SECURITY PROFILE FOR DISTRIBUTION MANAGEMENT

Prepared for:

The **NIST SGIP Cyber Security Working Group** & The **UCAIug SG Security Working Group**

Prepared by:

The Advanced Security Acceleration Project for the Smart Grid (ASAP-SG)

Managed by:

EnerNex Corporation
620 Mabry Hood Road
Knoxville, TN 37923
USA
(865) 218-4600
www.enernex.com

Version
1.0

Revision History

Rev	Date	Summary	Marked
0.01	20100513	Outline established.	N
0.02	20100520	Outline revised. Use Cases added.	N
0.03	20100624	Outline revised. Use Cases updated.	N
0.04	20100713	Front matter added or edited.	N
0.05	20100802	Incorporated content from various sources to fill in sections.	N
0.06	20100803	A few new and modified controls.	N
0.07	20100803	Fleshed out explanatory prose in several sections. Also edited role descriptions and added material describing the approach.	N
0.08	20100804	Integrated policy controls and additional explanatory prose in several sections. Added a few new controls and brought out network segmentation controls more explicitly.	N
0.09	20100807	Added references. Edits in 3.1, 4.1, and 4.2. Incorporated glossary.	N
0.10	20100811	Reordered technical controls to match order in mapping table. Fixed table and glossary formatting. Misc edits throughout. Incorporated material for 2.2.	N
0.11	20100812	Misc edits throughout.	N
0.12	20100816	Added DER mapping for 2.2. Misc edits throughout. Dismissed internal commentary.	N
0.13	20110314	Added edits from the Usability Analysis review	N
0.9	20110418	Updated document version number to reflect document status	N
0.91	20110912	Additional edits from secondary review	Y
0.92	20111014	Clean version for voting review	N
1.0	20120220	Ratified by the SG Security Working Group, UCAIug	N

Executive Summary

This guideline identifies best practices for securing automated distribution management (DM) functions in a smart grid environment, including steady state operations and optimization. This document addresses concerns related to using communications and automation in field equipment that controls the configuration and operation of the electric distribution system. Other electric system operation scenarios may also be addressed using this profile, as the various roles defined herein have been abstracted in such a way as to support mapping to different environments.

This document defines a set of use cases and a corresponding set of security controls for systems and components that implement the use cases. The security controls in this document are based in part on the controls from the Department of Homeland Security Catalog of Control Systems Security (U.S. Department of Homeland Security, March 2010). The underlying approach is to define the function of DM systems through abstract roles and use cases; define broad security objectives for DM systems; identify potential failures for each role in the context of the use cases; define security controls to address the failures; and assign controls to the roles. The roles have been designed abstractly to ensure applicability across a range of DM applications. Likewise, the use cases have been designed to be modular in order to facilitate combining them in different arrangements to describe different business models.

The primary audience of this document is organizations that are developing or implementing solutions providing various aspects of distribution management. This document is written at the normal level of utility security experience for system owners, system implementers and security engineers.

Table of Contents

Table of Figures

Table of Tables

Acknowledgements

The Advanced Security Acceleration Project for Smart Grid (ASAP-SG) would like to thank:

1. Supporting utilities, including American Electric Power, BC Hydro, Con Edison, Consumers Energy, Florida Power & Light, National Grid, Oncor, and Southern California Edison.

2. Supporting organizations including The United States Department of Energy and the Electric Power Research Institute.

3. The utility and vendor representatives that provided ASAP-SG with essential foundational knowledge and insight into the Distribution Management problem space, with a special thanks to Oncor and American Electric Power.

ASAP-SG would also like to thank the Department of Homeland Security (DHS) Cyber Security Division, National Institute of Standards and Technology (NIST) Computer Security Division, North American Reliability Corporation (NERC), and Smart Grid Today for the works that they have produced that served as reference material for the Security Profile for Distribution Management.

The ASAP-SG Architecture Team included resources from Consumers Energy, EnerNex Corporation, InGuardians, Oak Ridge National Laboratory, the Software Engineering Institute at Carnegie Mellon University, and Southern California Edison.

Authors

Glenn Allgood

Len Bass

Bobby Brown

Kevin Brown

Matthew Carpenter

Jim Cebula

Slade Griffin

Teja Kuruganti

Howard Lipson

Jim Nutaro

Justin Searle

Brian Smith

James Stevens

Edited by: Darren Highfill and James Ivers

1 Introduction

This guideline identifies best practices for securing automated distribution management (DM) functions in a smart grid environment, including steady state operations and optimization. This security profile addresses concerns related to using communications and automation in field equipment that controls the configuration and operation of the electric distribution system. Other electric system operation scenarios may also be addressed using this profile, as the various roles defined herein have been abstracted in such a way as to support mapping to different environments.

This document defines a set of use cases and a corresponding set of security controls for systems and components that implement the use cases. The security controls in this document are based in part on the controls from the Department of Homeland Security Catalog of Control Systems Security (U.S. Department of Homeland Security, March 2010). The underlying approach is to study real-world DM systems; define the function of DM systems by presenting a reference architecture that defines abstract roles and use cases; map the architecture's roles to real-world DM systems; define broad security objectives for DM systems; identify potential failures for each role in the context of the use cases; define security controls to address the failures; and assign controls to the roles.

An understanding of the roles is essential to applying the security controls defined in this document. Roles have been designed abstractly to ensure applicability across a range of DM applications. The key roles are those of a sensor, an actuator, and an application—each of which represents functionality that may be implemented by physical devices. A sensor is able to gather data about physical equipment in a DM system. An actuator is able to take action on physical equipment in a DM system. An application is able to make decisions, with or without human supervision, about what actions should be taken in a DM system. These roles are elaborated and decomposed (e.g., distinguishing between field applications and centrally deployed applications) in section 2.1.

It is important to note that a single device or product may implement multiple roles. Moreover, each role could 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 address 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 assigned to each of the roles.

1.1 Scope

This security profile addresses automated distribution management (DM) functions including steady state operations and optimization. The document considers "distribution automation" to refer to a specific portion of distribution management related to automated system reconfiguration such as SCADA, and therefore within scope for this security profile.

1.1.1 Field Equipment

From a field equipment perspective, the scope is bounded on the utility end by the distribution substation. While the transition from distribution to transmission may vary from one organization to another, distribution management field equipment lies primarily between the last substation and the point of service for the customer. In general, the substation fence serves as a scoping boundary with at least two notable exceptions:

1. Substation feeder breakers are considered in scope as they often need to be managed in conjunction with distribution feeder devices for system protection coordination and system reconfiguration.

2. Equipment in the substation that is part of overall voltage and volt-ampere reactive (VAR) control applications is also considered in scope. This may include on-load tap changers, voltage regulators, and capacitor controls in the substation.

The boundary on the customer end is defined logically as some distribution management functions will inherently involve communication with customer-owned equipment. Distribution management and control functions in direct communication with appropriate customer equipment are considered in scope. Some examples:

1. **Distributed generation equipment** (including photovoltaics and distributed wind): Customer-owned distributed generation equipment is in scope insofar as it comprises part of distribution voltage control applications and requires coordination for protection functions.

2. **Energy storage**: Customer-owned energy storage is in scope insofar as it comprises part of distribution management functions for reconfiguration, islanding, and voltage control.

3. **Direct load control**: Direct communication with customer loads is in scope insofar as load control comprises part of distribution management functions. This includes direct

communication with devices managing load control functions and may include verification of the load response if appropriate (e.g., an energy services manager device, meter, or controller directly on the load).

1.1.2 Applications

At an application level, many distribution functions can be implemented with a range of different architectures involving varying degrees of distributed control. Some functions may be primarily enterprise applications while other functions involve a combination of enterprise functionality with distributed controls that operate relatively autonomously (although coordinated). The distinction between enterprise level functionality and distributed control systems is addressed for the specific categories of functions in terms of how this influences the security requirements.

Specific functions that were considered in the development of this security profile include:

Function	Purpose	Examples
Distribution Protection and Configuration Management		
Monitoring and Elective Control of Primary Switchgear	System Protection Fault Isolation Reconfiguration	Outage Management System
		Fault Location, Isolation, and Service Restoration
		Mobile Workforce Management
		Dynamic Management of Protection Coordination Settings
		Faulted Circuit Indicator Management and Integration
		Predictive Fault Location
Distribution System Management and Optimization		
Changes to System Variables or Equipment	Optimize System Performance Manage System Performance Energy Savings Demand Response	Load Control
		Voltage Optimization and Control
		VAR Management
		Integrated Volt-VAR Control
		Power Quality Control
		Integration with Distributed Resources
		Electric Vehicle Management and Control
Distribution System Monitoring		
Monitoring Conditions and System Performance	Contract Fulfillment Asset Preservation Billing Planning	Power Quality Monitoring
		Equipment Condition Monitoring and Assessment
		Metering
		Maintaining the Electrical Model
		Load Forecasting and Load model Maintenance
		On-Line Power Flow and State Estimation
		Topology Analysis
		Contingency Analysis

1.1.3 Explicit Exclusions

While closely related to distribution management for some organizations, this document explicitly considers the functions of system protection (high speed response to a fault condition) and advanced metering to be out of scope for this profile. Advanced metering is covered under the Security Profile for Advanced Metering Infrastructure. System protection (i.e. automated high-speed response to a fault condition) will be covered under its own security profile under the topic of substation automation. However, management of protection settings for coordination within and configuration of protection equipment is within scope of this security profile.

1.2 Approach

The approach used to develop this security profile is shown in Figure 1 and summarized as follows

1. Functional analysis: research existing and planned DM systems, define the profile's scope, define abstract roles and use cases describing the functionality representative of DM systems, and validate the functional analysis by mapping the roles and use cases against real world examples. This step is elaborated and the results are presented in Section 2.

2. Failure analysis: define broad security and operational objectives that should be achieved by DM systems complying with the security profile and analyze the roles and use cases to determine the types of failures that could jeopardize achievement of the security objectives. This step is elaborated and the results are presented in Section 3.

3. Control definition and assignment: define the security controls required for DM systems to achieve the security objectives and identify the controls that each role must implement. This step is elaborated and the results are presented in Section 4.

4. Control validation: perform a cross check to determine that all failures are addressed and that all controls are necessary. The controls and failures presented in this document represent the results of this refinement and validation.

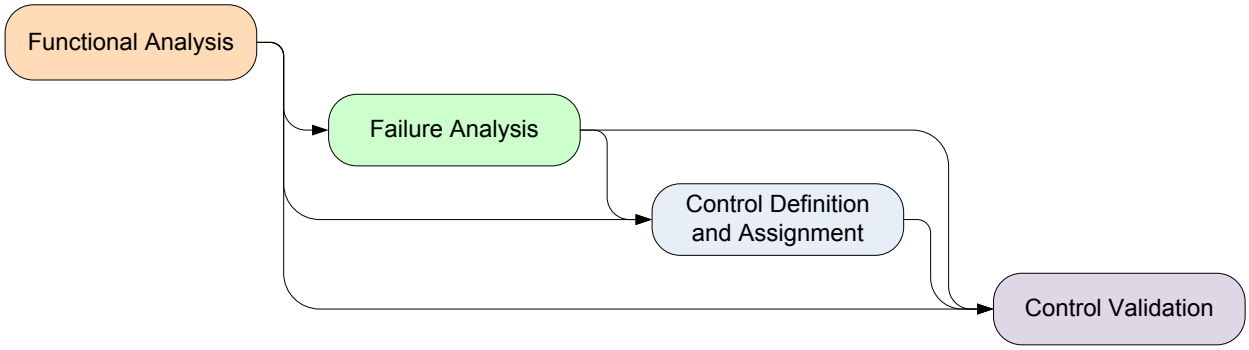

Figure 1 – Overview of Security Profile Development Approach

As shown in Figure 1, each step in the approach builds on the results of the preceding steps.

1.3 Audience

The primary audiences of this document are organizations that are developing or implementing solutions requiring or providing automated distribution management functionality. This document is written at the normal level of utility security experience for system owners, system implementers, and security engineers. 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. A utility much evaluate the controls, as well as balancing the cost of security against the operational impact and possibility of an operational impact.

1.3.1 How This Document Should Be Used

This profile presents the superset of controls that should be implemented by DM components and systems. This section discusses how the document should be used by various stakeholders. The document is designed to be used in whole or in-part. The profile development approach guides the reader through the process developed by the ASAP-SG team 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.

Electric Utility

The utility may use this document to help achieve several security objectives for their organization through activities such as:

1. developing security requirements for DM procurement activities
2. configuring and operating a DM system
3. evaluating planned or deployed DM architectures (see Appendix B: 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 perform a risk analysis to confirm the adequacy of the alternative control.

DM Vendors

Vendors may use this document to incorporate security controls needed for the development of DM products and solutions. 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 offer tools for understanding DM applications in an abstract sense.

1.4 Disclaimer/Status

The controls recommended in this document have been explicitly written for systems and components implementing the various functions of distribution management. Many of these custom controls were inspired by or adapted from the DHS Control Systems Catalog, however the controls are not meant to be representative of the DHS work. This document also provides numbers for the DHS control sections that inspired custom controls where applicable for reference and traceability.

2 Functional Analysis

The purpose of the functional analysis is to define a clear picture of the scope, architecture, and functionality of DM systems, as addressed by this security profile. The specifics of DM systems vary in function, scope, and technology among different deployments; however this profile focuses on what is common among DM systems. Consequently, the information in this profile is expressed in terms of abstract roles that capture the essence of a variety of specific realizations. For example, a Central Application role is defined that captures the essence of what is performed by a variety of more concrete applications such as Volt/VAR control, power quality monitoring, fault location/isolation, and service restoration.

The following steps were performed in the functional analysis:

1. Interview domain experts (utility and vendor) and review publicly available resources to understand existing and planned DM systems and functions.
2. Define abstract roles that characterize elements of DM systems concisely. 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 2.1.
3. Define use cases describing how the roles interact to implement DM 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 2.3.
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 **Error! Reference source not found.** (this is presented before the use cases to reinforce the meaning of the roles).

Steps 2 and 3 together define a precise scope for this security profile. This profile does not provide security recommendations for functions or roles that are not defined in this profile.

2.1 Roles

The roles defined in this profile are *abstract* or *logical* roles; that is, each role does not necessarily map one-to-one with a device or system. It is possible for a device to implement the functionality of multiple roles. However, it is also possible for the same set of roles to be implemented by discrete devices. As such, we focus on defining the roles, their functionality, and ultimately the security controls each role must implement at this abstract level and leave the task of mapping roles to specific products, devices, or systems to those developing or procuring these elements (see Section 1.3.1 for more information).

The essential roles involved in distribution management systems are shown in Figure 2. This diagram presents several ideas:

- Human and software/hardware roles are distinguished by shape. Roles that are implemented in software and/or hardware are shown as rectangles and roles representing people are shown as stick figures.
- Rounded, shaded regions represent different areas in which the roles are typically deployed. The principle distinction is between roles that are deployed in the field vs. roles deployed in a central location like a control center. Centrally deployed assets are typically under utility control and are more likely to be server-based than embedded. Substations are considered part of a field deployment. A DM system is not restricted to a single Centrally Deployed or Field Deployed region (see Section 4.1 for more information on how these concepts relate to network segments).
- Lines between roles represent interactions; arrows indicate the direction of *primary* interaction.[1] Lines between a role and a shaded region indicate an ability for that role (e.g., a Maintainer) to interact with any role within that region.
- Multiplicities between roles are not depicted, but are generally many-to-many. That is, a given Field Application may receive data from multiple Sensors and may also interact with multiple other Field Applications. The exception is that there is typically only one Control Authority per centrally deployed location. Lines doubling back to a role indicate where one instance of a role may communicate with another instance of the same role.

[1] For example, Sensors most often send new data to an Information Repository, but occasionally receive requests from an Information Repository to provide fresh data. In the figure, this is depicted using an arrow from the Sensor to the Information Repository, but not the other way around.

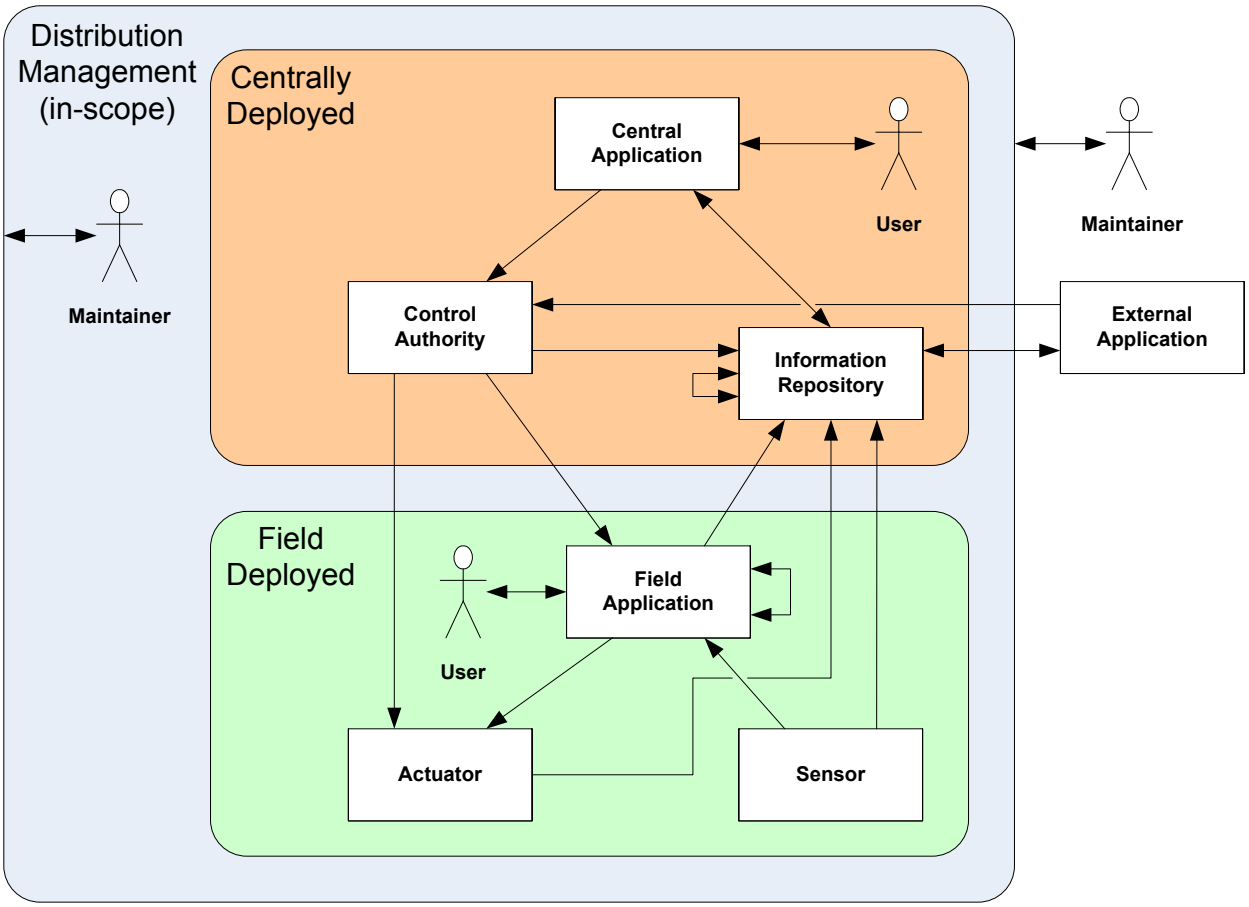

Figure 2 – Distribution Management Roles

All software/hardware roles are assumed to have some inherent communications ability (i.e., there is no need to model a distinct communications element associated with each software/hardware role). Each role is defined in the following sub-sections.

