SECURITY PROFILE FOR OPENADR

Prepared for:

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

Prepared by:

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

Managed by:

UCAIug OpenADR Task Force

Version
0.02

Revision History

Rev	Date	Summary	Marked
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 defintions; 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

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.

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

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.

Table of Contents

INTRODUCTION 10

1.1 SCOPE 11
1.1.1 Explicit Exclusions 12
1.2 APPROACH 12
1.3 AUDIENCE & RECOMMENDED USE 14
1.3.1 Electric Utility and Demand Response Aggregators 15
1.3.2 OpenADR Vendors 15

2 FUNCTIONAL ANALYSIS 16

2.1 LOGICAL ARCHITECTURE 17
2.2 ROLE DEFINITIONS 19
2.2.1 Demand Response (DR) Controlling Entity 19
2.2.2 Demand Response (DR) Resource 20
2.2.3 Demand Response (DR) Asset 20
2.3 ROLE MAPPINGS 21
2.4 USE CASES 21
Use Case 1: Demand Response Resource Registers with a Demand Response Controlling Entity 24
Use Case 2: DR Controlling Entity Notifies DR Resource of DR Event (Point-to-point Push) 26
Use Case 3: DR Controlling Entity Notifies DR Resource of DR Event – (Broadcast) 28
Use Case 4: DR Resource Requests New DR Event from DR Controlling Entity (Point-to-point Pull) 30
Use Case 5: DR Resource Requests New DR Event from DR Controlling Entity (Anonymous Pull) 32
Use Case 6: DR Controlling Entity Schedules DR Resource for Periodic Feedback (Point-to-point Push) 34
Use Case 7: DR Resource Notifies DR Controlling Entity of Event Performance with Feedback by Request (Point-to-point Pull) 36
Use Case 8: DR Resource Notifies DR Controlling Entity of Event Performance with Feedback Self-Scheduled (Point-to-point Push) 38

3 FAILURE ANALYSIS 40

3.1 FAILURE ANALYSIS PROCESS 40
3.2 SECURITY AND OPERATIONAL OBJECTIVES 41
3.2.1 Contextual Assumptions 42
3.2.2 Security Principles 43
3.3 FAILURES 45

4 SECURITY CONTROLS 50

4.1 SCOPE OF SECURITY CONTROLS 50
4.2 CONTROL DEFINITIONS 51
4.2.1 Access Control 53
4.2.2 Audit and Accountability 54
4.2.3 Configuration Management 55
4.2.4 Continuity of Operation 56
4.2.5 Identification & Authentication 57
4.2.6 Physical & Environment Security 58
4.2.7 System & Communications Protection 58
4.2.8 System & Information Integrity 60

4.2.9 Controls Mapped to Roles 61

APPENDIX A: RELATION TO THE NIST INTERAGENCY REPORT 7628 65

A.1 TRACEABILITY 65
A.2 NIST IR 7628 ACTORS TO WAMPAC ROLES MAPPING 66
A.3 NIST IR 7628 SECURITY OBJECTIVES TO OPEN ADR SECURITY PRINCIPLES MAPPING 68
A.4 NIST IR 7628 TECHNICAL REQUIREMENTS MAPPED OPEN ADR CONTROLS 69

APPENDIX B: USE CASE NOTATION GUIDE 78

APPENDIX C: USING THE SECURITY PROFILE TO EVALUATE AN OPENADR DEPLOYMENT 80

APPENDIX D: GLOSSARY AND ACRONYMS 82

APPENDIX E: REFERENCES 90

APPENDIX F: OPENADR CRYPTOGRAPHIC SECURITY PROFILE 93

F.1 METHOD 93
F.2 REFERENCES 94
F.3 HASH 95
CONSIDERATIONS 95
RECOMMENDATION 95
F.4 SYMMETRIC ENCRYPTION 95
CONSIDERATIONS 95
RECOMMENDATION 95
F.5 PUBLIC KEY/DIGITAL SIGNATURE 96
CONSIDERATIONS 96
RECOMMENDATIONS 96
CIPHER SUITES 96

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 66
FIGURE 8 – UNIFIED LOGICAL ARCHITECTURE FOR OPENADR 67
FIGURE 9 – AN ANNOTATED SEQUENCE DIAGRAM 79

Diagram: Use Case 1: Register DR Resource 25
Diagram: Use Case 2: DR Event Notification 27
Diagram: Use Case 3: DR Event Notification – Broadcast 29
Diagram: Use Case 4: DR Resource Requests DR Controlling Entity for New DR Event 31
Diagram: Use Case 5: Anonymous DR Resource Requests DR Controlling Entity for New DR Event 33
Diagram: Use Case 6: DR Controlling Entity Schedules DR Resource for Periodic Feedback 35
Diagram: Use Case 7: DR Resource Notifies DR Controlling Entity of Event Performance (Feedback) 37
Diagram: Use Case 8: DR Resource Notifies DR Controlling Entity of Event Performance with Feedback Self-Scheduled 39

Table of Tables

TABLE 1 – CONTROLS: ACCESS CONTROL 53
TABLE 2 – CONTROLS: AUDIT AND ACCOUNTABILITY 54
TABLE 3 - CONTROLS: CONFIGURATION MANAGEMENT 55
TABLE 4 - CONTROLS: CONTINUITY OF OPERATIONS 56
TABLE 5 - CONTROLS: IDENTIFICATION & AUTHENTICATION 57
TABLE 6 - CONTROLS PHYSICAL & ENVIRONMENT SECURITY 58
TABLE 7 - CONTROLS: SYSTEM & COMMUNICATIONS PROTECTION 58
TABLE 8 - CONTROLS: SYSTEM & INFORMATION INTEGRITY 60
TABLE 9 - CONTROLS MAPPED TO ROLES 61
TABLE 10 – NIST IR 7628 ACTOR TO WAMPAC ROLE MAPPING 68
TABLE 11 - NIST IR 7628 USE CASE OBJECTIVES TO OPENADR SECURITY PRINCIPLES 68
TABLE 12 - NIST IR 7628 TECHNICAL REQUIREMENTS MAPPED TO OPENADR CONTROLS 69

Acknowledgements

Authors

Bruce Bartell

Darren Highfill

Ed Koch

Phillip Lee

Tom Markham

Edited by: Bruce Bartell

Introduction

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

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*[1] to OpenADR systems and technology. While NIST IR 7628 serves as an industry-wide reference that a utility or other OpenADR participants may use as a starting point to identify intersystem-level security requirements, this document provides the next level of detail by specifically addressing the use of OpenADR Signals and defining security controls. The controls presented herein may then, in turn, be satisfied by communications protocol definition-level standards and manufacturing specifications. The underlying approach for developing this document was (1) to draw on existing and developing OpenADR Standards and

[1] 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.

implementations, (2) define the function of these systems by presenting a reference architecture that defines abstract roles and use cases, (3) map the architecture's roles to OpenADR interactions, (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.

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

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

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

1.1 Scope

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

The types of DR interactions in scope are:

- Direct Load Control Signals
- Dispatching of Load Profiles
- DR Related Pricing Signals
- 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.

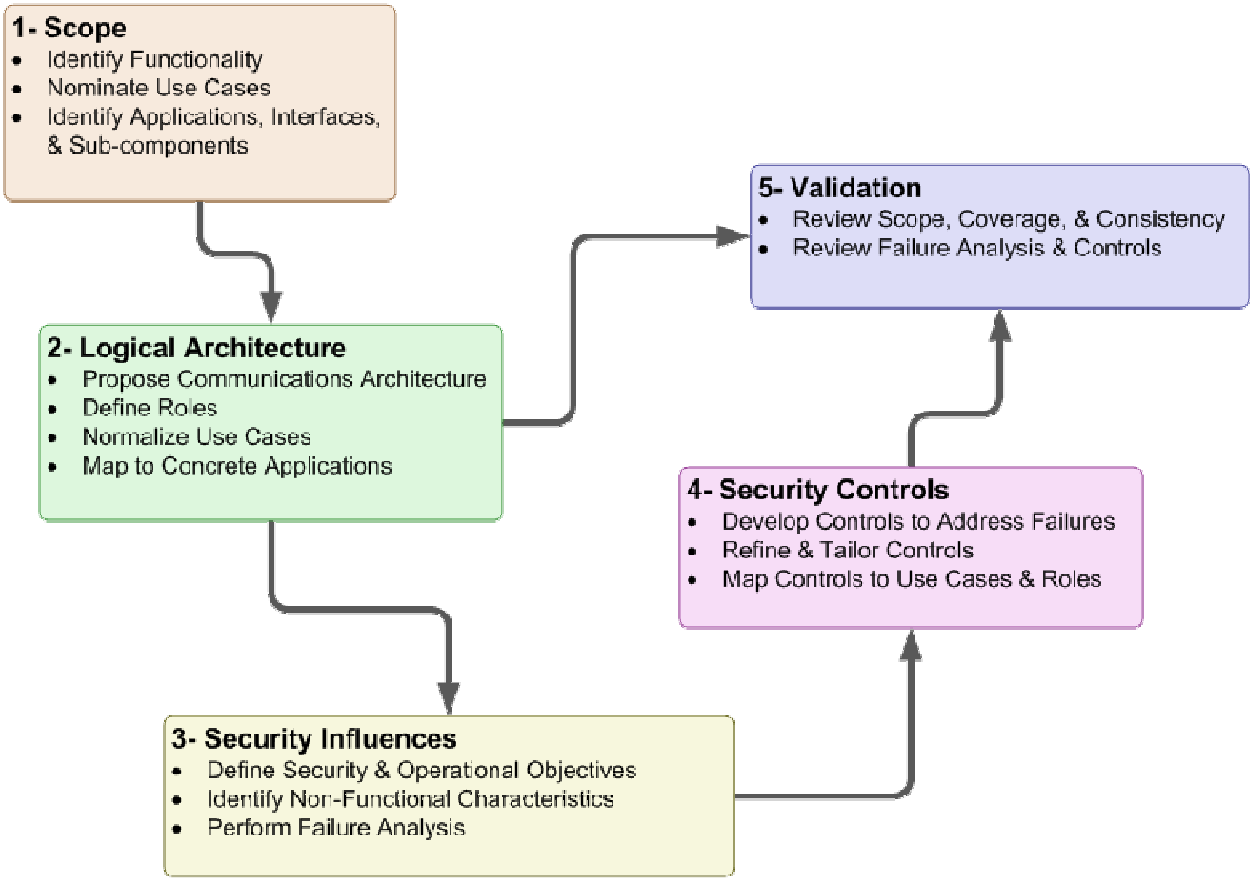


Figure 1 - Overview of Security Profile Development Approach

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

1. *Define the scope of the security profile.* The first step is to decide what aspects of the system are to be included in the security profile. This step requires discussion with stakeholders, consideration of existing and planned systems that will fall within the scope of the profile, and the construction of a conceptual model of those systems that refines and clarifies the statement of scope. The conceptual model includes use cases that define what uses of the system are addressed by the security profile and identifies the roles within those use cases that are the targets of the security guidance to be developed.

