of\\_Contents](https://www.owasp.org/index.php/Guide_Table_of_Contents)

1426 Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., Lear, E. (1996). *RFC:*  
 1427 *1918:Address Allocation for Private Internets*

1428

1429 **Appendix F: OpenADR**  
1430 **Cryptographic Security Profile**

---

1431 The purpose of this document is to specify the cryptographic algorithms (security  
1432 controls) for use with OpenADR 2.0. The set of controls includes:

- 1433 • Hash
- 1434 • Public Key
- 1435 • Symmetric key
- 1436 • Key exchange/key agreement

1437

1438 Transport Layer Security (TLS) 1.2 is used to provide the secure transport for OpenADR.  
1439 The cryptographic algorithms defined in Section 0 are to be used with TLS.

1440 **F.1 Method**

1441 NISTIR 7628, Subsection 4.2 - Cryptography and key management Solutions and Design  
1442 Considerations - provides broad guidance on the use of cryptography within the smart  
1443 grid.

1444 This analysis looked at the specific data exchanged under OpenADR and considered the  
1445 volume of data as well as requirements for confidentiality, availability, integrity and non-  
1446 repudiation.

1447 FIPS 140-2 specifies requirements for validating cryptographic implementations for  
 1448 conformance to the FIPS and SPs. The validation of the cryptographic implementations is  
 1449 outside the scope of this document. Vendors who have validated cryptographic modules  
 1450 may be found at <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>

1451 The algorithms selection process considered

- 1452 • Ensuring adequate security
- 1453 • Minimizing overhead
- 1454 • Promoting interoperability.

1455 **F.2 References**

- 1456 • IETF RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2, Aug  
 1457 2008
- 1458 • NISTIR 7628, Guidelines for Smart Grid Cyber Security:
  - 1459 ○ Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level  
 1460 Requirements,
  - 1461 ○ Vol. 2, Privacy and the Smart Grid
  - 1462 ○ Vol. 3, Supportive Analyses and References
- 1463 • NIST FIPS 180-3 Secure Hash Algorithm (SHA)  
 1464
- 1465 • NIST FIPS 186-3, Digital Signature Algorithm (ECDSA)
- 1466 • NIST FIPS 197 - Advanced Encryption Standard
- 1467 • NIST SP 800-57, Recommendation for Key Management Part 1
- 1468 • NIST SP 800-90, Recommendation for Random Number Generation Using Deterministic  
 1469 Random Bit Generators (Revised).  
 1470
- 1471 • NIST SP 800-22, A Statistical Test Suite for Random and Pseudorandom Number  
 1472 Generators for Cryptographic Applications
- 1473
- 1474 • NIST SP 800-107, Recommendation for Applications Using Approved Hash Algorithms  
 1475
- 1476 • NIST SP 800-131A, Transitions: Recommendation for Transitioning the Use of  
 1477 Cryptographic Algorithms and Key Lengths, January 2011
- 1478

1479 **F.3 Hash**

1480 **Considerations**

- 1481 • The OpenADR data to be hashed has a relatively short lifetime (typically less than  
1482 60 days).
- 1483 • The data has a moderate amount of structure to it making it more difficult for an  
1484 attacker to create a meaningful collision.
- 1485 • SHA-256 provides an estimated collision resistance of 128 bits which is  
1486 consistent with the NIST recommended AES key length.

1487 **Recommendation**

- 1488 • SHA-256 as specified in NIST FIPS 180-3 shall be used.
- 1489 • The guidelines provided in NIST SP 800-107 are to be applied.

1490 **F.4 Symmetric Encryption**

1491 **Considerations**

1492 **Probable plaintext/ciphertext**

1493 Much of the data pulled down from the website will be the same for multiple recipients.  
1494 Thus, an attacker could establish one legitimate account and observe a set of plaintext. It  
1495 is reasonable for the attacker to assume that other users accessing the web server will  
1496 initially receive similar data (e.g. the home page). This provides the attacker with  
1497 probable plaintext/ciphertext.

1498 This threat is offset by the fact that HTTPS (TLS) will establish a new key for each  
1499 session. Thus, the lifetime of the key is limited. In addition, the value of data fades  
1500 quickly with time. It is tactical, not strategic.

1501 **Volume**

1502 Volume of data to be exchanged is relatively small compared to the amount of data that  
1503 can safely be encrypted using modern block ciphers.

1504

1505 **Recommendation**

- 1506 • AES 128 as specified in NIST FIPS 197 shall be used.
- 1507 • The use of stream ciphers in the context of OpenADR is prohibited.

1508



1509 **F.5 Public Key/Digital Signature**

1510 **Considerations**

1511 After December 31, 2013, key lengths providing less than 112 bits of security strength  
1512 shall not be used to generate digital signatures.

1513

1514 Keys used by certification authorities to sign certificates shall be longer than the keys  
1515 used by servers in establishing secure sessions with clients.

1516

1517 The Transport Layer Security (TLS, RFC 5246) protocol will be used within the context  
1518 of OpenADR.

1519

1520 **Recommendations**

1521 For User Certificates containing elliptic curve public keys:

1522 Certification authorities signing server certificates: ECDSA-P384, SHA-384

1523 Operations other than certification authority certificate signing

- 1524 • Key establishment - ECDHE P-256
- 1525 • Server authentication - ECDSA P-256
- 1526 • Signatures - ECDSA P-256

1527

1528 For User Certificates containing RSA public keys:

1529 Certification authorities signing server certificates: RSA 3072

1530 Operations other than certification authority certificate signing

- 1531 • Key establishment – RSA 2048
- 1532 • Server authentication – RSA 2048
- 1533 • Signatures – RSA 2048

1534

1535 **Cipher Suites**

1536 Some protocols (e.g., TLS) specify a suite of protocols to be used together. When TLS  
1537 1.2 is used in the context of OpenADR the following one of the following cryptographic

1538 suites shall be used. The selection of the specific Cipher Suite is at the discretion of the  
1539 implementing organizations.

1540

<b>Suite</b>	<b>Message Authentication Code (MAC)</b>	<b>Pseudorandom Function (PRF)</b>
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Galois Ctr.	P_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256	Galois Ctr.	P_SHA256

1541

1542

1543