2.1.1 User

This role represents a human actor who participates in or observes control decisions or telemetry data. Users are typically constrained to a pre-determined set of interactions with an application based on system design and individual user privileges. An application may have one or more users.

2.1.2 Maintainer

This role represents a human actor who interacts with the system or system components for the purposes of maintaining the distribution management system. Unlike a User, a Maintainer is typically not constrained to a limited set of interactions with the system or component. This profile does not prescribe how a Maintainer interacts with other roles, but the Maintainer is included for consideration when defining security controls that apply to other roles.

2.1.3 Central Application

This role represents arbitrary functionality that may be deployed at a regional or enterprise level. All central applications in DM ultimately support decision making, though some may only aggregate and process telemetry data to support offline decision making (e.g., event analysis, asset monitoring, or power quality). Other applications may automate (i.e., without User intervention) decision making.

A typical DM system includes multiple Central Applications, supporting functions such as:

- distribution SCADA applications
- volt/VAR control
- fault location/isolation, and service restoration
- automatic feeder reconfiguration

Any human machine interface that is provided exclusively for a Central Application is considered part of that Central Application.

2.1.4 Field Application

This role, like a Central Application, represents arbitrary functionality that ultimately supports decision making. Unlike Central Applications, a Field Application is deployed in the field. Field Applications typically employ automated decision making, with limited local human machine interfaces. A typical DM system may include multiple Field Applications, supporting functions such as:

- feeder reconfiguration
- reactive power compensation

Any human machine interface that is provided exclusively for a Field Application is considered part of that Field Application. Field Applications may be implemented in such a way that internal elements mimic the functionality of Information Repository and Control Authority roles, but these elements are not directly addressable by other elements of a DM system and so are not considered separate roles requiring separate security controls.

2.1.5 External Application

This role represents arbitrary functionality that may not be essential to the DM mission, but that makes use of information from or provides information to a DM system. External Applications are not considered part of a DM system (as defined by the scope of this security profile), but their interactions with elements of a DM system are relevant to security control recommendations.

External Applications typically interact with elements of a DM system via one or more of the DM system's Information Repositories. Examples of External Applications include systems such as:

- transmission SCADA applications

- outage management system (OMS)
- advanced metering infrastructure (AMI)
- topology processors (i.e., state estimators)
- distribution power flow applications

2.1.6 Information Repository

This role represents a store of information that is used to communicate information among different roles of a DM system. It serves as an aggregation point at a centrally deployed region for information from field deployed roles (i.e., Sensors, Actuators, and Field Applications). Central Applications and External Applications typically retrieve data from an Information Repository, rather than directly from Sensors, Actuators, or Field Applications.

A centrally deployed DM region may include multiple Information Repositories, each oriented towards a specific type of data such as:

- real-time distribution system information from Sensors and Field Applications
- distribution system event data
- "health" data from Sensors, Actuators, and Field Applications
- distribution management system event logs

2.1.7 Control Authority

This role arbitrates and coordinates the dispatch of control commands to field destinations. Control commands are intended to change the state of equipment directly connected to Actuators or influence the behavior of Field Applications. A Control Authority is only used to govern commands sent to Actuators and Field Applications and does not participate in requests to retrieve data from Sensors or Field Applications.

2.1.8 Actuator

This role encompasses the ability to take action on the physical electric system (e.g., trip a breaker). Actuators do not detect current conditions or make decisions; they execute the actions they have been directed to take.

2.1.9 Sensor

This role encompasses the ability to gather data about the physical electric system, including equipment that may be directly connected by an electrical signal. Sensors only detect and forward information; they do not make decisions or take actions.

2.2 Role Mappings

The relationship pattern among different DM roles is shown in Figure 3. The use cases governing this relationship are described in Section 2.3 can be applied to different sets of actors realizing this pattern. In this section, we demonstrate several such possible applications of the pattern.

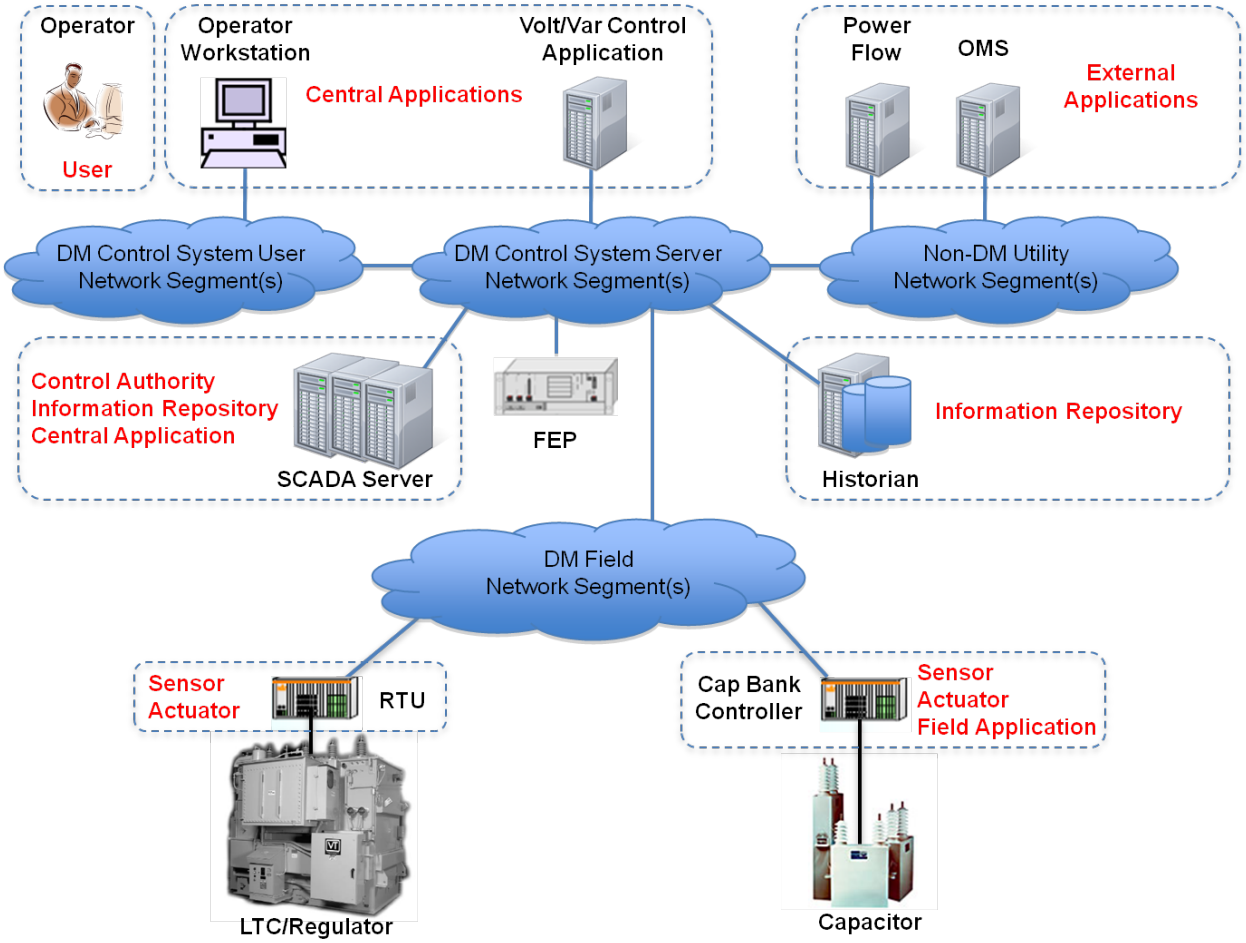

Figure 3 – Centralized Volt/VAR Control Application

The distribution-level power system may experience over-voltage/under-voltage condition that can be mitigated using Volt/VAR control (VVC). The objective of VVC is to optimize voltage levels and reactive correction to minimize energy use and minimize peak demand the power loss while maintaining acceptable voltage levels and distribution substation power factor limit (reactive power limit). VVC optimization is typically made possible by controlling the tap position or by varying the shunt capacitance. To regulate the voltage output on a distribution transformer load tap changer (LTC) or regulator is used. Switchable capacitor banks are used to provide the reactive power compensation. VVC is a central application that receives the voltage levels at each bus and reactive power requirements in the distribution network. The central application computes the power flow in the network under given constraints and communicates the set points to LTC and capacitor banks. While LTC executes the set point from the central application, the switchable capacitor bank controller has a field application that will discretize the solved capacitance set point to control the banks of capacitance.

Figure 3 shows how this pattern could be applied in a fully centralized SCADA application with the centrally deployed SCADA server acting as the Control Authority. The VVC is the Central Application performing voltage and reactive power control within the distribution network. The Operator Workstation provides the human machine interface of VVC to the User and considered part of the Central Application. Power Flow and Outage Management System (OMS) are the External Applications, as shown in Figure 3. The Historian acts as the Information Repository that stores the data from the sensors, field applications, and actuators. While a persistent information authority exists in the Historian, a real-time database exists within the SCADA server for operations and therefore it also qualifies for the role of Information Repository. The User is the human-in-the-loop operator that oversees reactive power flow control within the distribution network.

The User, VVC application, SCADA server, and Historian are centrally located within a utility control center (there may be variations due to system architecture though). The centrally located components communicate with the field devices (sensors, actuators, RTU, LTC, and capacitor banks) through a front-end processor (FEP) and communication network (wired, wireless).

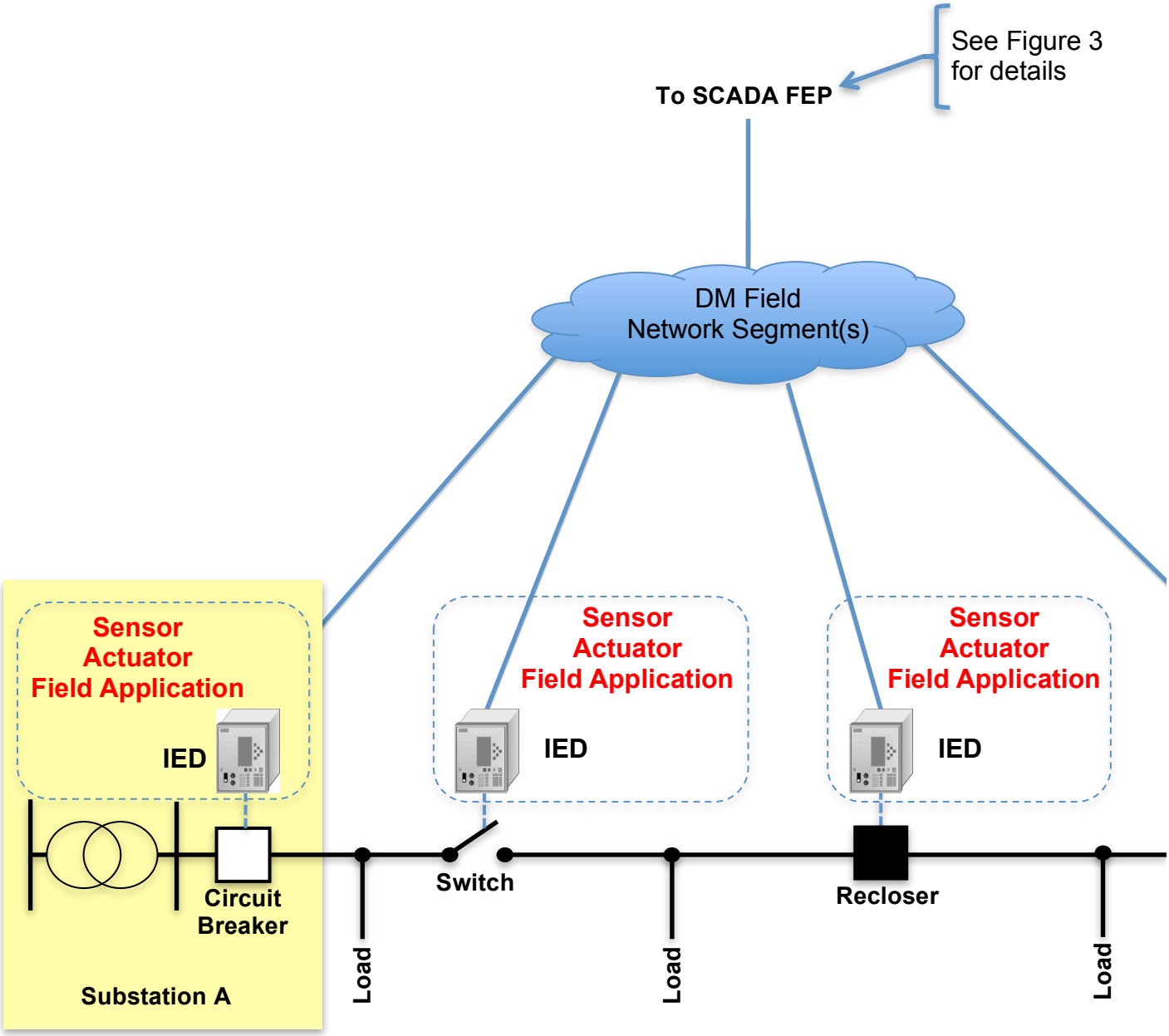

Figure 4 – Distributed Automatic Feeder Restoration Application

Automatic feeder reconfiguration is a distribution operations planning application used for closing and opening switches within the distribution network system (whole system or groups of sub-systems) to restore power to portions of the network after contingencies and topology changes (varying loading conditions). This kind of application pattern describes a fully distributed mechanism for feeder reconfiguration. The feeders in the distribution system are equipped with intelligent electronic devices (IED) which are wireless automatic reclosers capable of forming a mesh network to autonomously communicate with each other without involvement of a central application. These IEDs can locally sense faults within a sub-system and communicate the status to the neighboring feeders. The feeders then react intelligently to reconfigure the distribution network topology to restore/de-energize service to sub-systems.

Figure 4 shows how the relationship pattern of DM roles could be applied in a fully distributed automatic feeder reconfiguration. The IEDs assume multiple roles within the distribution network. They act as a Sensor for identifying fault in the lines, as a Field Application for communicating with other feeder switches to isolate the fault, and as an Actuator for performing automatic opening/closing of the circuit. The IEDs have a limited control authority as described in the Field Application role for influencing the local control of switches.

The centrally deployed assets are abstracted from Figure 4 and will mimic Figure 3. The Central Application is maintained centrally, which oversees and tracks the service restoration. The Historian acts as the Information Repository and provides the topology updates to the External Applications as service is being restored. Optimal power flow and outage management system (OMS) are the external applications that utilize the service area and outage area to compute real-time topology.

Multiple applications of the pattern can occur within a single distribution setting. The utility could have both centralized and distributed applications deployed. This security profile can be used in both of the contexts.