2. *Construct a logical architecture showing the relationships between roles in the use cases.* The logical architecture ties the conceptual model developed in step 1 above to architectures and concrete applications familiar to stakeholders. The logical architecture shows which roles and relationships fall within the scope of the profile and which, though appearing in the use cases, may nonetheless fall outside the scope of the profile.

3. *Identify security influences and objectives.* The specific aims of the security profile are defined here in terms of the logical architecture from step 2. These aims include high-level security guidance that the profile will refine, related security guidance that will be tailored for the security profile, and characteristics of the system that must be preserved as security controls are put into place. This step also includes identification of security related failures that may inhibit the operation of the system.

4. *Define the security controls.* New security controls are defined, existing controls from other security documents are referenced, or both to meet the security objectives defined in step 3. Each role is associated with the set of roles it is expected to implement.

5. *Validation.* This step encompasses a collection of validation checks, such as ensuring that the selected controls are complete with respect to the identified failures (i.e., that there is at least one control for each failure) and that there are no superfluous controls (i.e., for each recommended control, there is a failure that it addresses).

The products of these steps are shown in Figure 2.

[2] 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

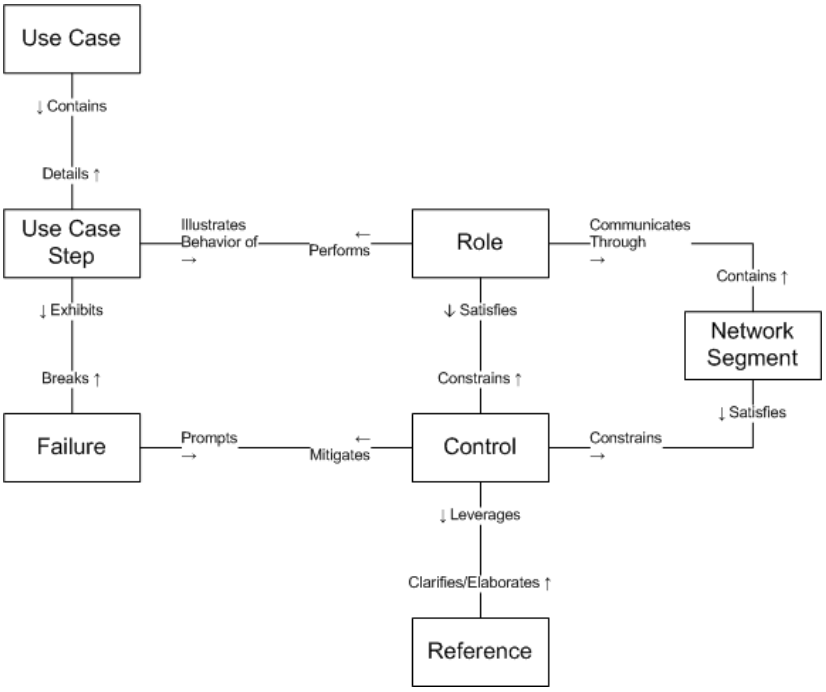


Figure 2 – Artifact Relationships

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

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

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

1.3 Audience & Recommended Use

The primary audience of 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. The user is assumed to be experienced at information asset risk estimation. The user is further assumed to be knowledgeable in applying security requirements and guidance. The user will ultimately

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

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

1.3.1 Electric Utility and Demand Response Aggregators

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

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

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

1.3.2 OpenADR Vendors

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

2 Functional Analysis

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

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

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

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

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

2.1 Logical Architecture

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

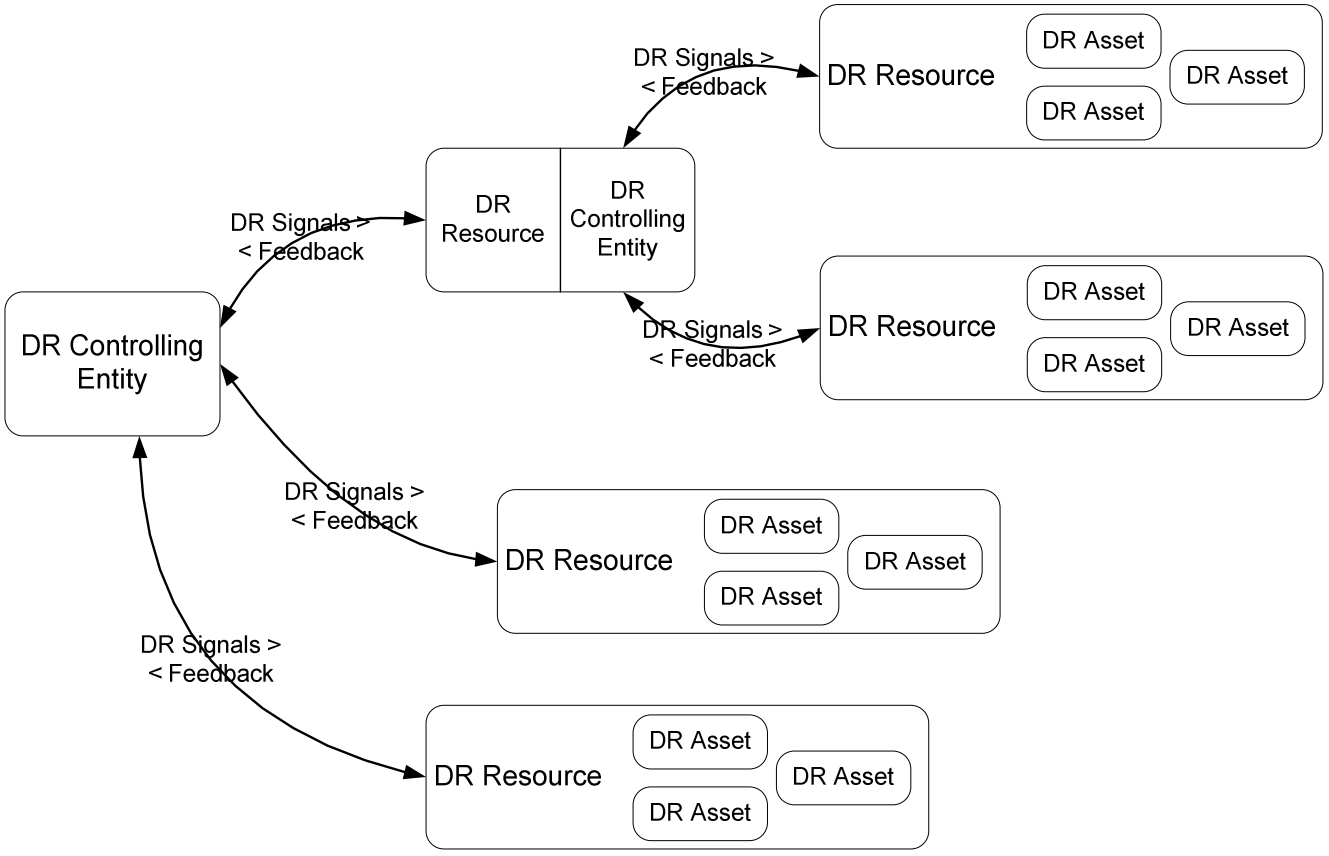


Figure 3 – Role Interaction Diagram

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

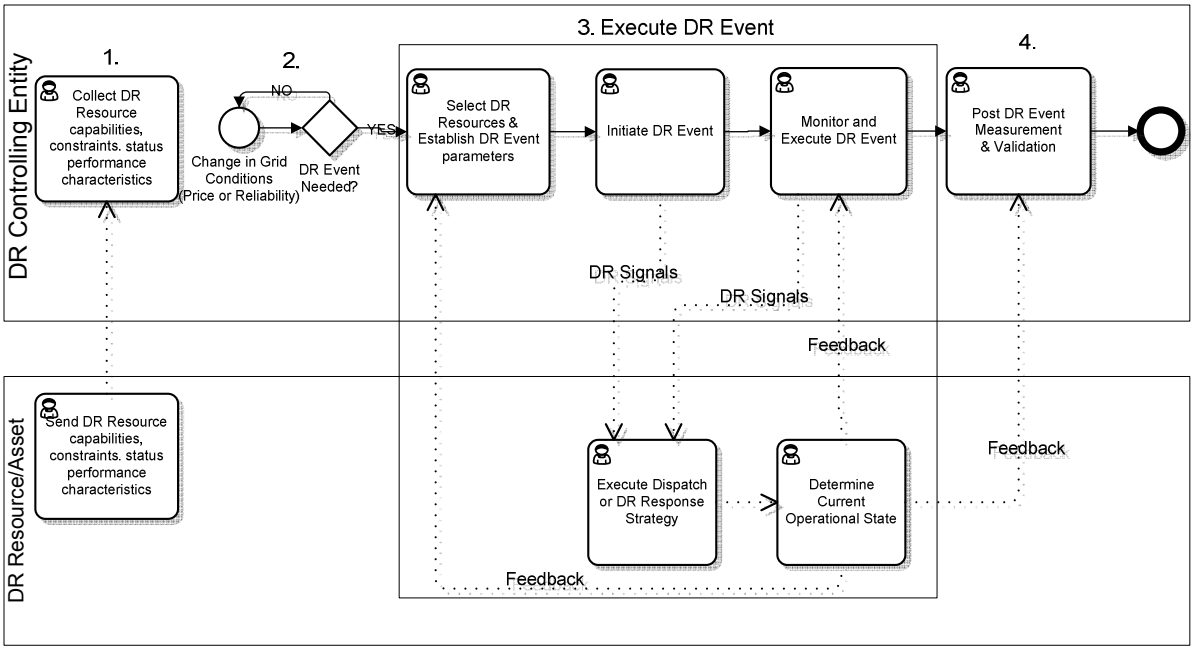


Figure 4 – DR Event Activity Diagram

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

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

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

4. Evaluation of what happened (out of scope for OpenADR)
    - Measurement and & Verification
    - Reconciliation (Billing)

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

2.2 Role Definitions

All roles are defined in the following sub-sections.

2.2.1 Demand Response (DR) Controlling Entity

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

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

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

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

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

2.2.2 Demand Response (DR) Resource

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

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

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

2.2.3 Demand Response (DR) Asset

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

---

[3] Concepts to Enable Advancement of Distributed Energy Resources: White Paper on DER. EPRI, Palo Alto, CA : 2010. 1020432

[4] 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

[5] 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.