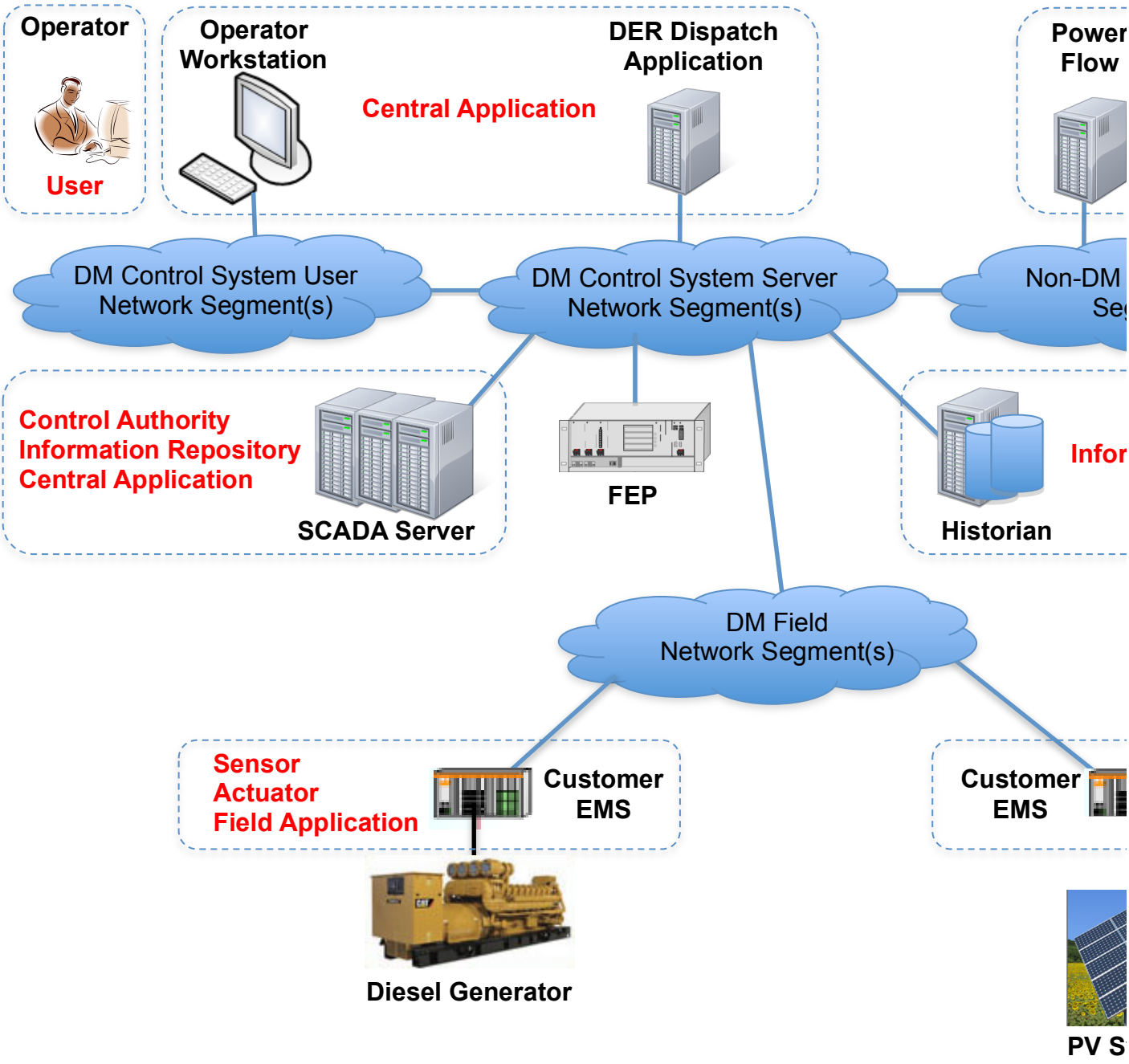

Figure 5 – Dispatch of Customer-owned Generation

Distribution management includes continuously monitoring load demand variations. Customer-owned Distributed Energy Resources (DER), which are typically distributed across the utility, and reside within customer premises, are integrated into the utility dispatching programs for dynamic load demand requirements. The utility continuously monitors the load on the distribution network and analyzes the geographical location, startup cost/performance of various DERs and dynamically issues dispatch commands. The customer energy management system (EMS) manages the local generation and electricity delivery to the grid. This application of pattern describes the dispatch of DERs.

Figure 5 shows how the relationship pattern of DM roles could be applied in a dispatch of DER. The Customer EMS assumes the roles of Sensor for measuring generation and Field Application for managing the generation based on the dispatch commands. The centrally deployed SCADA Server acts as the Control Authority. The DER Dispatch Application is the Central Application performing near real-time utility dispatch. The Operator Workstation supports the graphical user interface which provides the human machine interface of DER dispatch to the User and considered part of the Central Application. Power Flow and Outage Management System (OMS) are the External Applications, as shown in Figure 5. Historian acts as the Information Repository that stores the data from the sensors, field applications, and actuators. While a persistent information authority exists in the Historian, a real-time database exists within the SCADA server for operations and qualifies for the role of Information Repository. The User is the human-in-the-loop operator that oversees reactive power flow control within the distribution network.

2.3 Use Cases

This section presents a superset of the use cases that are needed to realize a distribution management system. A given DM system may choose to only implement a subset of these use cases.

The use cases are designed to be composable. For example, a particular activity may be the result of several different actions; in such cases the common activity is called out as a separate use case that is then linked to other use cases that it precedes or that follow it. The result is that a single, long thread of activity may be represented by the composition of several related use cases.

This security profile defines DM functionality using the following use cases:

- Use Cases 1 and 2 deal with actions taken by Field Applications.
- Use Case 3 deals with how Actuators, Sensors, and External Applications deliver information to an Information Repository.
- Use Case 4 deals with keeping information synchronized between two Information Repositories.
- Use Case 5 deals with how an Information Repository processes new information and how it decides whether to inform other roles of the availability of new information (each of which triggers another use case).
- Use Case 6 deals with how a Central Application processes new information.
- Use Cases 7-10 deal with how a User interacts with Central and Field Applications to take an action, enter data, change operational mode, or change application parameters.
- Use Cases 11 and 12 deals with how a Control Authority processes command requests for Field Applications and Actuators.
- Use Case 13 deals with how Central Applications or Information Repositories request fresh data from Field Applications and Sensors.
- Use Cases 14 and 15 deals with how External Applications process new information and send command requests to a Control Authority.

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

Each use case contains the following sections

- 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 will be 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 A) and each step is summarized in text.

Use Case 1: Field Application Makes Decision

Use Case Description: A Field Application re-evaluates conditions based on new stimulus such as the arrival of new data from a Sensor or another Field Application or a change to the Field Application's operational parameters. The Field Application analyzes current conditions, determines whether any actions are required, and initiates any necessary actions. The Field Application's decision is made without supervision of a User or communication with any Central Application.

Preconditions:

- Field Application, Sensor, and Actuator have been initialized with operational parameters, routing/communication information, and have established initial system picture.

Minimal Guarantees:

- No unnecessary actions will be taken by the Actuator.

Success Guarantees:

- Whenever a physical action should be taken, the appropriate Actuator executes the required action.

Trigger:

There are three possible triggers for this use case

- Conditions at the Field Application have changed such that it needs to re-evaluate. This is usually caused when a Field Application has received a directive to change its operational parameters or to forward a directive to an Actuator (as coming from use case 7, 10, or 11).
- A Sensor has sent new data to the Field Application. This could be a scheduled event, a spontaneous event, or a response to a request for new information (as coming from use case 2).
- Another Field Application has sent new data to the Field Application. This could be a scheduled event, a spontaneous event (as coming from this use case), or a response to a request for new information (as coming from use case 2).

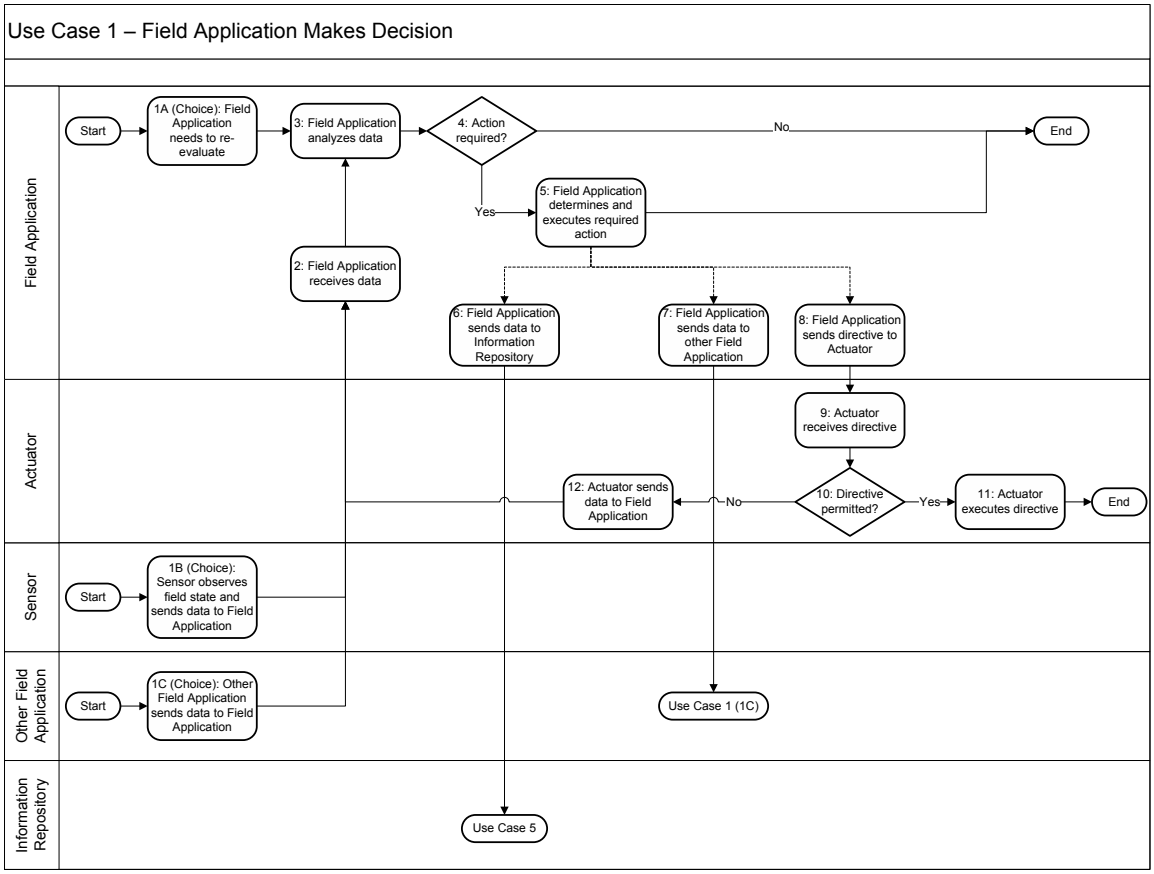

Diagram: Use Case 1 – Field Application Makes Decision

Main Success Scenario:

1A: The Field Application needs to re-evaluate conditions based on changes influencing its behavior. Examples include changes to operational parameters or instruction to forward a directive to an Actuator.

1B: A Sensor makes a field observation and sends data to the Field Application. Such observations can be scheduled, spontaneous (e.g., triggered by a measurement exceeding a threshold), or in response to a request (e.g. data update request).

1C: Another Field Application sends data to the Field Application. This update could be scheduled, spontaneous (e.g., triggered by conditions exceeding a threshold), or in response to a request (e.g. data update request).

2: The Field Application receives the data sent by the Sensor or Other Field Application

3: The Field Application analyzes its data to re-evaluate current conditions. This analysis could include examining new input data, instructions directing a specific action to be taken, computation of derived data, or any other processing that is required to determine if the Field Application needs to take an action.

4: The Field Application determines if it needs to take any action. Possible actions include sending a directive to an Actuator, sending data to an Information Repository or another Field Application, or adjusting its own operational parameters.

5: If action is required, the Field Application determines what action or actions are required. Any actions that can be completed locally by the Field Application are initiated.

6: If appropriate, the Field Application sends data to the Information Repository (e.g., when new derived data has been computed). This step triggers Use Case 5, in which the Information Repository processes the new data.

7: If appropriate, the Field Application sends data to other Field Applications (e.g., when Field Applications are coordinating their responses and new information needs to be propagated). This step triggers a new occurrence of this use case for the other Field Application (which will take on the role of the primary Field Application).

8: If physical action is required, the Field Application sends a directive to the appropriate Actuators.

9: The Actuator receives the directive from the Field Application.

10: The Actuator determines if the directive is permitted. The Actuator makes a simple determination as to the safety of the directive based on local knowledge. For example, if the Actuator has been physically disabled (e.g., by a lockout switch), then the directive cannot be executed. Because Actuators receive directives from multiple, potentially uncoordinated sources, they must perform this kind of "last chance" safety check.

11: If the directive is permitted, the Actuator processes the directive. No feedback is provided to the Field Application on success.

12: If the directive is not permitted, the Actuator sends data to the Field Application indicating that the directive could not be processed. This allows the Field Application to re-evaluate based on this feedback and potentially determine an alternate action or notify the Information Repository of the failure.

Use Case 2: Field Application Requests Data from Sensor or Other Field Application

Use Case Description: A Field Application determines that it needs new or updated data from a Sensor or another Field Application and directly requests that data.

Preconditions:

- Field Applications and Sensors are operational and have been initialized with routing/communication information.

Minimal Guarantees:

- No operational changes will be made by the data supplier.

Success Guarantees:

- The data supplier has received the request for updated data.

Trigger:

The Field Application determines that it needs updated data from a Sensor or another Field Application.

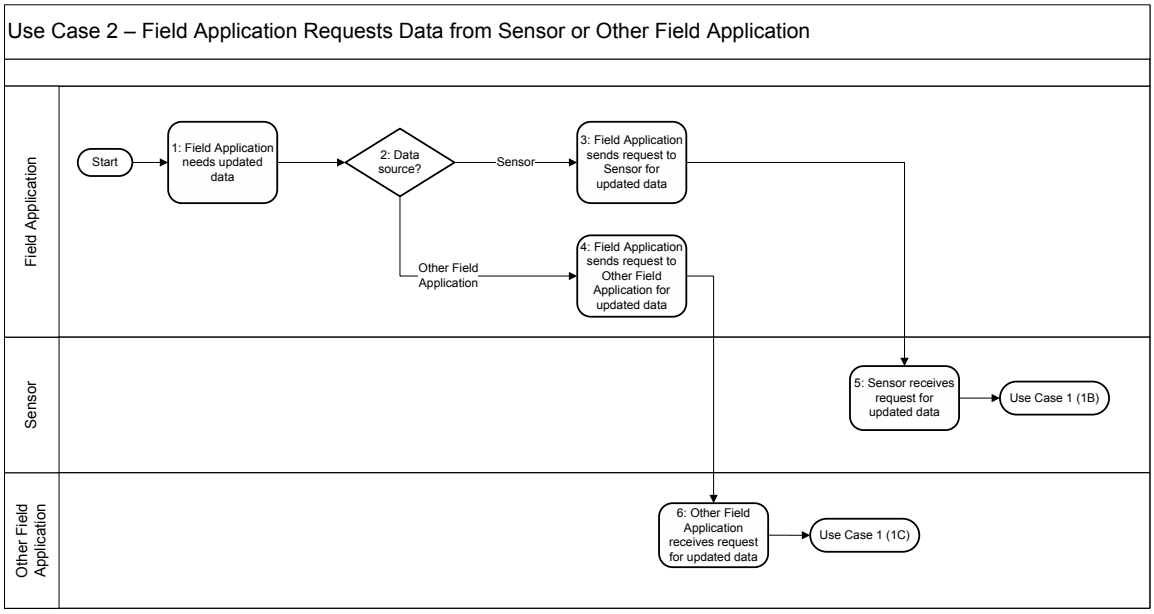

Diagram: Use Case 2 – Field Application Requests Data from Sensor or Other Field Application

Main Success Scenario:

1: The Field Application determines that it needs updated data from a Sensor or another Field Application. This could be because a Sensor has not reported recently or changing conditions indicate a need to get more frequent updates.

2: The Field Application determines which actor has the required data.

3: If a Sensor is responsible for the data, the Field Application sends a request to the Sensor for an update to that data.

4: If another Field Application is responsible for the data, the Field Application sends a request to that Field Application for an update to that data.

5: The Sensor receives the request from the Field Application. This step triggers Use Case 1 (option 1B), in which the Sensor sends the requested data to the Field Application.

6: The other Field Application receives the request from the original Field Application. This step triggers Use Case 1 (option 1C), in which the other Field Application sends the requested data to the original Field Application.

Use Case 3: Actuator, Sensor, or External Application Sends Data to Information Repository

Use Case Description: A Sensor, Actuator, or External Application sends data to the Information Repository.

Preconditions:

- Sensors, Actuators, External Applications, and the Information Repository are operational and have been initialized with routing/communication information.

Minimal Guarantees:

- No operational changes will be made by the information supplier.
- No false information will be sent to the Information Repository.

Success Guarantees:

- The Information Repository receives and begins processing the sent data (in a subsequent use case).

Trigger:

There are three possible triggers for this use case

- An Actuator sends data to the Information Repository. This usually only occurs when an Actuator is reporting health or logging information, such as when a problem is encountered.
- A Sensor sends data to the Information Repository. This could be a scheduled event, a spontaneous event, or a response to a request for new information (as coming from Use Case 13).
- An External Application sends data to the Information Repository. This is usually a spontaneous event (as coming from Use Case 14).

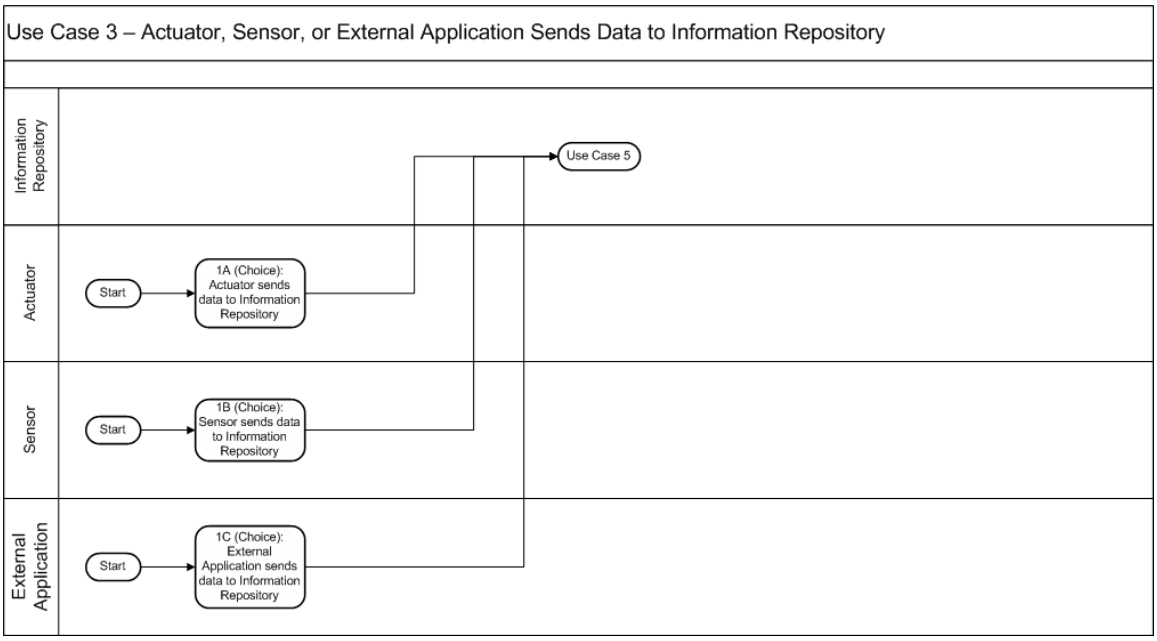

Diagram: Use Case 3 – Actuator, Sensor, or External Application Sends Data to Information Repository

Main Success Scenario:

1A: An Actuator sends data to the Information Repository. This usually only occurs when an Actuator is reporting health or logging information, such as when a problem is encountered. This step triggers Use Case 5, in which the Information Repository processes the new data.

1B: A Sensor sends data to the Information Repository. This could be a scheduled event, a spontaneous event, or a response to a request for new information. This step triggers Use Case 5, in which the Information Repository processes the new data.

1C: An External Application sends data to the Information Repository. This is usually a spontaneous event. This step triggers Use Case 5, in which the Information Repository processes the new data.

Use Case 4: Information Repository Synchronizes with Another Information Repository

Use Case Description: An Information Repository, based on some internal criteria, synchronizes some portion of its data with another Information Repository. The synchronization is one-way—a push from the initiating Information Repository to a destination Information Repository.

Preconditions:

- Information Repositories are operational and have been initialized with routing/communication information.
- An agreement has been reached as to the extent of data that should be synchronized between Information Repositories.

Minimal Guarantees:

- No data will be modified at the Information Repository initiating the synchronization.

Success Guarantees:

- The destination Information Repository receives and begins processing the synchronized data (in a subsequent use case).

Trigger:

The Information Repository determines that it is time to update another Information Repository with some portion of its data. This determination may be based on a timer or some other criteria (e.g., accumulation or criticality of unsynchronized data). Updates that are performed as soon as data is received by the Information Repository are handled in Use Case 5.

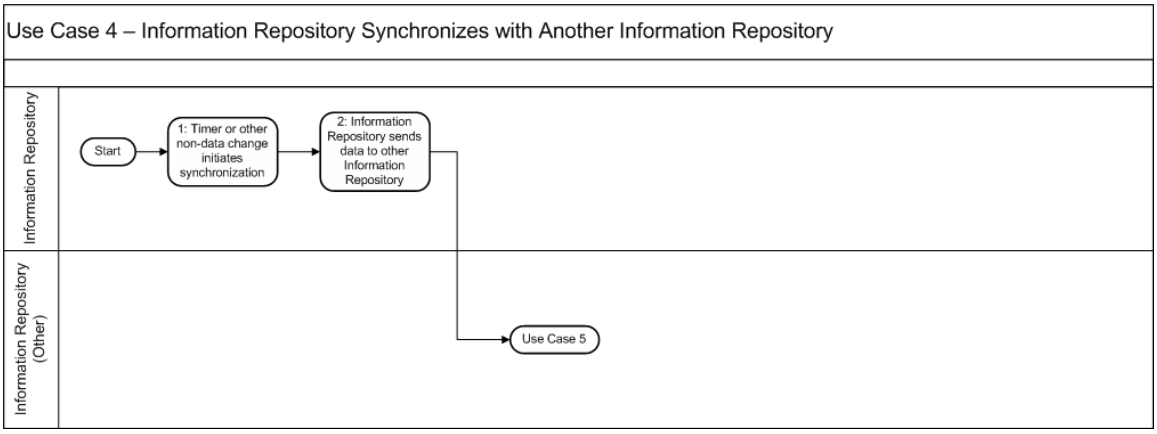

Diagram: Use Case 4 – Information Repository Synchronizes with Another Information Repository

Main Success Scenario:

1: The Information Repository determines that it is time to update another Information Repository with some portion of its data. This determination may be based on a timer or some other criteria (e.g., accumulation or criticality of unsynchronized data). The synchronization may involve individual data items or batches of data.

2: The Information Repository sends all data that should be synchronized to the other Information Repository. The exact means of transfer is unspecified; the other Information Repository may be local or remote. This step triggers Use Case 5, in which the other Information Repository processes the new data (taking on the role of the primary Information Repository).

Use Case 5: Information Repository Processes New Data

Use Case Description: An Information Repository receives new or updated data and responds by sending the data to any Central Application, External Application, or other Information Repository which may be linked to or using said data from the Information Repository.

Preconditions:

- The Information Repository is able to receive data updates (from Sensors, Actuators, Field Applications, Central Applications, External Applications, and other Information Repositories).
- A valid relationship has been established between an Information Repository and any actor which is attempting to write new data to or update existing data in the Information Repository.
- A valid relationship has been established between an Information Repository and any actor which is interested in/subscribed to specific data within the Information Repository.

Minimal Guarantees:

- An Information Repository will not accept data from an unauthorized source (Actor).
- Data which has been written to or updated in an Information Repository will not be altered by the Information Repository.

Success Guarantees:

- Whenever an Information Repository receives authorized data writes or updates, all interested/subscribed Central Applications, External Applications, or other Information Repositories will be notified.
- An Information Repository will provide information, such as time and/or quality, about the validity of the data being provided to Central Applications, External Applications, or other Information Repositories.

Trigger:

This use case is triggered whenever data is received by an Information Repository (from Sensors, Actuators, Field Applications, Central Applications, External Applications, and other Information Repositories).

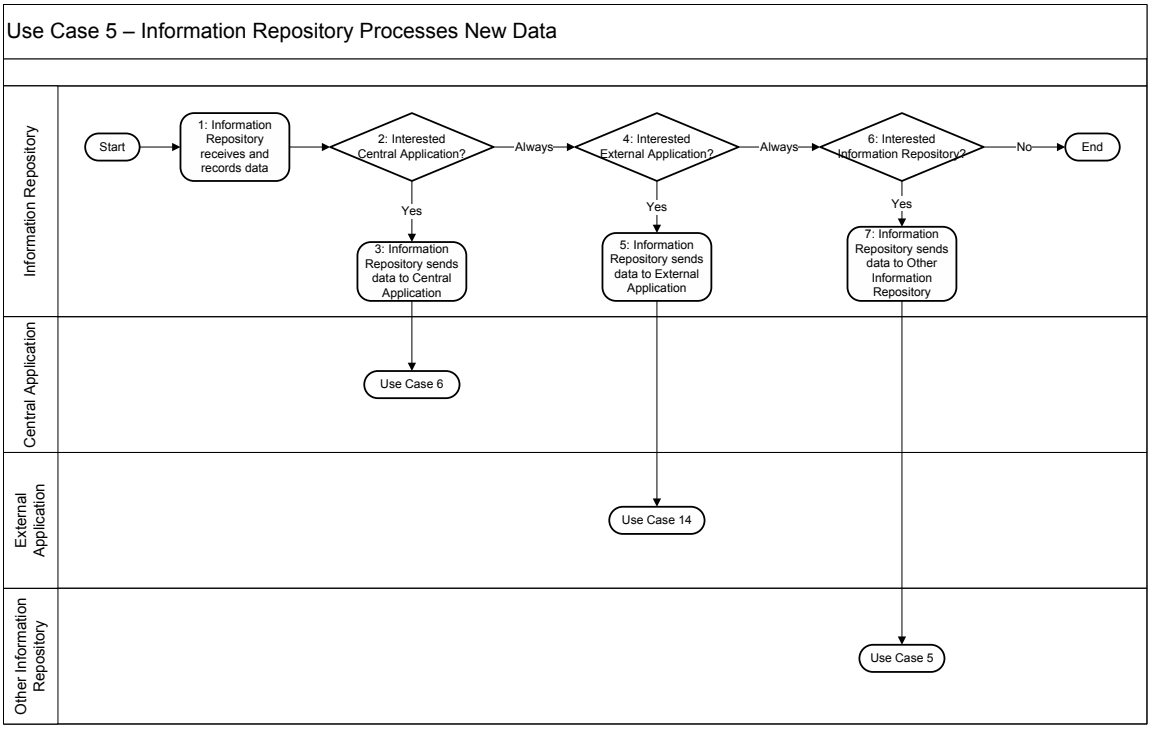

Diagram: Use Case 5 – Information Repository Processes New Data

Main Success Scenario:

1: An Information Repository receives new data from a Sensor, Actuator, Field Application, Central Application, External Application, or other Information Repository. The Information Repository then records the data within its associated storage mechanism.

2: The Information Repository determines if there are any Central Applications that are interested in the data. This may be via a pre-existing publish/subscribe mechanism between the Information Repository and Central Application(s).

3: If there are Central Application(s) that are interested in the specific data, the Information Repository sends data to the Central Application(s). This can be a push of the new data to from the Information Repository to the Central Application(s), a notification from the Information Repository to the Central Application(s) that new data is available, or some other mechanism. This step triggers Use Case 6, in which the Central Application processes new data.

4: The Information Repository determines if there are any External Applications that are interested in the data. This may be via a pre-existing publish/subscribe mechanism between the Information Repository and External Application(s).

5: If there are External Application(s) which are interested in the specific data, the Information Repository sends data to the External Application(s). This can be a push of the new data to from the Information Repository to the External Application(s), a notification from the Information Repository to the External Application(s) that new data is available, or some other mechanism. This step triggers Use Case 14, in which an External Application processes new data.

6: The Information Repository determines if there are any other Information Repositories that are interested in the data. This may be via a pre-existing publish/subscribe mechanism between the two Information Repositories.

7: If there are other Information Repositories that are interested in the specific data, the Information Repository sends data to the other Information Repositories. This can be a push of the new data to from one Information Repository to the other, a notification from the Information Repository to the other that new data is available, or some other mechanism. This step triggers a new occurrence of this use case for the other Information Repository (which will take on the role of the primary Information Repository).

Use Case 6: Central Application Processes New Data

Use Case Description: A Central Application receives new or updated data and processes it by updating displays, alerting users, deriving new data and writing it back to an Information Repository, and/or sending a directive to a Control Authority.

Preconditions:

- A valid relationship has been established between the Central Application and Information Repository(s) that it uses.
- The Central Application is able to receive new or updated data from the Information Repository(s) that it uses.
- Thresholds have been defined within the Central Application to determine when (and when not to) process data changes.

Minimal Guarantees:

- A Central Application will not process data from an unauthorized source.
- A Central Application will not process data from an authorized source unless it meets a predefined, minimum threshold.

Success Guarantees:

- The Central Application processes new or updated data correctly.

Trigger:

This use case is triggered whenever the Central Application receives new or updated data from an associated Information Repository.

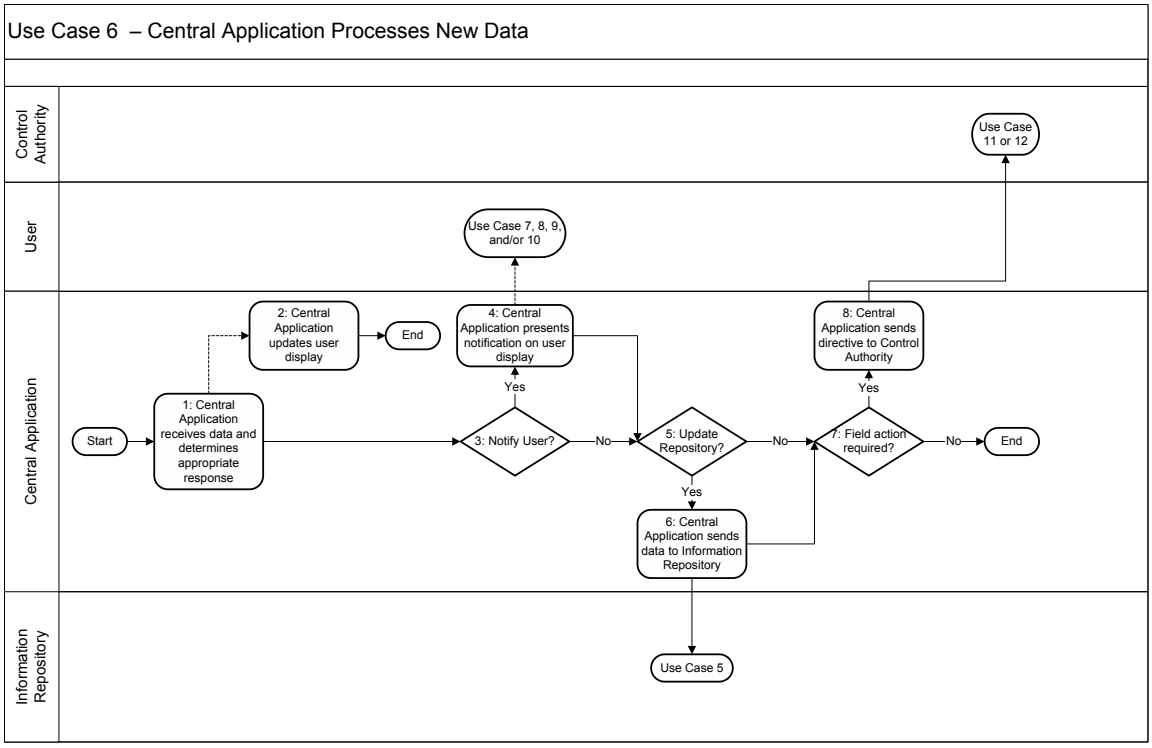

Diagram: Use Case 6 – Central Application Processes New Data

Main Success Scenario:

1: A Central Application receives new or updated data from an Information Repository. The new or updated data is then processed by the Central Application based on the application's defined set of rules. Thresholds may be employed so that data changes or updates which do not meet the established threshold are not processed. This practice is typically used for analog type data to minimize unnecessary resource utilization.

2 (Optional Step): The Central Application may update user displays that are linked to the new or updated data received from the Information Repository. This is a passive update; it does not prompt the User for any kind of decision.

3: The Central Application determines, based on its predefined set of rules, if a User should be notified and what type of notification should be used.

4: If the Central Application determines that a User should be notified (in a more explicit manner than in step 2), the Central Application generates the notification via the user display. This notification can range from simple output display to more sophisticated outputs which contain recommended user actions. This step may trigger Use Cases 7, 8, 9, and/or 10, in which the User interacts with the Central Application.

5: The Central Application determines, based on its predefined set of rules, if an Information Repository should be updated. An update may be necessary, for example, if the Central Application computes derived or composite data as part of it's processing.

6: If the Central Application determines that an Information Repository should be updated, the Central Application sends data to the Information Repository. This step triggers Use Case 5, in which the Information Repository processes the new data.

7: The Central Application determines, based on its predefined set of rules, if a field action is required and what that action should be. A field action can consist of change of Equipment (i.e. breaker, switch, recloser, etc.) state or input data into a Field Application.

8: If the Central Application determines that a field action is necessary, the Central Application sends a directive to the Control Authority. This step triggers Use Cases 11 or 12, in which the Control Authority processes the directive.

Use Case 7: User Sends Command Request to Application

Use Case Description: A User of a Central Application or Field Application directs the application to take a desired action.

Preconditions:

- A valid relationship has been established between the User and the Central Application or Field Application.
- The User is able to interact with the Central Application or Field Application.
- The Control Authority is able to receive a directive from the Central Application.

Minimal Guarantees:

- A Central Application or Field Application will not process any directive from an unauthorized User.
- A Central Application or Field Application will not process an invalid directive from an authorized User.

Success Guarantees:

- The Central Application or Field Application accepts and processes the directive.
- The Central Application or Field Application provides feedback to the User of acceptance or rejection of the request.

Trigger:

This use case is triggered whenever a User directs a Central Application or Field Application to take an action. This may be in response to new information available via a user display or may be the result of a spontaneous decision by the User.

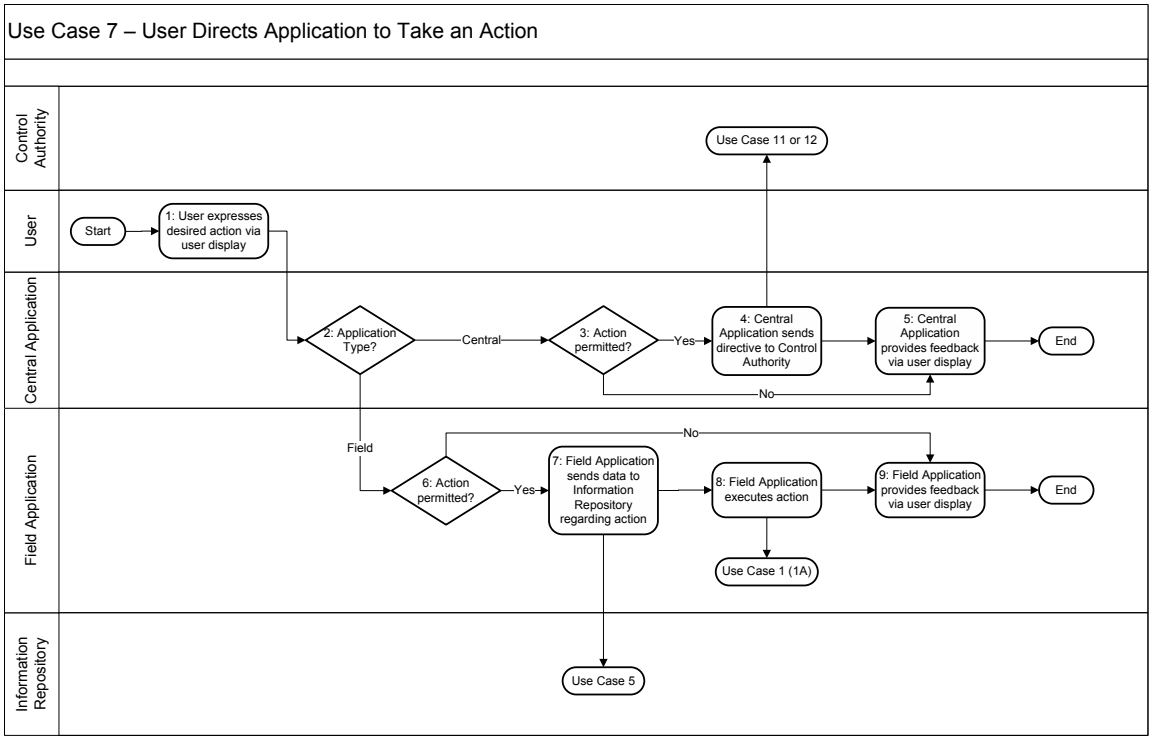

Diagram: Use Case 7 – User Directs Application to Take an Action

Main Success Scenario:

1: A User of a Central Application or Field Application directs the application to take a desired action via the user display. This action could be in response to a notification from a Central Application or a spontaneous act by the User.

2: This use case is crafted to cover either a User interacting with a Central Application or a Field Application. For a User of a Central Application, use case steps 3 – 5 are applicable. For a User of a Field Application, use case steps 6 – 9 are applicable.

3: The Central Application determines if the action specified by the User is permitted. This is an internal application check to validate basic availability of the application to carry out the request.