2.3 Role Mappings

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

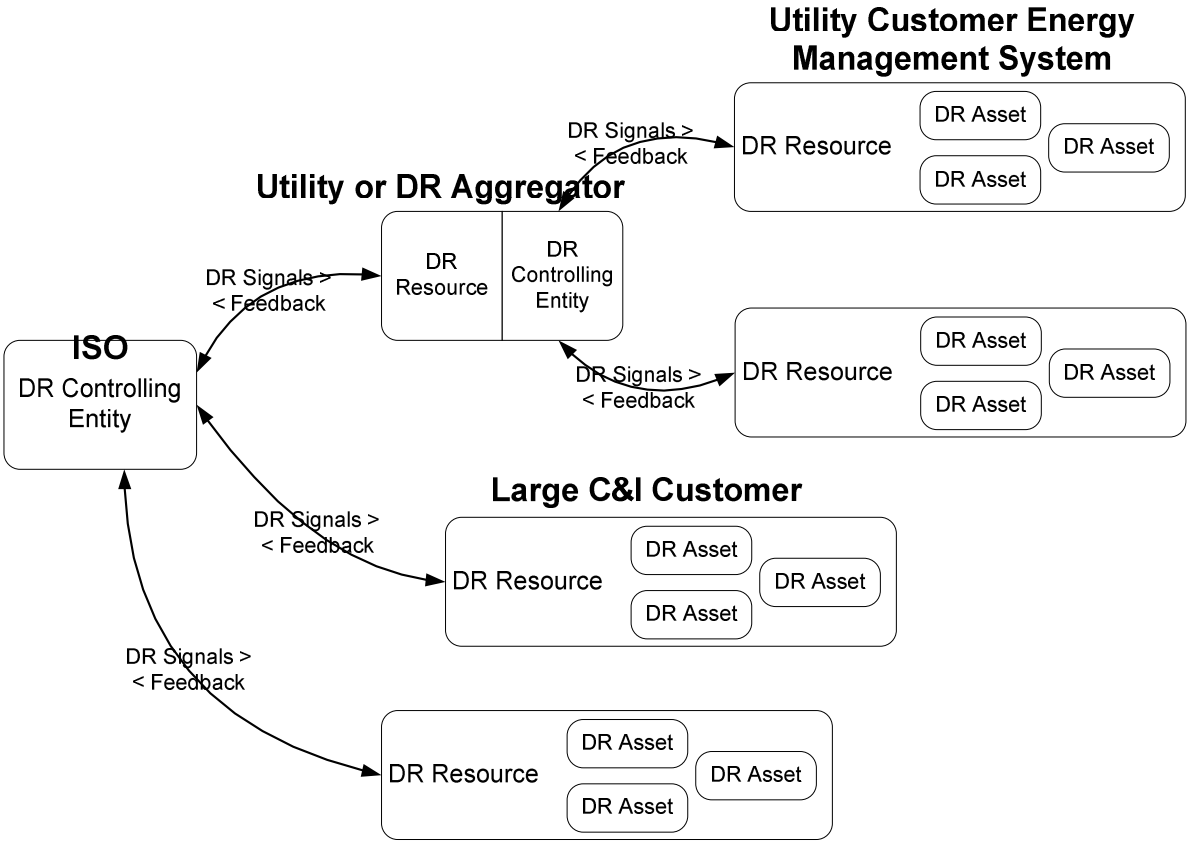


Figure 5 - Role Mapping

2.4 Use Cases

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

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

- Use Case 1 deals with the interactions initiated by a DR Resource to provide the DR Controlling Entity with information on the capabilities and constraints of a DR Resource to participate in DR Events. These include:
    - Notice of capabilities and constraints and subsequent changes these capabilities and constraints.
    - Notice of scheduling constraints based on temporary changes to availability
- Use Cases 2-5 deal with the interactions used by a DR Controlling Entity to manage the DR Resources during the execution of a DR Event. The DR Signals used by a DR Controlling Entity can influence the behavior of a DR Resource through the use of signal types for Objectives, Price, and Direct Load Control. For the purposes of failure analysis the use cases are broken out based on the interaction pattern[6]:
    - Point to Point Push – Point to Point Push is an interaction initiated by the producer or creator of the message. This pattern assumes that the communications is point to point and between entities that are aware of each others identity.
    - Point to Point Pull – Point to Point Pull is an interaction initiated by the message consumer. It requires that a callback can be associated with a request. This pattern assumes that the communications is point to point and between entities that are aware of each others identity.
    - Broadcast – A Broadcast is a message sent to a set of parties where the sender does not know who the recipients may be. Access to the broadcast message could be through a message board, a message broker, or other means. A Broadcast may also be considered an anonymous push.
    - Anonymous Pull – The Anonymous Pull pattern is similar to the point to point pull except that the identity of the consumer is unknown to the sender. It is also assumed that no reply from the consumer is required or expected.
- Use Cases 6-8 deal with Feedback provided by a DR Resource to a DR Controlling Entity during the execution of a DR Event. Feedback interactions use Point-to-point Pull and Point-to-point Push as defined above. Use Cases 7-8 are derivatives of Use Case 6.

These use cases do *not* include security controls, such as the use of authentication or encryption. Security controls and their mapping to the roles performing these use cases are found in Section 4.

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

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

Each use case contains the following elements:

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

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

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

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

Preconditions:

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

Minimal Guarantees:

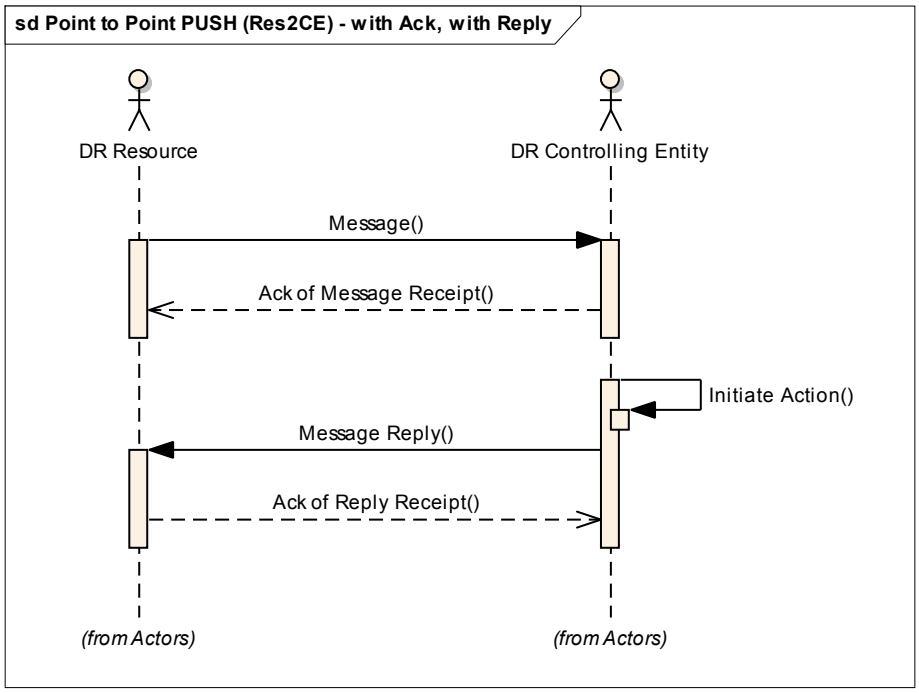
- The DR Resource does not reveal any information to another party that would allow that party to provide any false information to a DR Controlling Entity attributed to the DR Resource.
- The DR Controlling Entity does not process any invalid data.

Success Guarantees:

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

Trigger:

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



412

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

414

415 **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.

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

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

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

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

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

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

Preconditions:

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

Minimal Guarantees:

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

Success Guarantees:

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

Trigger:

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

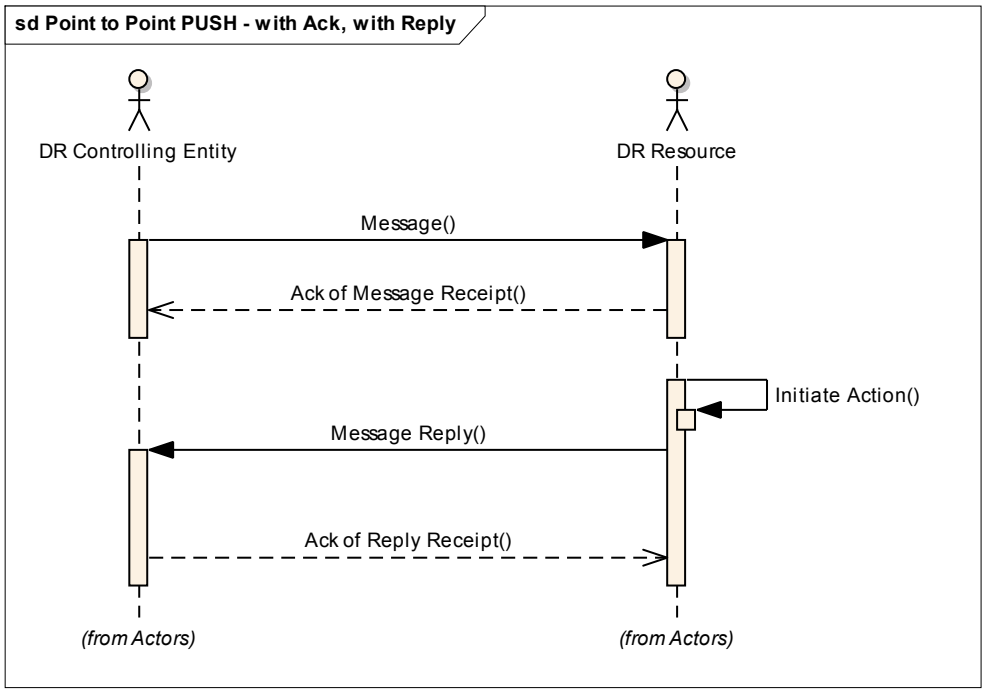


Diagram: Use Case 2: DR Event Notification

Main Success Scenario:

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

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

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

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

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

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

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

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

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

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

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

Preconditions:

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

Minimal Guarantees:

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

Success Guarantees:

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

Trigger:

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

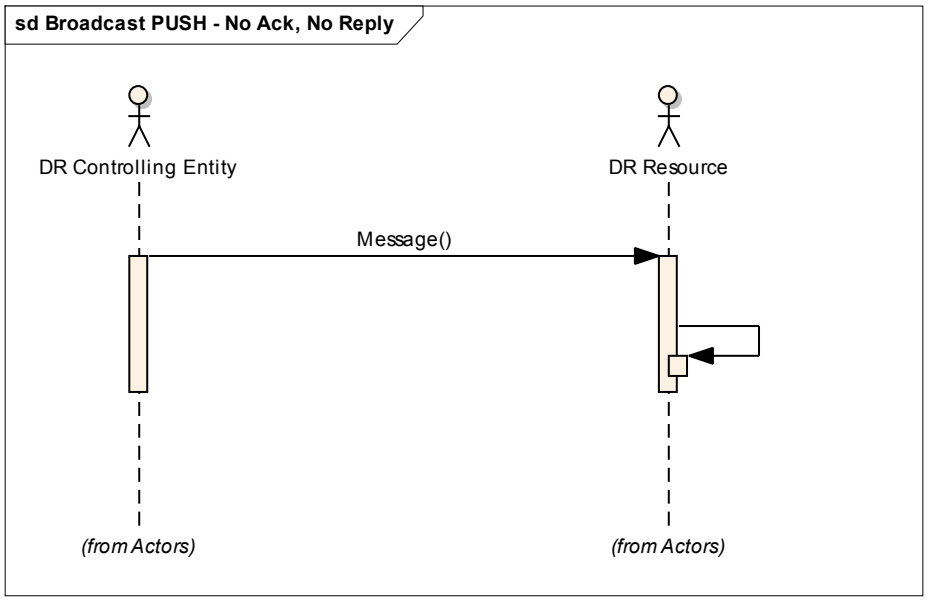


Diagram: Use Case 3: DR Event Notification – Broadcast

Main Success Scenario:

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

2: The DR Resource receives the DR Event message.