4: If the action specified by the User is permitted, the Central Application sends a directive to the Control Authority. The step triggers Use Case 11 or 12, in which the Control Authority processes a directive.

5: The Central Application provides feedback to the user of acceptance or rejection of the directive via the user display.

6: The Field Application determines if the action specified by the User is permitted. This is an internal application check to validate basic availability of the application to carry out the request.

7: If the directive is permitted, the Field Application sends data to the Information Repository regarding pending directive processing. This step triggers Use Case 5, in which the Information Repository processes new data.

8: The Field Application processes the directive. This step triggers Use Case 1, in which the Field Application makes a decision.

9: The Field Application provides feedback to the user of acceptance or rejection of the directive via the user display.

Use Case 8: User Sends Data to Central Application

Use Case Description: A User enters data in a Central Application. Data entered by the User is then sent to the Information Repository by the Central Application.

Preconditions:

- A valid relationship has been established between a User and a Central Application.
- The Central Application is able to receive data entered by a User.

Minimal Guarantees:

- A Central Application will not process any data entered from an unauthorized User.
- A Central Application will not process invalid data entered from an authorized User.

Success Guarantees:

- The Central Application accepts the User data input request and sends the User data to the Information Repository.
- The Central Application provides feedback to the User of acceptance or rejection of the data entry.

Trigger:

This use case is triggered whenever a User enters data via a Central Application. This may be in response to new information available via a user display or may be the result of a spontaneous decision by the User.

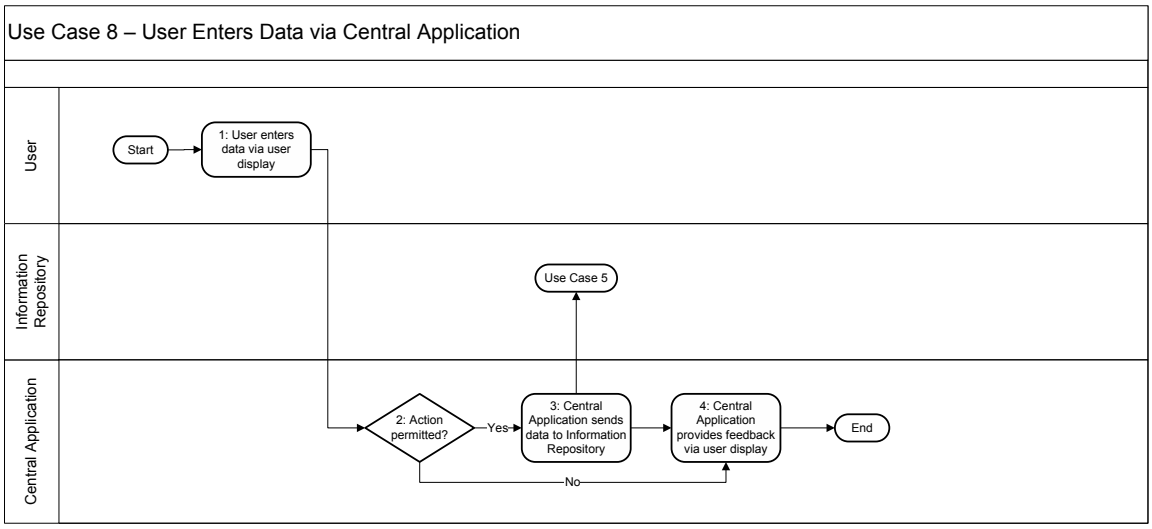

Diagram: Use Case 8 – User Enters Data via Central Application

Main Success Scenario:

1: A User enters data via the Central Application. This action could be in response to a notification from a Central Application or a spontaneous act by the User.

2: The Central Application determines if the User entered data is accepted. This is an internal application check to validate basic availability of the application to carry out the request.

3: If the User entered data is accepted, the Central Application sends the data to the Information Repository. This step triggers Use Case 5, in which the Information Repository processes new data.

4: The Central Application provides feedback to the User of acceptance or rejection of the data entry via the user display.

Use Case 9: User Requests Application Mode Change

Use Case Description: A User of a Central Application or Field Applications initiates a change in the operating mode of the application.

Preconditions:

- A valid relationship has been established between a User and a Central Application or a Field Application.
- The User is able to interact with the Central Application or the Field Application.

Minimal Guarantees:

- A Central Application or Field Application will not process any input initiated by an unauthorized User.
- A Central Application or Field Application will not process an invalid input initiated by an authorized User.

Success Guarantees:

- If the User input is accepted, the operating mode of the Central Application or Field Application is changed.
- The Central Application or Field Application provides feedback to the User of acceptance or rejection of the operating mode change.

Trigger:

This use case is triggered whenever a User initiates a change to the operating mode of a Central Application or Field Application. This may be in response to new information available via a user display or may the result of a spontaneous decision by the User.

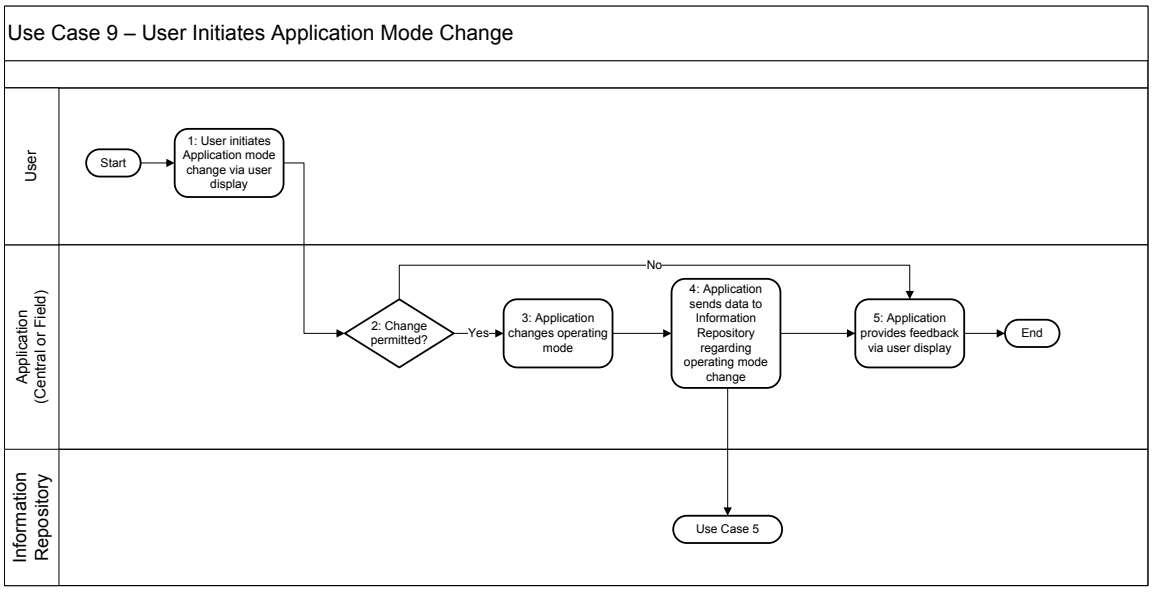

Diagram: Use Case 9 – User Initiates Application Mode Change

Main Success Scenario:

1: A User of a Central Application or Field Application initiates a request to change the operating mode of the application via the user display. This action could be in response to a notification from a Central Application or a spontaneous act by the User.

2: The Central Application or Field Application determines if the User is permitted to change the operating mode. This is an internal application check to validate basic availability of the application to carry out the request.

3: If the operating mode change is permitted, the Central Application or Field Application changes to the requested operating mode.

4: The Central Application or Field Application sends data to the Information Repository regarding the new operating mode of the application. This step triggers Use Case 5, in which the Information Repository processes new data.

5: The Central Application or Field Application provides feedback to the user of acceptance or rejection of the operating mode change request via the user display.

Use Case 10: User Requests Application Parameter Change

Use Case Description: A User of a Central Application or Field Applications initiates a change to an operating parameter of the application.

Preconditions:

- A valid relationship has been established between a User and a Central Application or a Field Application.
- The Central Application or the Field Application is able to receive an input (e.g. application parameter) from a User.

Minimal Guarantees:

- A Central Application or Field Application will not process any input initiated by an unauthorized User.
- A Central Application or Field Application will not process an invalid input initiated by an authorized User.
- A Central Application or Field Application will only change the requested parameter.

Success Guarantees:

- If the User input is accepted, the operating parameter of the Central Application or Field Application is changed.
- The Central Application or Field Application provides feedback to the User of acceptance or rejection of the application parameter change.

Trigger:

This use case is triggered whenever a User initiates a change to an operating parameter of a Central Application or Field Application. This may be in response to new information available via a user display or may the result of a spontaneous decision by the User.

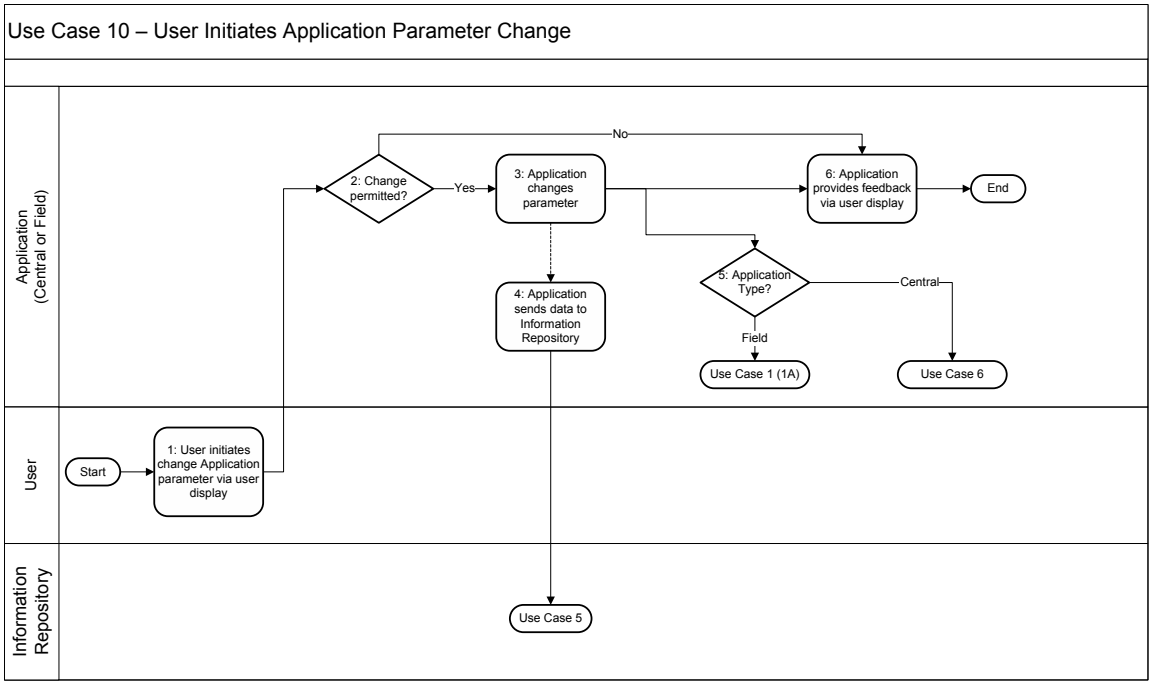

Diagram: Use Case 10 – User Initiates Application Parameter Change

Main Success Scenario:

1: A User of a Central Application or Field Application initiates a change to an operating parameter of the application via the user display. This action could be in response to a notification from a Central Application or a spontaneous act by the User.

2: The Central Application or Field Application determines if the User is permitted to change the application parameter. This is an internal application check to validate basic availability of the application to carry out the request.

3: The Central Application or Field Application changes the specified operating parameter.

4 (Optional Step): The Central Application or Field Application sends data to the Information Repository regarding the operating parameter change. This step triggers Use Case 5, in which the Information Repository processes new data.

5: This use case is crafted to cover either a User interacting with a Central Application or a Field Application. For a User of a Central Application, Use Case 6 is triggered, in which the Central Application processes data based on its new parameters. For a User of a Field Application, Use Case 1 (Option 1A) is triggered, in which the Field Application re-evaluates conditions based on its new parameters.

6: The Central Application or Field Application provides feedback to the user of acceptance or rejection of the operating mode change request via the user display.

Use Case 11: Control Authority Processes Command Request for Field Application

Use Case Description: A Control Authority responds to a directive for a Field Application (either from a Central Application or an External Application) by first determining whether the directive is permitted. If permitted, the Control Authority forwards the directive to the appropriate Field Application. The Field Application also makes a determination as to whether the directive is permitted (based on local conditions) and then processes the directive. All actions and non-actions are recorded in the Information Repository.

Preconditions:

- The Control Authority is able to receive a directive.

Minimal Guarantees:

- The Control Authority will not forward directives that are not permitted to the Field Application.
- The Field Application will not process directives that are not permitted.

Success Guarantees:

- Whenever the Control Authority receives authorized directives, they will be forwarded to the Field Application for processing.
- The actions or non-actions will be recorded in the Information Repository.

Trigger:

This use case is triggered whenever the Control Authority receives a directive for a Field Application. These directives can come from Central Applications or External Applications.

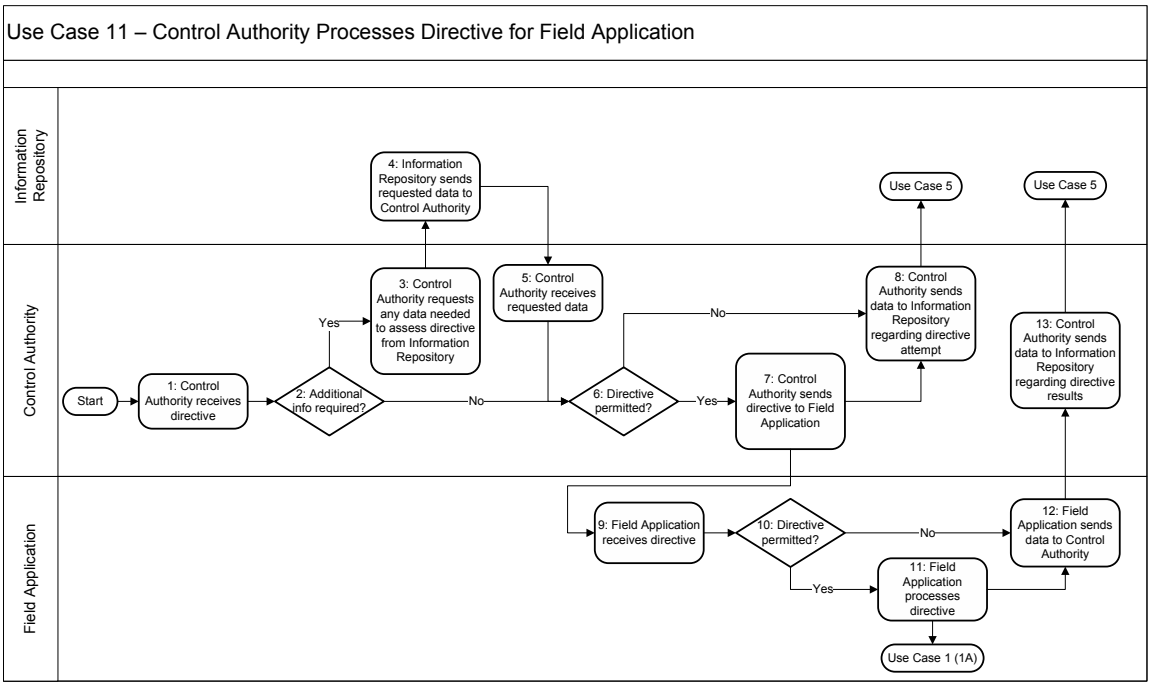

Diagram: Use Case 11 – Control Authority Processes Directive for Field Application

Main Success Scenario:

1: The Control Authority receives a directive to be dispatched to a Field Application. These directives can come from Central Applications or External Applications.

2: The Control Authority determines whether any additional information is required to assess the directive. The kind of information required includes current operational state of devices or applications (e.g., whether the target application is currently in service or ongoing maintenance).

3: If additional information is required, the Control Authority requests this data from the Information Repository.

4: The Information Repository receives the data request and sends the requested data back to the Control Authority.

5: The Control Authority receives the requested data from the Information Repository.

6: The Control Authority determines if the directive is permitted. A directive may not be permitted if the target Field Application is currently out-of-service or if competing or conflicting directives are being processed for the Field Application. A directive may also be temporarily blocked at this step until it can proceed (e.g., until a different directive for the same Field Application has been completed).

7: If permitted, the Control Authority forwards the directive to the Field Application.

8: The Control Authority sends data to the Information Repository regarding the directive. Reported information will minimally include the directive, the target Field Application, and whether the directive was permitted. If the directive was not permitted, this information also includes a reason for the directive failure. This step triggers Use Case 5, in which the Information Repository processes the new data.

9: The Field Application receives the directive from the Control Authority.

10: The Field Application determines if the directive is permitted. The Field Application may determine that the directive is not permitted because of a conflicting directive or a current status issue such as a local lockout or disable when someone is working in the vicinity.

11: If the directive is permitted the Field Application processes the directive. Such processing may involve changing the Field Application's parameters or recording directives that should be issued to Actuators. This step triggers Use Case 1 (option 1A), in which the Field Application re-evaluates its state and completes any necessary actions.

12: The Field Application sends data to the Control Authority regarding the disposition of the directive—successful or not permitted (along with any explanatory information).

13: The Control Authority sends data to the Information Repository regarding whether the Field Application processed the directive. Reported information will minimally include the directive, the target Field Application, and whether the Field Application processed the directive. If the directive was not processed, this notification also indicates why the Field Application did not allow the directive to be processed. This step triggers Use Case 5, in which the Information Repository processes the new data.

Use Case 12: Control Authority Processes Command Request for Actuator

Use Case Description: A Control Authority responds to a directive for an Actuator (either from a Central Application or an External Application) by first determining whether the directive is permitted. If permitted, the Control Authority forwards the directive to the appropriate Actuator. The Actuator also makes a determination as to whether the directive is permitted (based on local conditions) and if so, processes the directive. All actions and non-actions are recorded in the Information Repository.

Preconditions:

- The Control Authority is able to receive a directive.