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

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

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

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

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

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

Preconditions:

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

Minimal Guarantees:

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

Success Guarantees:

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

Trigger:

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

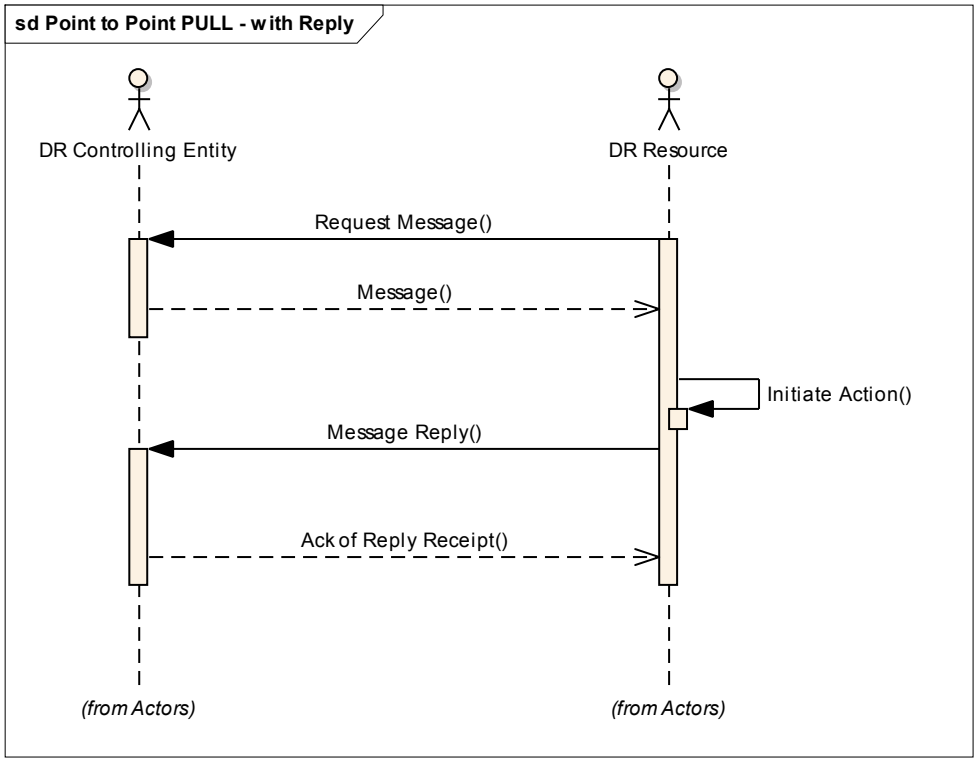


Diagram: Use Case 4: DR Resource Requests DR Controlling Entity for New DR Event

Main Success Scenario:

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

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

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

4: DR Resource receives the DR Event Notification.

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

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

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

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

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

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

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

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

Preconditions:

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

Minimal Guarantees:

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

Success Guarantees:

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

Trigger:

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

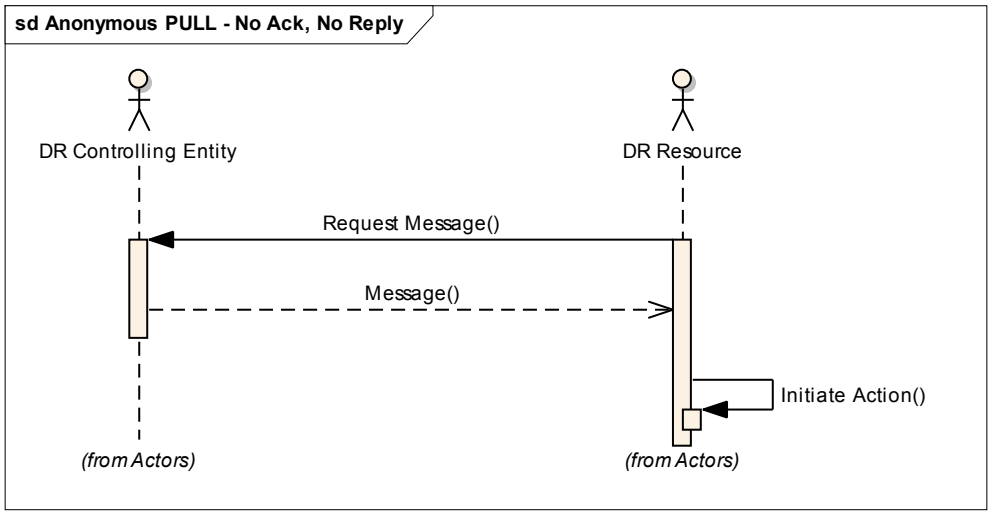


Diagram: Use Case 5: Anonymous DR Resource Requests DR Controlling Entity for New DR Event

Main Success Scenario:

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

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

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

4: DR Resource receives the DR Event Notification.

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

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

This use case is comprised of three interaction patterns:

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

Preconditions:

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

Minimal Guarantees:

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

Success Guarantees:

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

Trigger:

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

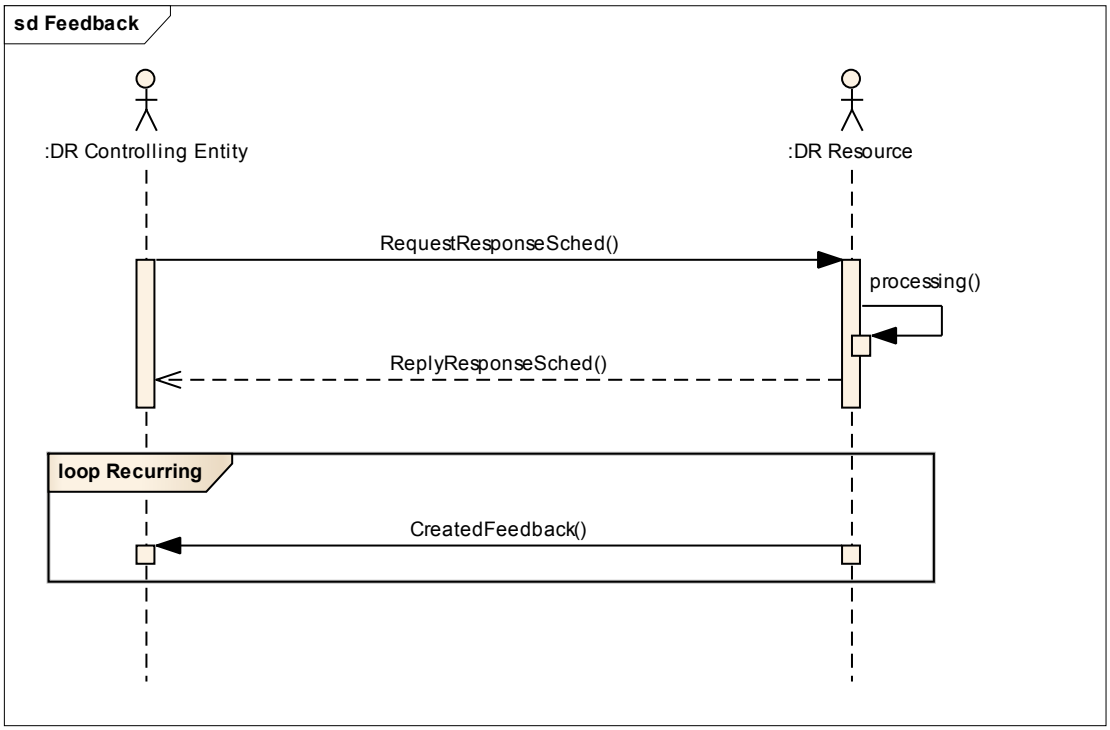


Diagram: Use Case 6: DR Controlling Entity Schedules DR Resource for Periodic Feedback

Main Success Scenario:

1. Initiate or terminate periodic feedback:

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

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

1.3: A DR Resource assesses the request and initiates action to provide a reply and subsequent feedback messages.

2. Provide periodic feedback

2.1: A DR Resource periodically summarizes performance status using an interval defined in the Feedback schedule request.

2.3: A DR Resource sends a Feedback message to a DR Controlling Entity containing the information assembled in the previous step.

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

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

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

Preconditions:

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

Minimal Guarantees:

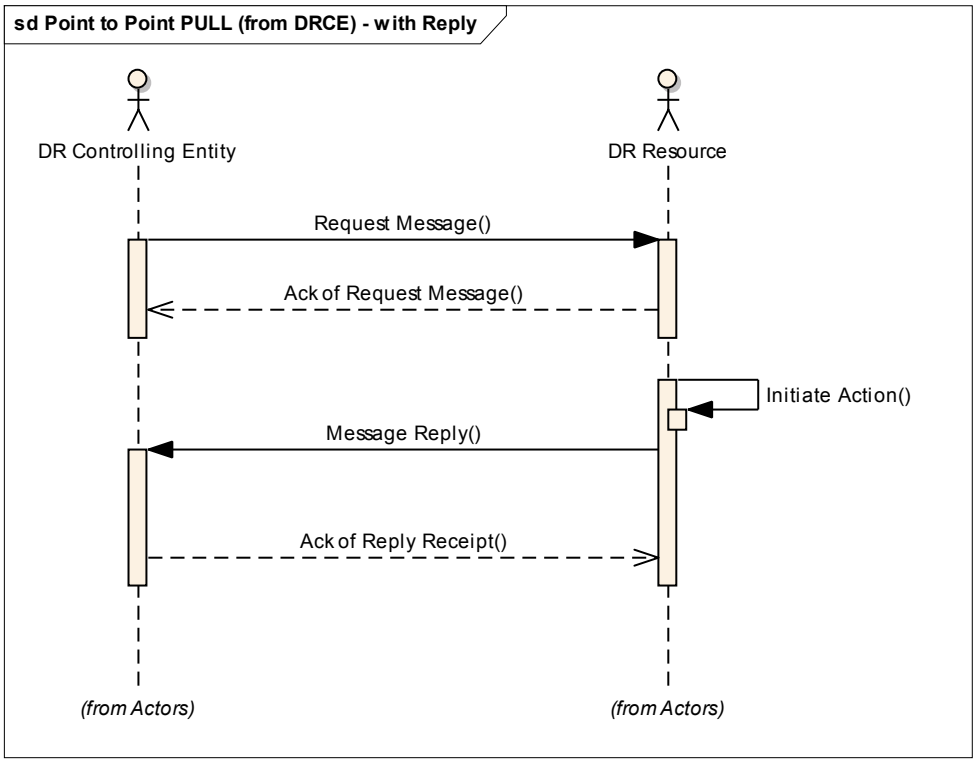
- The DR Resource does not reveal any information that could allow another party to present false identification, or intercept or alter future messages sent to the DR Controlling Entity.
- The DR Controlling Entity does not process any invalid data.