Minimal Guarantees:

- The Control Authority will not forward directives that are not permitted to the Actuator.
- The Actuator will not process directives that are not permitted.

Success Guarantees:

- Whenever the Control Authority receives authorized directives, they will be forwarded to the Actuator for processing.
- The actions or non-actions will be recorded in the Information Repository.

Trigger:

This use case is triggered whenever the Control Authority receives a directive for an Actuator. These directives can come from Central Applications or External Applications.

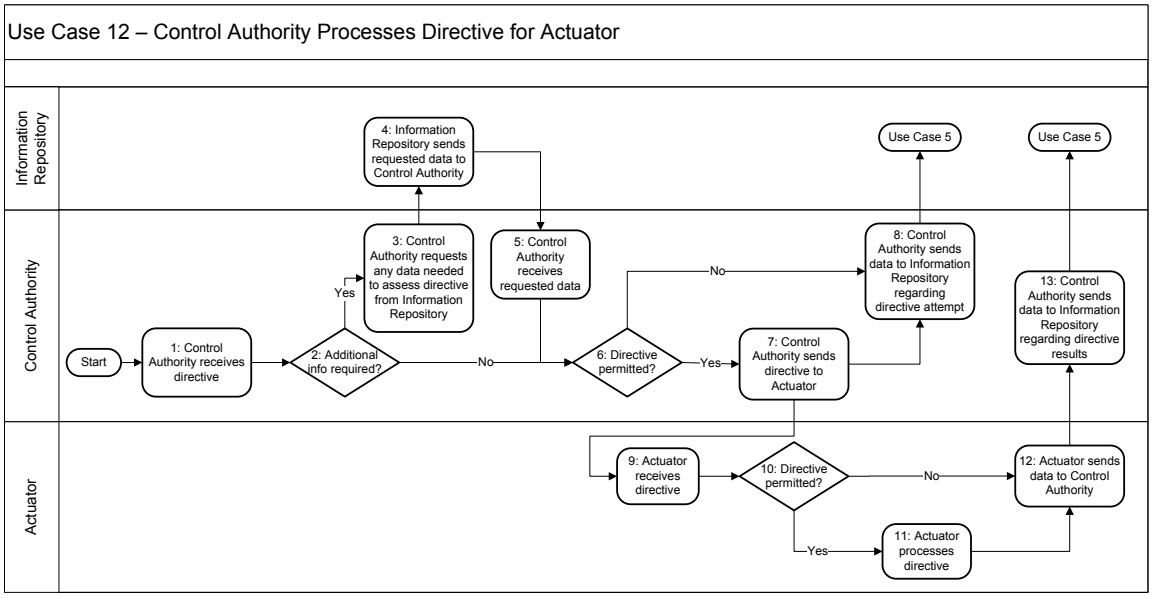

Diagram: Use Case 12 – Control Authority Processes Directive for Actuator

Main Success Scenario:

1: The Control Authority receives a directive to be dispatched to an Actuator. These directives can come from Central Applications or External Applications.

2: The Control Authority determines whether any additional information is required to assess the directive. The kind of information required includes current operational state of devices or applications (e.g., whether the target Actuator is currently in service or ongoing maintenance).

3: If additional information is required, the Control Authority requests this data from the Information Repository.

4: The Information Repository receives the data request and sends the requested data back to the Control Authority.

5: The Control Authority receives the requested data from the Information Repository.

6: The Control Authority determines if the directive is permitted. A directive may not be permitted if the target Actuator is currently out-of-service or if competing or conflicting directives are being processed for the Actuator. A directive may also be temporarily blocked at this step until it can proceed (e.g., until a different directive for the same Actuator has been completed).

7: If permitted, the Control Authority forwards the directive to the Actuator.

8: The Control Authority sends data to the Information Repository regarding the directive. Reported information will minimally include the directive, the target Actuator, and whether the directive was permitted. If the directive was not permitted, this information also includes a reason for the directive failure. This step triggers Use Case 5, in which the Information Repository processes the new data.

9: The Actuator receives the directive from the Control Authority.

10: The Actuator determines if the directive is permitted. The Actuator may determine that the directive is not permitted because of a conflicting directive or a current status issue such as a local lockout or disable when someone is working in the vicinity.

11: If the directive is permitted, the Actuator processes the directive. Such processing may involve changing the Actuator's parameters or recording directives that should be issued to Actuators.

12: The Actuator sends data to the Control Authority regarding the disposition of the directive—successful or not permitted (along with any explanatory information).

13: The Control Authority sends data to the Information Repository regarding whether the Actuator processed the directive. Reported information will minimally include the directive that was requested, the target Actuator, and whether the Actuator processed the directive. If the directive was not processed, this notification also indicates why the Actuator did not allow the directive to be processed. This step triggers Use Case 5, in which the Information Repository processes the new data.

Use Case 13: Central Application or Information Repository Requests Data from Field Application or Sensor

Use Case Description: A need for up to date data within the Information Repository leads to the Information Repository requesting data from either a Field Application or Sensor. This can be initiated by either an internal mechanism within the Information Repository or via a request to the Information Repository from a Central Application. The Field Application or Sensor then returns the requested data to the Information Repository.

Preconditions:

- A valid relationship has been established between the Information Repository and Central Application.
- The Central Application is able to send requests to the Information Repository.
- A valid relationship has been established between the Information Repository and Field Application or Sensor.
- The Information Repository is able to send requests to the Field Application and Sensor.
- The Field Application or Sensor is able to send data to the Information Repository.

Minimal Guarantees:

- Data will be requested from the correct Field Application or Sensor corresponding to the data within the Information Repository.
- The Information Repository will not process any requests from unauthorized Central Applications.

Success Guarantees:

- Up to date Field Application or Sensor data will be available from the Information Repository after requested by a Central Application or scheduled by the Information Repository.

Trigger:

This use case is triggered by one of two conditions relating to data within the Information Repository that is derived from a Field Application or Sensor.

- The Information Repository determines via internal mechanism that an update or refresh to Field Application or Sensor data within the Information Repository is necessary.
- The Information Repository receives a request from a Central Application for an update or refresh to Field Application or Sensor data within the Information Repository is necessary.

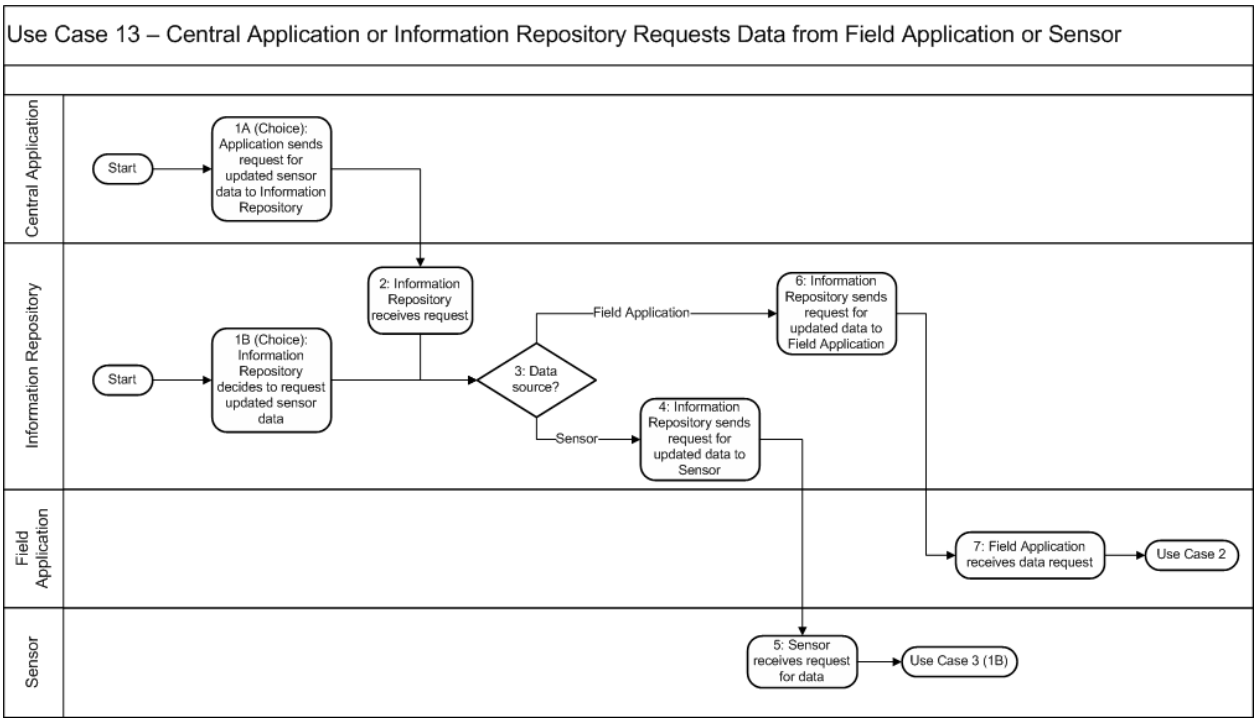

Diagram: Use Case 13 – Central Application or Information Repository Requests Data from Field Application or Sensor

Main Success Scenario:

1A: A Central Application sends a request for an update of Field Application or Sensor data to the Information Repository.

1B: The Information Repository determines via internal mechanism that an update of Field Application or Sensor data within the Information Repository is necessary.

2: The Information Repository receives the request for updated data from the Central Application.

3: The Information Repository determines the specific Field Application or Sensor that can provide the requested data. This may involve queries to determine device/messaging specific data such as protocol address, IP address, etc.

4: If a Sensor can provide the data, the Information Repository sends a request for updated data to the Sensor.

5: The Sensor receives the request for updated data. This step triggers Use Case 3 (option 1B) in which the Sensor sends data back to the Information Repository.

6: If a Field Application can provide the data, the Information Repository sends a request for updated data to the Field Application.

7: The Field Application receives the request and sends the updated data back to the Information Repository. This step triggers Use Case 5, in which the Information Repository processes the new data.

Use Case 14: External Application Processes New Data

Use Case Description: An External Application receives and processes new or updated data.

Preconditions:

- A valid relationship has been established between the External Application and Information Repository(s) which it uses.
- The External Application is able to receive new or updated data from the Information Repository(s) which it uses.
- Thresholds have been defined within the External Application to determine when (and when not to) process data changes.

Minimal Guarantees:

- An External Application will not process data from an unauthorized source.

Success Guarantees:

- The External Application processes new or updated data correctly.

Trigger:

This use case is triggered whenever the External Application receives new or updated data from an associated Information Repository.

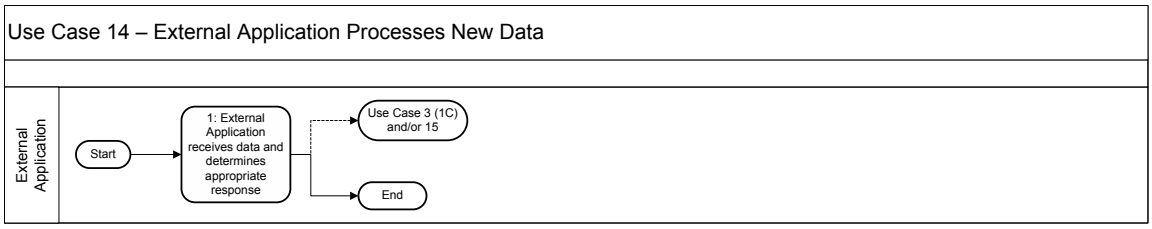

Diagram: Use Case 14 – External Application Processes New Data

Main Success Scenario:

1: An External Application receives new or updated data from an Information Repository. The new or updated data is then processed by the External Application based on the application's defined set of rules. Thresholds may be employed so that data changes or updates which do not meet the establish threshold are not processed. This practice is typically used for analog data to minimize unnecessary resource utilization. This step may trigger Use Case 3 (option 1C), in which the External Application sends data to the Information Repository. This step may also trigger case 15, in which the External Application sends a directive to the Control Authority.

Use Case 15: External Application Sends Command Request to Control Authority

Use Case Description: An External Application sends a directive to the Control Authority. This need for the External Application to send the directive could be initiated by events such as the routine execution of the application, input data change, or User request. These interactions with the External Application however, are out of scope in the context of this use case.

Preconditions:

- The Control Authority is able to receive a directive from the External Application.

Minimal Guarantees:

- None.

Success Guarantees:

- The External Application successfully sends the directive to the Control Authority.

Trigger:

This use case is triggered whenever the External Application sends a directive to the Control Authority.

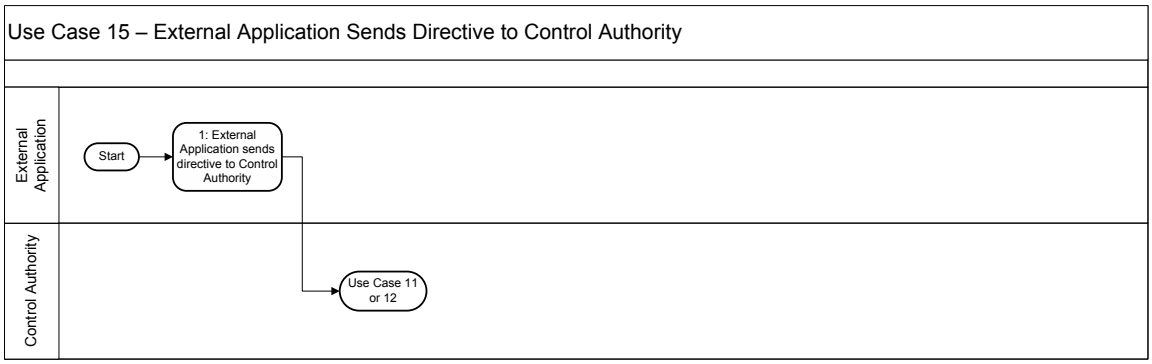

Diagram: Use Case 15 – External Application Sends Directive to Control Authority

Main Success Scenario:

1: An External Application sends a directive to the Control Authority. This step triggers Use Cases 11 and/or 12, in which the Control Authority processes a directive for a Field Application or Actuator respectively.

3 Failure Analysis

The underlying approach used to create this security profile began with defining the functions of the DM system through abstract roles and use cases. The development of the use cases and the definition of roles took into account a foundational set of security and operational objectives that is also used in the next step of the process, failure analysis. The failure analysis is the focus of this section. A brief overview of the foundational security and operational objectives is presented in Section 3.1 and a more detailed view of the identified failures and the connection between use cases and the failures is presented in Section 3.2.

The failure identification and analysis process is loosely based on conducting a Failure Modes and Effects Analysis (FMEA) on the logical DM architecture presented in Section 2, however the analysis was performed with a security bias to failure identification. A FMEA is a procedure for analyzing potential system failures and their associated modes as a function of system entities--assemblies, subassemblies, components, subcomponents, etc. This process leads to an understanding of the severity of the failure (consequences) and its impact on the system's operations and stability.

For this security profile, failure analysis centered on the roles and use cases defined in Sections 2.1 and 2.3 and the impact of potential failures on a distribution management system. This process was used to identify DM system issues, which were 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 was examined for potential failures against the security and operational objectives with respect to each role. All of the identified failures were then aggregated and generalized across all use cases.

3.1 Security and Operational Objectives

The goal of this document is to establish a cyber environment in which a DM system can successfully and securely operate. Meeting this goal requires that a number of security and operational objectives that support that goal are achieved. Ten objectives for the DM system were identified and utilized throughout the profile development process. These objectives served as the "ground rules" for the DM systems and helped with use case development and failure identification. The ten objectives are as follows:

1. Security controls shall not interfere with the primary mission of the DM system.
2. The operational state of the DM system and its components must be deterministic.[2]
3. The Control Authority must be independent from the applications that generate control commands.
4. Users shall not be allowed to perform any action that falls outside of their assigned role.
5. No unauthorized or unauthenticated remote access shall be granted by a DM system device or component.
6. No unauthorized or unauthenticated control commands shall be processed by a DM system device or component.
7. All control activity (successful and unsuccessful) on the DM system shall be auditable.
8. No unauthorized or unauthenticated download of software (firmware, configuration, etc.) shall be accepted by a DM system device or component.
9. Any DM system device or component must be able to validate the authenticity and integrity of all data acquired from another DM device or component.
10. Asset owners must not rely on security measures outside their direct observation and control for protection from unauthorized access.

3.2 Failures

Failure analysis was performed by first analyzing each step of each use case against the security and operational objectives in Section 3.1. Failures that could lead to a violation of the objectives or interfere with the functional goal of the step were captured. After the initial failure identification step, the list of failures were grouped and generalized across the entire collection of use cases. The following tables below summarize the failure analysis.

Table 1 defines the failures. It includes a unique failure ID, a short definition of the failure, and a more elaborate explanation. It should be noted that the failure ID number does not imply any kind of priority assignment. In this table, a <Role> can be one of the nine essential roles (see Section 2.1) involved in distribution management systems, though a given failure may not be

[2] Deterministic means that future system state and actions of roles can be predicted from inputs to the system and the system's current state.

applicable to some roles. The failure analysis for this security profile resulted in the identification of 23 distinct failures.