Success Guarantees:

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

Trigger:

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



665

666 **Diagram: Use Case 7: DR Resource Notifies DR Controlling Entity of Event Performance**
667 **(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.

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

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

Preconditions:

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

Minimal Guarantees:

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

Success Guarantees:

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

Trigger:

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

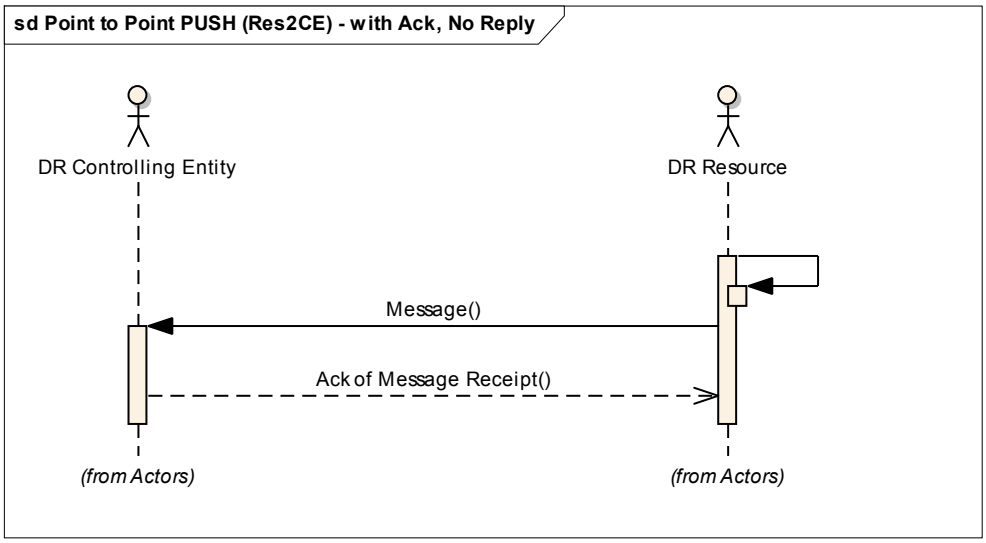


Diagram: Use Case 8: DR Resource Notifies DR Controlling Entity of Event Performance with Feedback Self-Scheduled

Main Success Scenario:

1.DR Resource accumulates Feedback information.

2 DR Resource sends Feedback to DR Controlling Entity.

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

3 Failure Analysis

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

3.1 Failure Analysis Process

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

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

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

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

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

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

3.2 Security and Operational Objectives

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

3.2.1 Contextual Assumptions

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

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

3.2.2 Core Operational Assumptions

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

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

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

3.2.2 Security Principles

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

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

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

3.3 Failures

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

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

	UC1				UC2					UC3			UC4							UC5				UC6.1			UC6.2			UC7					UC8	
Failure #	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	-	-	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	-	-	-	-	-	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	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	x	-	-	-
GF14	-	-	x	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	-	-	-	-

Generic Failures

Generic failures apply to all the roles with in OpenADR.

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.
F3	<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.
F4	<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.
F5	<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.
F6	<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.
F7	<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.

F8	<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.
F9	<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.
F10	<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.
F11	<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.
F12	<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.
F13	<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.
F14	<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.
F15	<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.
F16	<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.
F17	<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.
F18	<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.
F19	<Role> executes wrong action based on changes to its operational parameters, its data, or its internal state	The roles 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

SF1	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).
SF2	Communication and storage devices of DRCE are physically compromised	A malicious user gains physical access to communication and storage devices.
SF3	<Role> is synchronized to a wrong time source	Either DRCE or DR Resource is synchronized to a wrong time source
SF4	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.
SF5	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.
SF6	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.
SF7	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

4 Security Controls

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

4.1 Scope of Security Controls

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

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

are outlined in Section 3.3 of "NIST SP 800-53 – Recommended Security Controls for Federal Information Systems and Organizations"[7] This includes "Specifying organization-defined parameters in the security controls via explicit assignment and selection statements to complete the definition of the tailored baseline"[7]. An example of an organization defined parameter as used in a control is:

"SC-5 DENIAL OF SERVICE PROTECTION

Control: The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined list of types of denial of service attacks or reference to source for current list]."[7]

4.2 Control Definitions

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

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

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

[7] "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)

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

- COBIT – the Control Objectives for Information and related Technology is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations. COBIT emphasizes regulatory compliance, helps organizations to increase the value attained from IT, enables alignment and simplifies implementation of the COBIT framework. (http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx)

- ISO 27000 series – consists of several parts numbering from 27001 – 27006 that provide a specification for an information security management system (ISMS). This work supersedes the BS7799 standard. (http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41933)

- ITIL (Information Technology Infrastructure Library) – ITIL is a widely adopted approach for IT Service Management. It provides a practical, no-nonsense framework for identifying, planning, delivering and supporting IT services to the business. (http://www.itil-officialsite.com)

- NIST SP 800-53 – Recommended Security Controls for Federal Information Systems and Organizations – provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government to meet the requirements of FIPS 200, Minimum Security Requirements for Federal Information and Information Systems. The guidelines apply to all components of an information system that process, store, or transmit federal information. (http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf)

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

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

- Control ID: This ID is composed of the control's category and a sequence number within that category.

- Short Name: This is a unique string that concisely references the intent of the control.

- Definition: This is the text that defines the control itself.

- Reference(s): These are the requirements from the NIST IR 7628 that are partially or fully satisfied by the control. Requirements listed in parenthesis are not required by the NIST IR 7628, but are included here for completeness.
- Failure(s): These are the failures from Section 3.3 addressed by the control.

4.2.1 Access Control

Table 3 – Controls: Access Control

Control ID	Short Name	Definition	Reference(s)	Failure(s)
Access Control.01	Automated Account Management	The system shall provide the ability to automatically authorize, activate, modify and remove user accounts within the organization-defined time period when changes occur on user accounts and associated privileges.	SG.AC-3 SG.AU-2	F6 F16
Access Control.02	Least Privilege	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.	SG.AC-6 SG.AC-7 SG.SC-19 SG.SC-29	F16
Access Control.03	Unsuccessful Access Attempts	The system: 1. Enforces a limit of organization-defined number of consecutive invalid login attempts by a user during an organization-defined time period. 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 considerations (e.g., emergency override). 3. When automatic locks are triggered, alerts shall be raised to the administrator.	SG.AC-8	F16
Access Control.04	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
Access Control.05	Session Duration	The system: 1. Prevents further user access to the system by expiring or terminating the session after no more than (TBD) of inactivity with appropriate safety considerations. 2. Sessions must be reestablished using appropriate identification and authentication procedures. 3. The existing information on the display shall be obfuscated during session lock. This requirement might be inappropriate in the context of long polling.	SG.AC-12 SG.AC-13	F1 F4
Access Control.06	Portable Device Attachment	The system limits attachment of portable devices and media to allow only specifically authorized users to do so. The default state shall disable all access from portable devices and media. Attachment of portable devices and media shall be enabled only where it is necessary for operation and/or	SG.AC-17	F16

Control ID	Short Name	Definition	Reference(s)	Failure(s)
		maintenance functions. The system prevents the automated execution of code located on portable media. Mobile devices traveling to high risk locations shall be appropriately hardened and subsequently sanitized upon return; i.e., such mobile devices shall contain only minimal information required to conduct business during the use period.		
Access Control.07	Remote Access Restrictions	The organization authenticates remote access, and uses cryptography to protect the confidentiality and integrity of remote access sessions; The Open ADR system routes all remote accesses through a limited number of managed access control points;	SG.AC-15 SG.SC-18	F6 F7
Access Control.08	Password Management	<Role> enforces the use of strong user passwords, in accordance with FIPS 112, and protects user passwords from potential exposure. This includes: 1. Ensuring that passwords never cross component boundaries in the clear. 2. Ensuring that passwords are never stored and that stored password hashes use a cryptographic one-way hash function in accordance with FIPS 180-2. 3. Ensuring that passwords are never included in or allowed to be embedded into 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, numerals, and special characters). 5. Changing passwords at defined intervals and minimizing reuse. 6. Expiring passwords after defined intervals of inactivity. 7. Protecting the password store from unauthorized modification.	SG.AC-21 SG.SC-12	F16

963

964 ### *4.2.2 Audit and Accountability*

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

Control ID	Short Name	Definition	Reference(s)	Failure(s)
Audit and Accountability.01	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-2	F14 F16 F19 SF7
Audit and Accountability.02	Contents of Audit Records for DR Resource	DR Resource 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, identity of the DR Resource where the event occurred and the state of DR Resource.	SG.AU-3 SG.AU-15	F14 F16 F17 F19 SF3 SF4

Control ID	Short Name	Definition	Reference(s)	Failure(s)
				SF5
Audit and Accountability.03	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 the result of the event.	SG.AU-3 SG.AU-15	F14 F16 F17 F19 SF3 SF4 SF5 SF7
Audit and Accountability.04	Electronic Log Format	The system shall make all physical access logs to facilities containing communication and storage devices of DRCE (e.g., DRAS) available in electronic form suitable for long term storage and retrieval.	SG.AU-4	SF2
Audit & Accountability.05	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 (TBD, might be different depending on whether the role is DRCE or DR Resource). <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 (TBD), with a minimum of (TBD) immediately available for analysis.	SG.AU-2 SG.AU-4 SG.AU-16	F14 F16 F19
Audit & Accountability.06	User Access Monitoring/Logging	The system shall monitor and log all user interactive sessions to <role> including all administrative and maintenance activities.	SG.AU-16 (SG.MA-6)	F16 F19