Failure ID	Definition	Explanation
1	<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. Examples include: 1) writing the message to an invalid socket descriptor; 2) missing a transmit deadline due to a task-scheduling failure.
2	<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. Examples include: 1) transposing bytes in the recipients IP address, 2) retrieving incorrect entries from a host lookup table.
3	<Role> sends an incorrect type of message	The role sends a message containing information other than what is required by the recipient. Examples include: 1) sending a health and status report when a sensor reading is required; 2) returning an incorrect object type from remote procedure call.
4	<Role> sends an incorrectly formatted message	The role transmits a message using a protocol or message format that is not understood by the recipient. Examples include: 1) using little-endian encoding when big-endian is expected; 2) using wide characters when ASCII characters are expected.
5	<Role> sends a spurious message	The role transmits a message that is not required or expected by a legitimate recipient. Examples include: 1) broadcasting health and status information that should only be provided upon request.
6	<Role> does not receive a message in a timely manner	The transmission of a message must occur within a particular span of time, but the role fails to initiate reception of the message in that time. Examples include: 1) a message is discarded due to insufficient space in the receive buffer; 2) deadline for acting on the message is missed due to a task-scheduler failure.
7	<Role> processes 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. Examples include: 1) role responds to a health and status request that arrives from an unknown source; 2) role changes its operational settings on receiving a message from a public access computer (e.g., in a public library).
8	<Role> processes an incorrect type of message	The role receives a message other than the type that is expected, but processes that message

Failure ID	Definition	Explanation
		regardless. Example of this failure include: 1) Processing an instruction to reconfigure when only requests for health and status are expected; 2) Responding to a request for status when in a state that disallows these messages.
9	<Role> processes an incorrectly formatted message	The role processes a message with an expected type from a legitimate source but that is ill formed. For example: 1) the role processes a message that fails its CRC check; 2) the role processes a command to change a control set point to some value that is outside of its valid range.
10	<Role> processes a spurious message	The role receives a message that is not expected and then processes the information in the message. For example: 1) the role expects new data every minute, but upon receiving data every second processes the unexpected data; 2) the role extracts and processes a broadcasted command when no commands are expected on the broadcast channel.
11	<Role> does not respond to a message in a timely fashion	The role fails to respond to a query or verify execution of a command within the span of time provided for a response. Examples include: 1) failure of the task-scheduler to satisfy its deadline requirements, 2) the process terminates abnormally while forming a response to the query.
12	<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. Examples include: 1) failure of the task-scheduler to execute the command as required, 2) execution of the command is delayed due to by software or hardware failures.
13	<Role> fails to protect information or resources against unauthorized access	The role allows a user or device to read or modify data without regard for their credential and access rights. Examples include: 1) a file that should be read-only is marked as read-write, 2) data that should be encrypted is stored as plain text.
14	<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. Examples include: 1) a corrupted password file prevents authorized users from accessing the role, 2) software error in the message validation software incorrectly classifies well-formed message as invalid.
15	<Role> fails to execute action based on changes to its operational parameters, its data, or its internal state	The role fails to act in response to input from its sensors, legitimate commands from operators, or other events that should trigger action on the part of the role. Examples include: 1) role receives and

Failure ID	Definition	Explanation
		processes message to resynchronize its clock, but fails to actually carry out the resynchronization; 2) the role receives a message to close a switch, but the switch is left open.
16	<Role> executes wrong action based on changes to its operational parameters, its data, or its internal state	The role improperly reacts to input from its sensors, operators, etc. For example: 1) a sensor is instructed to raise its reporting threshold, but lowers it instead, 2) the role is instructed to delete a user's account, but instead resets the account password to a default value.
17	Manufacturer of the device that implements the <role> fails to apply appropriate methods for software engineering, human factors, and secure coding	The organization responsible for the design or manufacture of a device fails to apply due diligence during its construction. For example: 1) software for a device is written and installed, but never tested; 2) payloads received in UPD data-grams are copied into a fixed size buffer without regard for the payload's size.
18	<Role> accepts corrupted configuration file	The role applies new configuration settings regardless of their integrity. For example: 1) a secure shell server loads and processes a configuration file that contains unrecognized instructions; 2) a device silently uses default settings when provided with incorrect configuration data.
19	Hardware, facilities or both fail and prevent proper operation	Loss of power, severed communication wires, failure of electronic or mechanical components, or other hardware failure prevents the device from operating.
20	Organization that maintains <role> fails to implement appropriate version control, configuration control, patch management, maintenance procedures, or any combination of these.	The organization responsible for maintenance of the device fails to apply due diligence. Examples include: 1) installing but never applying patches to a Windows (or other) operating system; 2) failing to identify known conflicts between software versions (e.g., installing 64-bit software on a 32-bit computer).
21	<Role> is physically accessed by unauthorized personnel	The locks, protection force, or other mechanism for preventing physical access to a device or facility fails and allows unauthorized persons in.
22	Failure to provide adequate protection against reasonable expectations for harm due to natural phenomenon, such as earthquakes, hurricanes, tornadoes, and electromagnetic interference	Examples include placing critical computer facilities on a 10-year flood plain; failing to install surge protectors on critical electronic devices; or operating key facilities without a secondary source of power.
23	Failure to provide recovery mechanisms essential for the restoration of a failed or compromised	Examples of these failures include 1) the deletion of data for which there is no backup copy, and 2) critical operations that rely on irreplaceable

Failure ID	Definition	Explanation
	system	hardware or software (e.g., software that is executable only on an obsolete microprocessor).

Table 1 - DM Failures

Table 2 provides a mapping of the failures identified in Table 1 onto an operational space defined by use cases. It is unique in that it is described by use case steps and roles. Use case operational behaviors are defined in Section 2.3. An example would be that within Use Case 1 (Field Application Makes Decision), the unique pairing of the Field Application role with step 1A (The Field Application needs to re-evaluate conditions based on changes influencing its behavior) has potential failure modes defined by Failures 6 and 15.

Use Case	Use Case Step	Role	Failure(s)
1	All	All	17, 19, 20, 21, 22, 23
	1A	Field Application	6, 15
	1B	Sensor	1, 2, 3, 4, 5, 13, 15, 16, 18
	1C	Other Field Application	1, 2, 3, 4, 5, 13, 15, 16, 18
	2	Field Application	6, 7, 8 , 9, 10, 11, 14, 18
	3	Field Application	15
	4	Field Application	16
	5	Field Application	15, 16
	6	Field Application	1, 2, 3, 4, 5, 13, 18
	7	Field Application	1, 2, 3, 4, 5, 13, 18
	8	Field Application	1, 2, 3, 4, 5, 13, 18
	9	Actuator	6, 7, 8 , 9, 10, 11, 14
	10	Actuator	14, 15, 16
	11	Actuator	15, 16
	12	Actuator	1, 2, 3, 4, 5, 13, 18

Use Case	Use Case Step	Role	Failure(s)
2	All	All	17, 19, 20, 21, 22, 23
	1	Field Application	8,9, 14
	3	Field Application	1, 2, 3, 4, 5, 13, 18
	4	Field Application	1, 2, 3, 4, 5, 13, 18
	5	Sensor	6, 7, 8 , 9, 10, 11, 14
	6	Field Application	6, 7, 8 , 9, 10, 11, 14
3	ALL	All	17, 19, 20, 21, 22, 23
	1A	Actuator	1, 2, 3, 4, 5, 6, 13, 18
	1B	Sensor	1, 2, 3, 5, 6, 13, 18
	1C	External Application	1, 2, 3, 5, 6, 13, 18
4	ALL	ALL	17, 19, 20, 21, 22, 23
	1	Information Repository	15
	2	Information Repository	1, 2, 3, 4, 5, 13, 18
5	ALL	ALL	17, 19, 20, 21, 22, 23
	1	Information Repository	6, 7, 8 , 9, 10, 11, 14
	3	Information Repository	1, 2, 3, 4, 5, 13, 18
	5	Information Repository	1, 2, 3, 4, 5, 13, 18
	7	Information Repository	1, 3, 4, 5, 13, 18
6	All	All	17, 19, 20, 21, 22, 23
	1	Central Application	6, 7, 8 , 9, 10, 11, 14
	2	Central Application	1, 2, 3, 4, 5
	3	Central Application	15, 16
	4	Central Application	1, 2, 3, 4, 5

Use Case	Use Case Step	Role	Failure(s)
	5	Central Application	15, 16
	6	Central Application	1, 2, 3, 4, 5, 13, 18
	7	Central Application	15, 16,
	8	Central Application	1, 2, 3, 4, 5, 13, 18
7	All	All	17, 19, 20, 21, 22, 23
	1	User	3, 4
	3	Central Application	14, 15, 16, 18
	4	Central Application	1, 2, 3, 4, 5, 13, 18
	5	Central Application	3, 4
	6	Field Application	14, 15, 16, 18
	7	Field Application	1, 2, 3, 4, 5, 13, 18
	8	Field Application	12, 15, 16, 18
	9	Field Application	3, 4, 15, 16
8	All	All	17, 19, 20, 21, 22, 23
	1	User	3, 4
	2	Central Application	14, 15, 16, 18
	3	Central Application	1, 2, 3, 4, 5, 13, 18
	4	Central Application	3, 4, 15, 16, 18
9	All	All	17, 19, 20, 21, 22, 23
	1.	User	3,4
	2	Central Application Field Application	14, 15, 16, 18
	3	Central Application Field Application	12, 15, 16

Use Case	Use Case Step	Role	Failure(s)
	4	Central Application Field Application	1, 2, 3, 4, 5, 13, 18
10	All	All	17, 19, 20, 21, 22, 23
	1	User	2, 3, 4
	2	Central Application Field Application	14, 15, 16, 18
	3	Central Application Field Application	12, 15, 16
	4	Central Application Field Application	1, 2, 3, 4, 5, 13, 18
	6	Central Application Field Application	3, 4
11	All	All	17, 19, 20, 21, 22, 23
	1	Control Authority	6, 7, 8 , 9, 10, 11, 14
	2	Control Authority	14, 15, 16, 18
	3	Control Authority	1, 2, 3, 4, 5, 13, 18
	4	Information Repository	1, 2, 3, 4, 5, 13, 18
	5	Control Authority	6, 7, 8 , 9, 10, 11, 14
	6	Control Authority	14, 15, 16, 18
	7	Control Authority	1, 2, 3, 4, 5, 13, 18
	8	Control Authority	1, 2, 3, 4, 5, 13, 18
	9	Field Application	6, 7, 8 , 9, 10, 11, 14
	10	Field Application	14, 15, 16, 18
	11	Field Application	12, 15, 16
	12	Field Application	1, 2, 3, 4, 5, 13, 18

Use Case	Use Case Step	Role	Failure(s)
	13	Control Authority	1, 2, 3, 4, 5, 13, 18
12	All	All	17, 19, 20, 21, 22, 23
	1	Control Authority	6, 7, 8 , 9, 10, 11, 14
	2	Control Authority	14, 15, 16, 18
	3	Control Authority	1, 2, 3, 4, 5, 13, 18
	4	Information Repository	1, 2, 3, 4, 5, 13, 18
	5	Control Authority	6, 7, 8 , 9, 10, 11, 14
	6	Control Authority	14, 15, 16, 18
	7	Control Authority	1, 2, 3, 4, 5, 13, 18
	8	Control Authority	1, 2, 3, 4, 5, 13, 18
	9	Actuator	6, 7, 8 , 9, 10, 11, 14
	10	Actuator	14, 15, 16, 18
	11	Actuator	12, 15, 16
	12	Actuator	1, 2, 3, 4, 5, 13, 18
	13	Control Authority	1, 2, 3, 4, 5, 13, 18
13	All	All	17, 19, 20, 21, 22, 23
	1A	Central Application	1, 2, 3, 4, 5, 13, 18
	1B	Information Repository	12, 15, 16
	2	Information Repository	6, , 8, 9, 10, 11, 14
	3	Information Repository	14, 15, 16, 18
	4	Information Repository	1, 2, 3, 4, 5, 13, 18
	5	Sensor	6, 7, 8 , 9, 10, 11, 14
	6	Information Repository	1, 2, 3, 4, 5, 13, 18

Use Case	Use Case Step	Role	Failure(s)
	7	Field Application	1, 2, 3, 4, 5, 13, 18 6, 7, 8 , 9, 10, 11, 14
14	All	All	17, 19, 20, 21, 22, 23
	1	External Application	6, 7, 8 , 9, 10, 11, 14, 12, 15, 16
15	All	All	17, 19, 20, 21, 22, 23
	1	External Application	17, 19, 20, 21, 22, 23

Table 2 - DM Failures Mapped against Use Cases and Roles

4 Security Controls

This section presents security controls recommended for DM systems. The controls are divided into three categories: network segmentation, policy, and technical.

- Network segmentation controls (Section 4.1) are based on the types of networks used in a DM system and their relationships.
- Policy controls (Section 4.2) provide guidance to the utility in terms of the policies and procedures they must have in place with respect to security.
- Technical controls (Section 4.3) are those that impact the hardware, software, and environment within which a DM system exists.

The controls in this document are based on information found in the Department of Homeland Security (DHS) Catalog of Control Systems Security, various FIPS standards, and industry best practices. In many cases, controls were derived from existing controls (primarily from controls in the DHS catalog) and customized to a DM setting. These customizations refined the original controls to be more specific and more actionable for the users of this security profile. To provide traceability, controls are mapped to related controls and standards (see that last column in Tables 3, 4, and 6).

The security controls are intended to address potential failures. When selecting and implementing controls, consider both the risks associated with a failure and the cost of implementing a particular control. Power system capabilities contribute to the resilience of the system and may fulfill the function of some of the security controls discussed below.

4.1 Required Network Segmentation

This section describes the types of communication networks used in a DM system and how to segment these networks to improve security. Network segmentation will allow organizations to more closely monitor for and detect inappropriate activity within the DM system and to contain the impact of such activity to a limited portion of the system.

Network types and their segmentation are not specific to any particular role or use case. This section presents a set of requirements for segmenting DM system networks that are based on best practices from a security perspective and that reflect the typical interaction among elements of a DM system. These requirements are listed in Table 3. Figure provides an overview of the network segments discussed in this section.

A DM system is a collection of different network types and segments within those types. Each segment within a network should be protected from unauthorized access by a set of controls at its boundary that are described in the protection controls of Section 4.3. Different sets of controls may be used at different types of boundaries and these controls are used based on the level of protection required for a particular segment. The level of protection required is based on such factors as the role of the hosts within that segment.

The most significant characteristic that distinguishes network types used within a DM system relative to cyber security is that of being either a public network or a private network. Public networks are available to the general public and private networks do not permit public access. Public networks provide no control, ownership, or guarantee of service to a user of that network; further, use of public networks increases the opportunities to attack assets connected to that network to unacceptable levels for a DM system. Private networks are restricted to utility use, provide the opportunity for control, ownership, and creation of service guarantees for the utility, and decrease the attack surface of a DM system. Virtual Private Networks (VPNs) are not an acceptable means of creating a private network for DM system use within a public network space due to potential availability and increased attack surface risks

A DM network is divided into four kinds of network segments.

1. DM Field Network – field deployed devices (i.e., devices implementing the Field Application, Sensor, and Actuator functionality) and supporting network devices are deployed in DM Field Network Segments. A DM implementation may have multiple DM Field Network Segments.
2. DM Control Systems Server Network – any system that directly communicates with and controls field deployed devices or provides centralized critical operational/support functions (i.e., systems implementing Control Authority, Information Repository, or automated Central Application functionality) is deployed in a DM Control Systems Server Network Segment.
3. DM Control Systems User Network – workstations and devices that provide interactive access to Central Applications in the DM Control Systems Server Network (i.e., systems providing a human-machine interface for Central Application functionality) are deployed in DM Control Systems User Network Segments.

4. Non-DM Utility Network– utility systems that provide other enterprise functions (i.e., systems providing External Application functionality), control systems unrelated to DM, and interfaces to control systems owned by other utilities are deployed in Non-DM Utility Network Segments. Example systems include AMI, ERP, CIS, Generation and Transmission management systems, or corporate business systems. This type of network is intended to include all types of utility networks outside of the scope of DM.

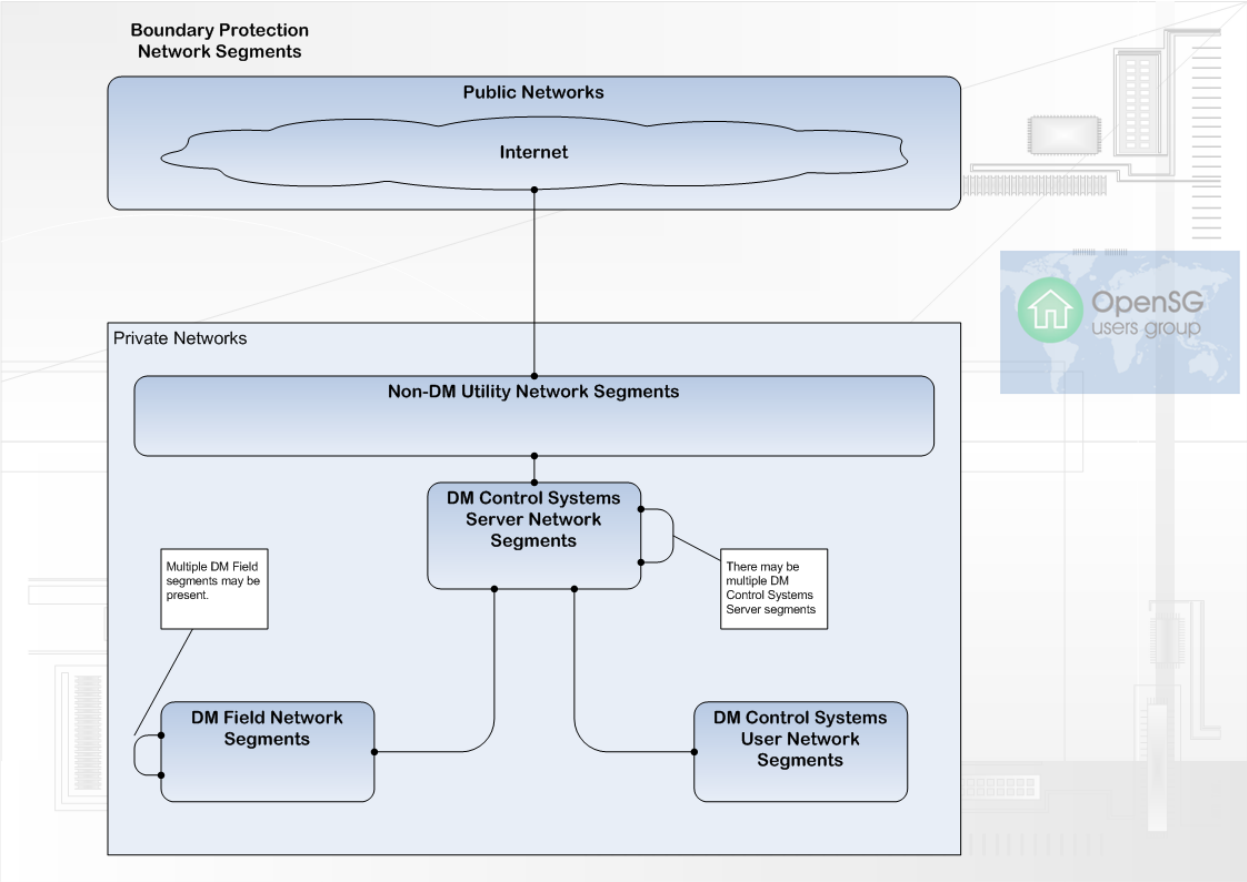

Figure 6 – Network Segments

The connections indicated in Figure shall be the only connections among these network segments. For example, only a Non-DM Utility Network Segment can have a connection to the Internet; any other network segment must go through a Non-DM Utility Network Segment to reach the Internet. Likewise, only DM Control Systems Server Network Segments can communicate with DM Field Network Segments or DM Control Systems User Network Segments. The restriction of communication paths allows access protection mechanisms to exist at the boundary instead of on all of the devices within a particular segment.