966

967 ### *4.2.3 Configuration Management*

968 **Table 5 - Controls: Configuration Management**

Control ID	Short Name	Definition	Reference(s)	Failure(s)
Configuration Management.01	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-5	F7 F14
Configuration Management.02	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
Configuration	Systems Inventory	The system shall create and maintain (on at least a daily basis) an inventory of Open ADR systems and devices that	SG.CM-8	F16

Control ID	Short Name	Definition	Reference(s)	Failure(s)
Management.03		includes information that uniquely identifies each component, such as manufacturer, type, serial number, version number, and location (logical and physical).		F19
Configuration Management.04	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 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-2 SG.SI-7	F14 F19
Configuration Management.05	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-7 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)
Continuity of Operation.01	Alternate Storage	DRCE shall provide an alternate storage to store essential configuration settings (e.g., participants and DR programs they are enrolled in).	SG.CP-7	F15 F16 F18
Continuity of Operation.02	Alternate Telecommunication Services	The system shall provide alternate telecommunication channel between DRCE and DR Resource when the primary channel becomes unavailable.	SG.CP-8 SG.SC-5	F2
Continuity of Operations.03	Operations Continuity	The system shall provide means to compensate for loss of a single component implementing DRCE without loss of system functionality.	(SG.PE-12) SG.SC-5	SF2
Continuity of Operations.04	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
Continuity of Operations.05	Alternative Time Source	The <role> shall support alternative time source for redundancy and consistency checking.	SG.SC-5	SF3 SF4

972

4.2.5 *Identification & Authentication*

Table 7 - Controls: Identification & Authentication

Control ID	Short Name	Definition	Reference(s)	Failure(s)
Identification & Authentication.01	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
Identification & Authentication.02	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
Identification & Authorization.03	Credential Management	The system shall provide a single point of initiation to distribute, manage, and revoke all logical and physical access credentials **fo**r all OPEN ADR systems and components. Revocation shall be carried out on all systems within 24 hours.	(SG.IA-3)	F16 F19
Identification & Authorization.04	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-15 SG.AU-16 SG.AU-2 SG.IA-4 SG.SC-15	F7 F11
Identification & Authorization.05	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	F5 F6 F7
Identification & Authorization.06	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.SC-12 SG.SI-7	F14 F19

4.2.6 *Physical & Environment Security*

Table 8 - Controls Physical & Environment Security

Control ID	Short Name	Definition	Reference(s)	Failure(s)
Physical& Environmental. 01	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
Physical& Environmental. 02	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
Physical & Environmental.03	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
Physical & Environmental.04	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
Physical & Environmental.05	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

4.2.7 *System & Communications Protection*

Table 9 - Controls: System & Communications Protection

Control ID	Short Name	Definition	Reference(s)	Failure(s)
System & Communications Protection.01	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
System & Communication Protection.02	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
System & Communication Protection.03	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)
System & Communication Protection.04	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. (Applicable to Slow, Medium DR only)	None	F7 F9 F11 F13
System & Communication Protection.05	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
System & Communication Protection.07	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
System & Communication Protection.08	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
System & Communication Protection.09	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
System & Communication Protection.10	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
System & Communication Protection.11	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
System & Communication Protection.12	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

4.2.8 *System & Information Integrity*

Table 10 - Controls: System & Information Integrity

Control ID	Short Name	Definition	Reference(s)	Failure(s)
System & Information Integrity.01	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
System & Information Integrity.02	Clock Record	DR Resource's clock record shall indicate time source used for synchronization and when last synchronized.	NONE	SF 3
System & Information Integrity.03	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
System & Information Integrity.04	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
System & Information Integrity.05	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
System & Information Integrity.06	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
System & Information Integrity.07	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
System & Information Integrity.08	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.		
System & Information Integrity.09	Minimal Error Message Content	<Role> shall not reveal potentially harmful (e.g., exploitable) information in error messages.	SG.SI-9	F16
System & Information Integrity.10	Message Time stamping	<Role> shall time stamp all configuration and management messages that it sends.	NONE	SF4
System & Information Integrity.11	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
System & Information Integrity.12	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
System & Information Integrity.13	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

4.2.9 Controls Mapped to Roles

Table 11 - Controls Mapped to Roles

Control ID	Short Name	DR Controlling Entity	DR Resource
Access Control.01	Automated Account Management	x	x
Access Control.02	Least Privilege	x	x
Access Control.03	Unsuccessful Access Attempts	x	x
Access Control.04	Concurrent Session Management		x
Access Control.05	Session Duration	x	x
Access Control.06	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

Appendix A: Relation to the NIST Interagency Report 7628

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

A.1 Traceability

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

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

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

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

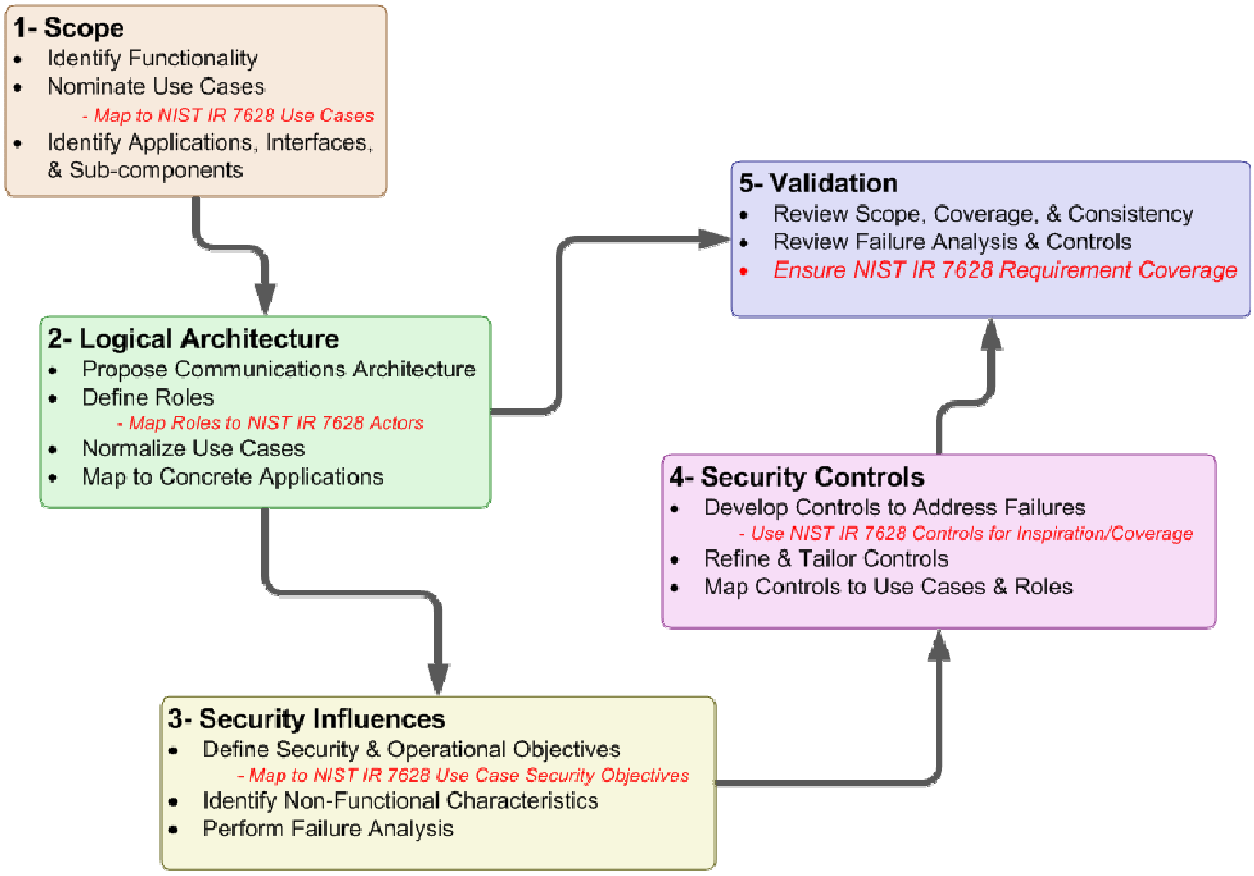


Figure 6 – Security Profile Workflow NIST-IR 7628 Mapping

A.2 NIST IR 7628 Actors to WAMPAC Roles Mapping

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

By comparison, although subtle, an "Actor" as defined by the OMG for unified modeling language is:

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

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

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

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

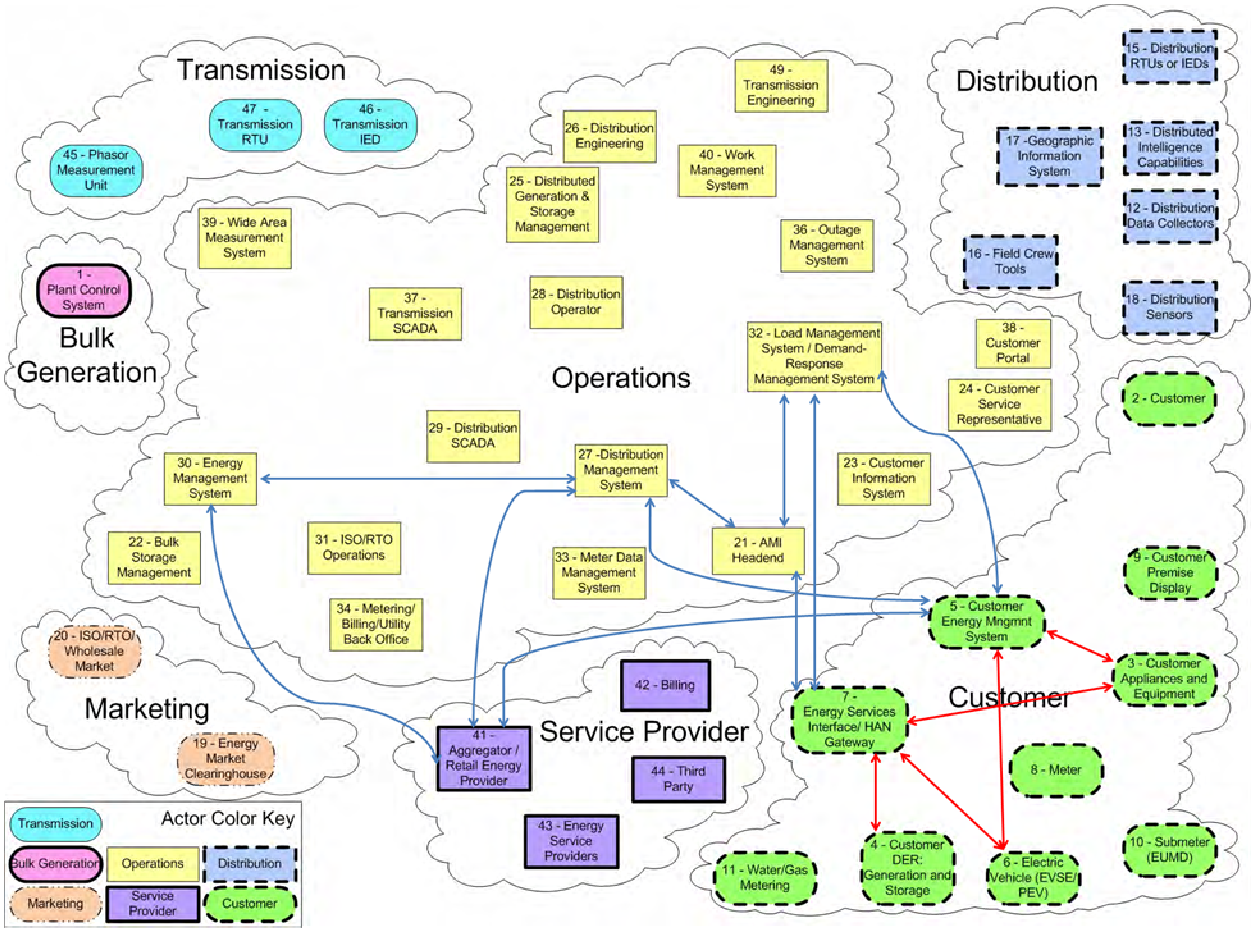


Figure 7 – Unified Logical Architecture for OpenADR

1041

1042

1043 **Table 12 – NIST IR 7628 Actor to WAMPAC Role Mapping**

NIST IR 7628 Actor Number	NIST IR 7628 Actor	Open ADR Role
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*
1046 *Security Principles Mapping*

1047 **Table 13 - NIST IR 7628 Use Case Objectives to OpenADR Security Principles**

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

NIST IR 7628 Scenario	Cyber Security Objective / Requirements	Open ADR Security Principle
Time of Use (TOU) Pricing	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
Net Metering for DER and PEV	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
Feed-In Tariff Pricing for DER and PEV	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
Critical Peak Pricing	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
Load Management	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

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

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

NIST IR 7628 Requirement	NIST IR 7628 Short Name	Open ADR Control	Coverage
SG.AC-5	Information Flow Enforcement	System & Communication Protection.12	fully covered
SG.AC-6	Separation of Duties	Access Control.2 Access Control.3	covers non-organizational portions
SG.AC-7	Least Privilege	Access Control.2 Access Control.3	fully covered
SG.AC-8	Unsuccessful Login Attempts	Access Control.4	fully covered
SG.AC-11	Concurrent Session Control	Access Control.6	fully covered
SG.AC-12	Session Lock	Access Control.7	fully covered
SG.AC-13	Remote Session Termination	Access Control.7	fully covered
SG.AC-14	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
SG.AC-15	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
SG.AC-16	Wireless Access Restrictions	Access Control.10 Access Control.11	fully covered
SG.AC-17	Access Control for Portable and Mobile Devices	Access Control.8	fully covered
SG.AC-21	Passwords	Access Control.12	fully covered
SG.AU-2	Auditable Events	Access Control.1 Access Control.5 Audit & Accountability.1 Audit & Accountability.3 Identification & Authorization.3	covers non-organizational portions
SG.AU-3	Content of Audit Records	Audit & Accountability.5	fully covered

NIST IR 7628 Requirement	NIST IR 7628 Short Name	Open ADR Control	Coverage
SG.AU-4	Audit Storage Capacity	Audit & Accountability.3 Audit & Accountability.4 System & Information Integrity.24 System & Information Integrity.25	fully covered
SG.AU-15	Audit Generation	Audit & Accountability.5	fully covered
SG.AU-16	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
SG.CM-7	Configuration for Least Functionality	Configuration Management.3 Configuration Management.4	fully covered
SG.CM-8	Component Inventory	Configuration Management.1	fully covered
SG.IA-4	User Identification and Authentication	Identification & Authorization.4	fully covered
SG.IA-5	Device Identification and Authentication	Identification & Authorization.5 Identification & Authorization7	fully covered
SG.IA-6	Authenticator Feedback	Identification & Authorization.8	fully covered
SG.SC-2	Communications Partitioning	System & Communication Protection.1	fully covered
SG.SC-3	Security Function Isolation	System & Communication Protection.2	fully covered
SG.SC-4	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
SG.SC-5	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.
SG.SC-6	Resource Priority	System & Communication Protection.6 System & Communication Protection.7 System & Communication Protection.8	
SG.SC-7	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
SG.SC-8	Communication Integrity	Access Control.10 System & Communication Protection.10 System & Information Integrity.9	fully covered
SG.SC-9	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

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

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

Appendix B: Use Case Notation Guide

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.

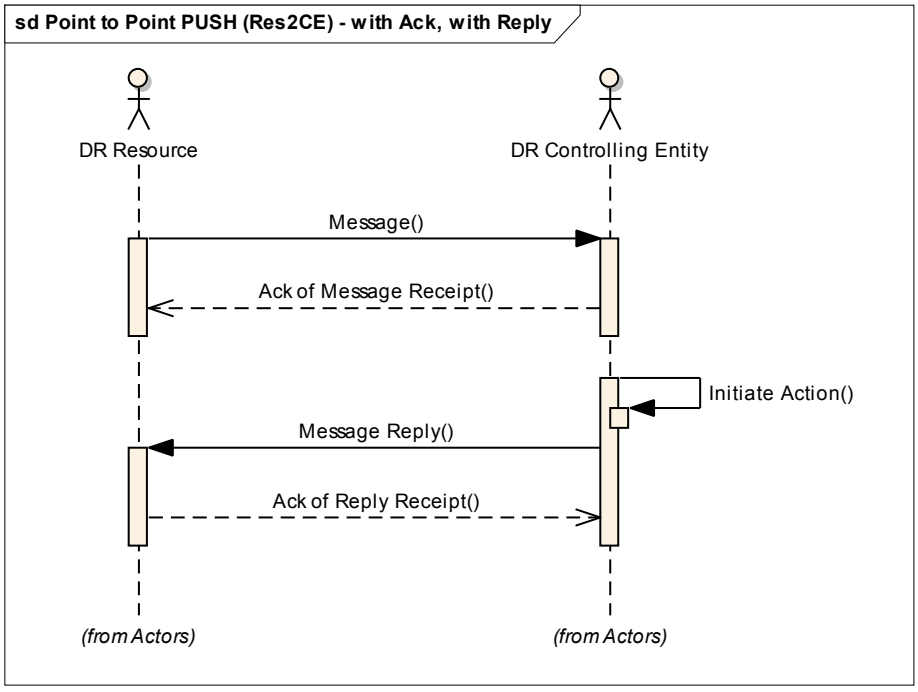


Figure 8 – An Annotated Sequence Diagram

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

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

Appendix C: Using the Security Profile to Evaluate an OpenADR Deployment

This document can be used to evaluate the security of a proposed OpenADR deployment[8]. The security controls and the failure analysis in this security profile are based on the definition of uses cases and roles. In different OpenADR deployments, the use cases and roles will be mapped to different elements of the actual deployment. An architectural analysis of a proposed deployment against this document has the following steps.

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

[8] 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)

cases and use case steps, proceeding through possible failures and determining the recommended controls. This is the information gathered in steps 1-4 above.

5. For each element of the proposed OpenADR deployment, and each recommended control for that element, determine how the control is implemented. If the control is not implemented, ensure that all the failures that would be mitigated by the recommended control are being mitigated by one or more alternate controls. Perform a risk analysis to determine the adequacy of the alternate control(s).

6. For each possible failure that is not mitigated, perform a risk analysis that determines the probability of the failure occurring and the cost if the failure does occur.

Appendix D: Glossary and Acronyms

Many of the definitions in this section have been adapted or directly quoted from Smart Grid Today's Glossary of Terms and Abbreviations.[9]

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

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

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

COBIT: Control Objectives for Information and related Technologies

CSWG: Cyber Security Working Group. A sub-group formed under the Smart Grid Interoperability Panel to address the cyber security aspects of the Smart Grid Interoperability Framework.[10]

[9] http://www.smartgridtoday.com/public/department40.cfm

[10] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG

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

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

DG: Distributed Generation

DHS: Department of Homeland Security

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

DOD: Department of Defense

DMZ: Demilitarized Zone

DNMTT: Data and Network Management Task Team

DNSSec: Domain Name System Security Extensions

DR: Demand Response

DSL: Digital Subscriber Line

EMS: Energy Management System

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

[11] 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/sgsystems/OpenADR/Shared%20Documents/SRS/OpenSG%20OpenADR%201.0%20SRS%20v1.0.pdf

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

FERC: The Federal Energy Regulatory Commission. An independent agency that regulates the interstate transmission of natural gas, oil, and electricity. FERC also regulates natural gas and hydropower projects.[12]

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

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

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

FMEA: Failure Modes and Effects Analysis

FPKI: Federal Public Key Infrastructure

FTP: File Transfer Protocol

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

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

GF: General Failure

GPS: Global Positioning System

GUID: Globally Unique Identifier

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

HTTP: Hyper Text Transmission Protocol

IDS: Intrusion Detection System. A passive monitoring system used to monitor network and/or system activity for malicious activity or policy violations.

IEC: International Electrotechnical Commission. A non-profit, non-governmental international standards organization that prepares and publishes International Standards for all electrical, electronic and related technologies – collectively known as "electrotechnology."

IED: Intelligent Electronic Device.

IEEE: Institute of Electrical and Electronics Engineers. An international non-profit, professional organization for the advancement of technology related to electricity.

[12] http://www.ferc.gov/about/about.asp

Information Repository: Any location where the DM system stores data.

IP: Internet Protocol. The primary protocol used for network communications in packet-switched networks. This protocol is specifically used for node addressing and packet routing.

IPS: Intrusion Prevention System. An active monitoring system, similar to an IDS, used to monitor network and/or system activity for malicious activity or policy violations. Additionally, an IPS can terminate a connection upon detecting suspicious activity.

IPv4, IPv6: IP (above) version 4 is the fourth revision of IP based on RFC 791. IPv4 uses 32-bit addressing with a total of 4,294,967,296 (2^32) unique addresses. IPv6 is designed to supersede IPv4 and uses 128-bit addressing for a total of 2^128 unique addresses.

IR: Interagency Report

ISO: International Organization for Standardization

ISO: Independent System Operator

IT: Information Technology.

ITIL: Information Technology Infrastructure Library

LAN: Local Area Network. A network covering a small physical area.

LIC: Logical Interface Category

Link: is a step labeled with the name of some other use case. A link indicates that the activity of this use case is followed by the activity of the linked use case.

Load: Electric utility term for the infrastructure that uses the power the utility distributes -- such as homes, businesses, industry and in-the-field equipment -- thus, locating a power generation or storage device near load, for example, means putting it close to where the power will be used.

Mesh network: A network technology where each node or end-device can communicate with any nearby devices to create "smart" data routing that finds the most efficient path for data and can change the path when a node stops working.

MPLS: Multiprotocol Label Switching

Multi-factor Authentication: Similar to two-factor authentication, using two or more independent methods, something you have (token or smart card), something you know (password or passcode), and something you are (biometric), for authentication.

NDA: Non-Disclosure Agreement.

NERC: North American Electric Reliability Corporation. A self-regulatory, non-government organization which has statutory responsibility to regulate bulk power

system users, owners, and operators through the adoption and enforcement of standards for fair, ethical and efficient practices.[13]

Network Equipment: Equipment implementing any intermediary function specifically aimed at facilitating or brokering exchange of synchrophasor data between organizations is in scope.

Network Segment: In networking, this is a network segment where all devices communicate using the same physical layer. Within WAMPAC, some switching devices may be used to extend the segment which is defined by the role of the devices in that segment.

NIST: National Institute of Standards & Technology. An office of the US Dept of Commerce, it handles standards and technology issued for the federal government including being tasked in the Energy Independence & Security Act of 2007 with heading up an effort to set interoperability standards for the smart grid industry.(www.nist.gov)

NOAA: National Oceanic and Atmospheric Administration

Non-WAMPAC Application: This is a utility operated application that does not rely critically on time-synchronized phasor measurements for its primary task.

NTP: Network Time Protocol

Open SG: Open Smart Grid users group – part of the UCA International users group.[14]

OMG UML: Object Management Group

Operations Center Equipment: Equipment in the Operations or Control Center that internalizes and processes phasor data in the course of performing synchrophasor application functionality is in scope.

Optional flows: An optional flow indicates a flow that may or may not always happen in a use case.

OWASP: Open Web Application Security Project

Phasor Gateway: This is software that bridges one or more utility networks for the purpose of exchanging phasor measurement data.

PKI: Public Key Infrastructure

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

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

---

[13] http://www.nerc.com/page.php?cid=1

[14] http://osgug.ucaiug.org/org/default.aspx

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

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

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

RFC: Request for Comments

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

RFP: Request for Proposal.

RTO: Regional Transmission Organization

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

SAMATE: Software Assurance Metrics and Tool Evaluation

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

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

SCL: Substation Configuration Language[15]

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

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

SGIP: Smart Grid Interoperability Panel[16]

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

Smart grid: The utility power distribution grid enabled with computer technology and two-way digital communications networking. The term encompasses the ever-widening palette of utility applications that enhance and automate the monitoring and control of electrical distribution networks for added reliability, efficiency and cost effective operations.

[15] As defined in IEC 61850

[16] http://www.nist.gov/smartgrid/

SOC: Security Operations Center. Often incorporated with the network operations center, but designed to monitor security logging and security-related events.

Step: indicates the activities performed by a role during a use case

Substation: An electrical substation is a subsidiary station of an electricity generation, transmission and distribution system where voltage is transformed from high to low or the reverse using transformers. Electric power may flow through several substations between generating plant and consumer, and may be changed in voltage in several steps.[17]

TCP, TCP/IP: Transmission Control Protocol. Usually written with internet protocol as TCP/IP and the two make up the suite of protocols that are used to communicate via the Internet.

TLS: Transport Layer Security

TO: Transmission Owner, as defined by NERC

TPM: Trusted Platform Module. The name of a published specification detailing a secure crypto-processor that can store cryptographic keys that protect information, as well as the general name of implementations of that specification, often called the "TPM chip" or "TPM Security Device"

Two-Factor Authentication: The act of using two independent authorization methods. Examples are mixing something you have (token or smart card), something you know (password or passcode), and something you are (biometric).

UCAIug: UCA International Users Group. A not-for-profit corporation focused on assisting users and vendors in the deployment of standards for real-time applications for several industries with related requirements. The Users Group does not write standards, however works closely with those bodies that have primary responsibility for the completion of standards (notably IEC TC 57: Power Systems Management and Associated Information Exchange).[18]

UML: Universal Modeling Language

UPS: Universal Power Supply

URL: Universal Resource Locator

USB: Universal serial bus, a cable system with rectangular plugs used to connect a wide variety of devices to computers and computer peripherals.

VLAN: Virtual Local Area Network. A method of segmenting and routing traffic between devices on an IP network so that they communicate as if they were attached to the same broadcast domain, regardless of their physical location.

---

[17] http://en.wikipedia.org/wiki/Electrical_substation

[18] http://www.ucaiug.org/default.aspx

VOIP: Voice over Internet Protocol.

VPN: Virtual Private Network. A VPN encapsulates data transfers between two or more networked devices not on the same private network so as to protect the transferred data from other devices on one or more intervening local or wide area networks.

WAMPAC: Wide-Area Monitoring, Protection, and Control

WAN: Wide Area Network. A computer network that covers a broad geographic area.

WASA: Wide-area Situational Awareness

WECC: Western Electricity Coordinating Council

WiFi: Wireless Fidelity -- a standard for sending and receiving data -- such as in a home or small office network or LAN (or even an entire city). The standard includes a number of sub-standards under the IEEE's 802.11 standards.

Appendix E: References

Mary Ann Piette, Girish Ghatikar, Sila Kiliccote, Ed Koch, Dan Hennage, Peter Palensky, and Charles McParland. 2009. *Open Automated Demand Response Communications Specification (Version 1.0). California Energy Commission, PIER Program. CEC-500-2009-063*. http://openadr.lbl.gov/index.html

UCAIug OpenSG OpenADR Task Force, *OpenADR 1.0 System Requirements Specification v1.0*, http://osgug.ucaiug.org/sgsystems/OpenADR/Shared%20Documents/SRS/OpenSG%20OpenADR%201.0%20SRS%20v1.0.pdf

UCAIug OpenSG Service Definition Team, *OpenADR 1.0 Service Definition - Common Version :R0.91*, http://osgug.ucaiug.org/sgsystems/OpenADR/Shared%20Documents/Services/OpenSG%20OpenADR%20SD%20-%20Common%20r0.91.doc

UCAIug OpenSG Service Definitions Team, *OpenADR 1.0 Service Definition – Web Services Implementation Profile Version: v0.91* http://osgug.ucaiug.org/sgsystems/OpenADR/Shared%20Documents/Services/OpenSG%20OpenADR%20SD%20-%20WS%20r0.91.doc

OASIS, *Energy Interoperation Version 1.0 Working Draft 2*[working draft – convert reference to latest specification when available]

ASAP-SG. (2009, December 14). Security Profile Blueprint. Knoxville, Tennessee, United States of America. Retrieved 1 28, 2010, from Open Smart Grid - OpenSG > SG Security: http://osgug.ucaiug.org/utilisec

U.S. Department of Homeland Security. (2010, March). *Catalog of Control Systems Security: Recommendations for Standards Developers*. Arlington, Virginia, United States of America. http://www.us-cert.gov/control_systems/pdf/Catalog%20of%20Control%20Systems%20Security%20-%20Recommendations%20for%20Standards%20Developers%20June-2010.pdf

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

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

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

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

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

IEEE C37.118 Synchrophasor Protocol

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

IEC 61850 "Communication Networks and Systems in Substations"

IEC 61850-90-5 "Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118" (Draft Technical Specification)

IEC 62351 "Information Security for Power System Control Operations"

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

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

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

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

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

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

1402 *SP 800-53A: Assessment Guidance for Security Controls in PKI Systems.* Gaithersburg,
1403 Maryland.

1404 National Institute of Standards and Technology, Department of Commerce, United States
1405 of America. Federal Information Processing Standards (FIPS) [as listed below, available
1406 at http://csrc.nist.gov/publications/PubsFIPS.html]. Gaithersburg, Maryland.

1407 OMG Unified Modeling Language (OMG UML), UML Superstructure Specification,
1408 Version 2.3. Online at http://www.omg.org/spec/UML/2.3/Superstructure/PDF/

1409 *FIPS 140-2 Security Requirements for Cryptographic Modules, May 2001*

1410 *FIPS 186-3 Digital Signature Standard (DSS), June 2009*

1411 *FIPS 112 Password Usage, May 1985*

1412 *FIPS 180 Secure Hash Standard, October 2008*

1413 North American SynchroPhasor Initiative. Data and Network Management Task Team.
1414 http://www.naspi.org/resources/dnmtt/dnmttresources.stm

1415 OWASP: Open Web Application Security Project Development Guide.
1416 https://www.owasp.org/index.php/Guide_Table_of_Contents

1417 Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., Lear, E. (1996). *RFC:*
1418 *1918:Address Allocation for Private Internets*

1419

Appendix F: OpenADR Cryptographic Security Profile

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

- Hash
- Public Key
- Symmetric key
- Key exchange/key agreement

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

F.1 Method

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

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

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

The algorithms selection process considered

- Ensuring adequate security
- Minimizing overhead
- Promoting interoperability.

F.2 References

- IETF RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2, Aug 2008
- NISTIR 7628, Guidelines for Smart Grid Cyber Security:
  - Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements,
  - Vol. 2, Privacy and the Smart Grid
  - Vol. 3, Supportive Analyses and References
- NIST FIPS 180-3 Secure Hash Algorithm (SHA)
- NIST FIPS 186-3, Digital Signature Algorithm (ECDSA)
- NIST FIPS 197 - Advanced Encryption Standard
- NIST SP 800-57, Recommendation for Key Management Part 1
- NIST SP 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised).
- NIST SP 800-22, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications
- NIST SP 800-107, Recommendation for Applications Using Approved Hash Algorithms
- NIST SP 800-131A, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, January 2011

F.3 Hash

Considerations

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

Recommendation

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

F.4 Symmetric Encryption

Considerations

Probable plaintext/ciphertext

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

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

Volume

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

Recommendation

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

F.5 Public Key/Digital Signature Considerations

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

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

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

Recommendations

For User Certificates containing elliptic curve public keys:

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

Operations other than certification authority certificate signing

- Key establishment - ECDHE P-256
- Server authentication - ECDSA P-256
- Signatures - ECDSA P-256

For User Certificates containing RSA public keys:

Certification authorities signing server certificates: RSA 3072

Operations other than certification authority certificate signing

- Key establishment – RSA 2048
- Server authentication – RSA 2048
- Signatures – RSA 2048

Cipher Suites

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

1529 suites shall be used. The selection of the specific Cipher Suite is at the discretion of the
1530 implementing organizations.

1531

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

1532

1533

1534