A given DM system may include multiple instances of each kind of network segment. For example, a DM system could include several DM Field Network Segments, one for each collection of devices controlled by a particular substation. Segments of the same type can be operated individually. This allows an individual segment to be disconnected in the event of a failure without impacting the workings of the remainder of the DM Field network.

Another use of segments is to inform the placement of applications on servers. For example, the user interface portion of Central Applications may be integrated with the server portion or deployed to separate hosts. If a Central Application provides a choice, deploy the user interface/console in a separate network segment. When allocating system server and workstation networks onto segments, the segments should not span non-contiguous physical security perimeters.

Control ID	Short Name	Definition	DHS Reference(s)
Network.1	DM Networks are Private	No DM network activity shall occur on a public network.	
Network.2	Limited Connection to Public Network	Non-DM utility network segments shall be the only DM network segments allowed to connect to the internet. The DM Control Systems Server Network, the DM Control Systems User Network Segments, and the DM Field Network shall not be connected to the internet.	
Network.3	Limited Connection to Non-DM Utility Network	The DM Field Network and the DM Control Systems User network shall not be connected to the Non-DM Utility Network.	
Network.4	Separation of the Field network from the Control Systems User Network	The DM Field Network shall not be connected to the DM Control Systems User network.	
Network.5	Redundancy	Network paths supporting critical DM elements must be deployed in redundant configurations and be architected in such a way as to avoid single points of failure.	2.8.5
Network.6	Emergency Network Segmentation	If an attack is detected, the organization shall prohibit traffic from compromised DM network segments. This assumes that defensible segments have been previously identified.	

Table 3 - Network Segmentation Security Controls

4.2 Policy Security Controls

This section contains recommendations for policy security controls that if followed will form the basis for an overall DM system security program. The policy security controls presented in Table 4 are the product of best practices and the operational experience of utility and security

professionals working in this domain. They are derived from, but not a copy of or constrained by, the DHS Catalog of Control Systems Security. A cross reference with the related counterparts in the DHS Catalog is shown in the last column of Table 4.

The effectiveness of these policies will be directly related to an organization's diligence in formally documenting the policies described in Table 4 and disseminating them to all personnel with access to or responsibility for the DM system. Regular review and update of the documented policies is critical to keeping them aligned with system architecture, business drivers, technology, and threats.

Control ID	Short Name	Definition	DHS References
Policy.1	Policy – Purpose and Scope	The organization develops and documents a DM system security policy, supporting plans, processes, and procedures that address the purpose and scope of the DM system security program including the following areas:	
		a) The purpose and scope of the security program as it relates to protecting the organization's DM system assets.	2.3.1, 2.4.1, 2.6.1, 2.8.1, 2.9.1, 2.10.1, 2.11.1, 2.12.1, 2.13.1, 2.14.1, 2.15.1, 2.16.1, 2.17.1, 2.19.1
		b) Risk management strategy	2.19.2
		c) Authorization boundary of the DM system	2.7.2, 2.18.5
		d) Industry best practices that influence the DM system security program	2.17.4
Policy.2	Policy - Organizational	The organization develops and documents a DM system security policy, supporting plans, processes, and procedures that address the organizational aspects of the DM system security program including the following areas:	
		a) Executive accountability and authority for the DM system security program	2.2.3, 2.19.2
		b) Management and leadership roles and responsibilities including; 1 approval of security policy, 2 assignments of security roles, 3 coordination, implementation, and accountability of the DM system security program	2.2.2, 2.2.3, 2.4.1, 2.6.1, 2.8.1, 2.9.1, 2.10.1, 2.11.1, 2.12.1, 2.13.1, 2.14.1, 2.15.1, 2.16.1, 2.17.1, 2.18.1
		c) Roles, responsibilities, and identification of the organization's DM security personnel	2.10.1, 2.11.1, 2.11.3, 2.14.5, 2.15.8, 2.18.1
		d) The organization's contracts with external entities that address the	2.2.3, 2.5.9

Control ID	Short Name	Definition	DHS References
		organization's DM system security policies and procedures with business partners, contractors, and outsourcing partners	
		e) Coordination among organizational entities of the DM system security program to ensure compliance with the organization's security policy and other regulatory commitments	2.3.1, 2.4.1, 2.6.1, 2.8.1
		f) Roles and responsibilities for all personnel involved in the organizations DM system incident response process	2.7.4, 2.12.1
		g) Initial and refresher training on the DM incident response process for all personnel involved in the organizations DM system incident response process	2.12.4
		h) Coordination efforts with law enforcement agencies, regulators, Internet service providers and other relevant organizations in the event of a DM system security incident	2.2.4, 2.12.1
		i) Roles, responsibilities, and expected behaviors for all personnel with electronic or physical access to the DM system, information, and documentation - The policy should clearly communicate the terms and conditions for identifying permitted behaviors and practices. Behaviors and practices thatnot covered explicitly in the policy shall require approval by the organizations designated management representative. This includes employees and contractors of the organization as well as external suppliers and partners. Disciplinary actions for failure to comply with the DM system security program policies and procedures shall be included.	2.2.5, 2.3.8, 2.5.9, 2.6.5, 2.7.11, 2.8.19, 2.9.1, 2.11.3, 2.13.1, 2.14.1, 2.15.8
		j) Initial and refresher training on the DM security program for all personnel with electronic or physical access to the DM system	2.7.5, 2.7.11, 2.11.2, 2.11.4, 2.11.6
Policy.3	Policy - System Development, Operation, and Maintenance	The organization develops and documents a DM system security policy, supporting plans, processes, and procedures that address the system development, operation, and	

Control ID	Short Name	Definition	DHS References
		maintenance aspects of the DM system security program including the following areas:	
		a) Certification and recommended accreditation of the DM system and security mechanisms	2.17.5, 2.17.6, 2.18.3
		b) DM system architecture including Internal and external logical boundaries of the DM system - The organization shall document the purpose and business justification for all traffic permitted between DM system network segments and between the DM system and external systems.	2.8.7, 2.18.5, 2.19.7
		c) Communications and data confidentiality, integrity, and availability requirements for the DM system	2.8.8, 2.8.9, 2.8.28, 2.18.5
		d) Acceptable use of wireless technologies within the DM system	2.15.26
		e) Inclusion of cyber security functional requirements in the acquisition of the DM system and supporting components	2.5.4
		f) Upgrades and/or mitigation of associated risks of legacy DM systems and components which do not fully support the DM system security controls	2.10.2
		g) The life-cycle of DM system and security components including long term planning for upgrades, replacements, and remedial actions to correct weaknesses of deficiencies noted during DM system security assessments, vulnerability assessments, and penetration testing	2.5.3, 2.14.13, 2.18.6, 2.19.4
		h) Documentation of the design and operation of the DM system including relationships or connection to other systems	2.5.5, 2.7.2, 2.8.18, 2.14.4
		i) Protection of and access to DM system documentation	2.5.5
		j) User installation of software	2.5.7
		k) Requirements for vendor configuration management - It is recommended that	2.5.10

Control ID	Short Name	Definition	DHS References
		the organization requires that all DM system developers and integrators implement and document a configuration management process that (1) manages and controls changes to the system during design, development, implementation, and operation; (2) tracks security flaws; and (3) includes organizational approval of changes.	
		l) Requirements for vendor security testing - it is recommended that the organization requires the DM system vendor to: 1) develop a security test and evaluation plan, 2) submit the plan to the organization for approval, 3) implement the plan once written approval from the organization is obtained, 4) document the results of the testing and evaluation and submit them to the organization for approval.	2.5.11
		m) Disposal and reuse of DM system components.	2.6.9
		n) Testing of security plans, processes, and procedures including planning of security-related activities and security vulnerability assessment	2.7.6, 2.7.12, 2.10.3, 2.10.6
		o) Cryptographic key use, establishment and management	2.8.11, 2.8.12, 2.8.15
		p) The use of mobile code within the DM system	2.8.16
		q) The use of VOIP protocol within the DM system	2.8.17
		r) The use of name/address resolution service	2.8.21, 2.8.22, 2.8.23
		s) The identification, approval, and monitoring of maintenance tools	2.10.7
		t) Remote maintenance of the DM system	2.10.9
		u) Monitoring DM system security mechanisms including measures of performance	2.18.7, 2.19.6
Policy.4	Policy - Electronic and Physical	The organization develops and documents a DM system security policy, supporting plans,	

Control ID	Short Name	Definition	DHS References
	Access Control	processes, and procedures that address electronic and physical access to the DM system including the following areas:	
		a) Acceptable use policy for the DM system	2.15.17, 2.15.27
		b) Screening individuals requiring and requesting electronic and unescorted physical access to the DM system before access is authorized - Screening criteria should include criminal background check, past 5 years of employment, education with verification of the highest degree received, past 3 years of residency, and references.	2.3.3
		c) Reviewing and approving requests for electronic and/or physical access to the DM system	2.6.5
		d) Identification of all personnel with authorized electronic and/or physical access to the DM system including review and approval by the designated organization official on at least an annual basis	2.4.2
		e) Visitor access to facilities containing DM system assets	2.4.5
		f) Review and documentation of personnel with approved electronic and/or physical access to the DM system	2.3.1
		g) Review and validation or modification of electronic and physical access permissions to the DM system when individuals are reassigned or transferred to other positions within the organization - Access permissions for all individuals shall be relevant to the individual's current role and responsibilities only. Complete execution of this control occurs within 7 days for employees or contractors who no longer require access to the DM system.	2.3.5
		h) Removal of electronic and physical access to the DM system upon termination of employment. Complete execution of this control shall occur within 24 hours for employees or contractors terminated for cause.	2.3.4

Control ID	Short Name	Definition	DHS References
		i) Removal of external supplier access to the DM system at the conclusion or termination of the contract	2.2.6
		j) Creation and maintenance of authentication credentials (including passwords) - Factory default authentication credentials should be changed prior to any component of the DM system being placed in service.	2.6.10, 2.15.4, 2.15.5, 2.15.16
		k) Account review and management - The organization shall on at least an annual basis review access authorizations and remove or modify access privileges when individuals no longer have a valid need.	2.15.3, 2.15.6, 2.15.19, 2.15.20
		l) Access privileges - Authorized access to the DM system shall be limited to only that required to accomplish the process or users assigned task.	2.15.9, 2.15.11
		m) Allowable methods for remote access to the DM system	2.15.23, 2.15.24, 2.15.29
		n) Assignment, protection, operation (including connection to the DM system), and physical location of DM system components and portable media which are not permanently installed (e.g. laptop computers, test sets, mobile media, and other mobile devices)	2.4.16, 2.4.17, 2.4.19, 2.6.9, 2.15.25
Policy.5	Policy – Security Assessments	The organization develops and documents a DM system security policy, supporting plans, processes, and procedures that address security assessment of the DM system including the following areas:	
		a) Risk assessment development, execution, and updates	2.18.1, 2.18.9, 2.18.10, 2.18.2, 2.19.11
		b) Vulnerability assessment	2.8.11, 2.18.2
Policy.6	Policy – Incident Handling, Response, Analysis, and Disaster Recovery	The organization develops and documents a DM system security policy, supporting plans, processes, and procedures that address the incident handling, response, analysis, and disaster recovery of the DM system including the following areas:	

Control ID	Short Name	Definition	DHS References
		a) Development of a documented incident handling and response process including identification and classification of potential interruptions which trigger the process	2.7.3, 2.12.1, 2.12.7, 2.12.8, 2.12.10
		b) Dissemination of security alerts and advisories	2.14.5
		c) Creation, handling, and storage of backups of critical system software, applications, and data for use if the control system operating system software becomes corrupted or destroyed - All DM system backups shall be stored in a secure off-site facility. Integrity of the backups shall be tested on at least an annual basis.	2.10.4, 2.12.13, 2.12.16
		d) Incident investigation, analysis, reporting and corrective action	2.7.7, 2.7.8, 2.12.8, 2.12.9, 2.12.11, 2.12.12
		e) Establishment, maintenance, and activation of alternate control center and telecommunication facilities	2.4.15, 2.12.15
		f) Alternate command/control methods when primary DM system capabilities are unavailable	2.12.14
		g) DM system recovery and reconstitution after disruption, compromise, or failure	2.12.17
		h) Response to unauthorized electronic and physical access to the DM system	2.4.4, 2.4.21
		i) Response to activation of fire detection systems in facilities containing DM system assets	2.4.11
		j) Response to DM system alarms indicating warnings, failures, or abnormal conditions within the DM system	2.4.12
		k) Response to unauthorized changes to the DM system configuration	2.6.4
Policy.7	Policy – Configuration and Change Management	The organization develops and documents a DM system security policy, supporting plans, processes, and procedures that address configuration and change management of the DM system including the following areas:	

Control ID	Short Name	Definition	DHS References
		a) Development of a documented configuration management process	2.6.11, 2.14.2, 2.14.8
		b) Development, documentation, and maintenance of a current baseline configuration of the DM system and components - Configurations of the various components should provide for only essential capabilities essential to operation of the DM system and security settings within these components should be defined in the most restrictive mode that does not adversely impact operation DM system.	2.6.2, 2.6.6, 2.6.7
		c) Maintaining an inventory of DM system assets and information	2.6.8, 2.6.9, 2.19.5
		d) Impact analysis of all proposed changes to the DM system	2.6.4, 2.10.5
		e) Authorization and documentation of changes, maintenance, and repair to the DM system - The organization shall document each scheduled change to the DM system or its components. At a minimum, this documentation shall include; 1) date and time of proposed change, 2) individual or organization requesting change, 3) detailed description of the change, and 4) approval of the change. Unscheduled changes or repairs to the DM system shall be reviewed on a daily basis for possible impact to other DM system functions and scheduled changes. Furthermore, the organization shall be capable of determining the status of all changes (e.g. planned, in progress, complete) at all times.	2.6.3, 2.10.5, 2.10.6, 2.10.8
Policy.8	Policy – Information, Media, and Document Management	The organization develops and documents a DM system security policy, supporting plans, processes, and procedures that address information, media, and document management aspects of the DM system security program including the following areas:	
		a) Managing control system-related data for both electronic and paper data and access to the data based on formally assigned roles and responsibilities or contractual and confidentiality	2.9.2, 2.9.3, 2.9.5, 2.9.6, 2.9.7, 2.13.2, 2.14.12, 2.18.8

Control ID	Short Name	Definition	DHS References
		agreements with external parties	
		b) Classification of information and documentation to indicate the protection required commensurate with its sensitivity and consequence	2.9.4, 2.9.6, 2.9.10, 2.9.11, 2.13.3, 2.13.4
		c) Destruction of written and electronic data	2.9.8
		d) Media storage, handling, sanitation, and disposal	2.13.5, 2.13.6, 2.13.7
Policy.9	Policy – Auditing and Reporting	The organization develops and documents a DM system security policy, supporting plans, processes, and procedures that address auditing and reporting aspects of the DM system security program including the following areas:	
		a) Identification of auditable events	2.16.2
		b) Audit monitoring, tools, analysis, and reporting	2.16.6, 2.16.11, 2.16.13, 1.16.14
		c) Establishment, monitoring, and analysis of security metrics	2.7.9
		d) Reviewing logs for electronic and physical access to the DM system on at least an annual basis	2.4.4, 2.6.5
		e) Long term retention, media, and format of all logs and records related to access to and operation of the DM system	2.4.6, 2.4.7, 2.6.3, 2.16.10
Policy.10	Policy - Review and Update	The organization annually reviews and revises if necessary the DM system security policy, supporting plans, processes, and procedures.	2.3.1, 2.4.1, 2.6.1, 2.7.2, 2.7.10, 2.8.1, 2.9.3, 2.17.2, 2.17.3, 2.17.1, 2.18.4

Table 4 - Policy Security Controls

4.3 Technical Security Controls

This section contains recommendations for technical security controls that if followed will improve the security of a distribution management system. These controls are derived from, but not a copy of or constrained by, the DHS Catalog of Control Systems Security and are the product of best practices and the operational experience of utility and security professionals working in this domain.

Each technical security control is categorized as primarily belonging to one of five categories inspired by the CISSP Common Body of Knowledge. These categories, defined along with examples in Table 5, are deterrence, protection, detection, reaction, and recovery. Though no deterrence controls are presented, the category is included for completeness. Deterrence controls are largely implemented by establishing clear legal recourse, which is out of scope for this security profile.

Category	Description	Castle Example	Modern/IT Example
Deterrence	Discouraging someone from engaging in an attack	Build an impressive looking castle; fly colors on a lot of guards and patrols; spread rumors that anyone opposing the King will be killed	Appropriate use banners; highly visible uniformed guards; penalty descriptions
Protection	Active measures used in normal circumstances that are designed to prevent an attack	Build thick castle walls; build a wide moat; build a drawbridge; wear armor; maintain stock of supplies	Access control mechanisms; message encryption; disabling unneeded ports/services
Detection	Identifying an attack or weakness	Patrol the kingdom; post guards on the castle walls and in the courtyard; have the court jester taste the King's food	Signature checking; anti-virus scanning; configuration validation; pre-deployment tests; log auditing
Reaction	Stopping an active attack using measures not normally implemented	Pour boiling oil into the gatehouse; fire arrows and catapults; engage in swordfight	Adjustable log granularity; network isolation; manual override
Recovery	Restoring to normal operations after an attack has been stopped	Clean the gatehouse and courtyard; bury the dead from battle; repair walls; restock arrows and projectiles	Debriefing and post-mortem analysis; system re-configuration; policy changes

Table 5 - Categories of Technical Security Controls

Each technical control, though simply expressed, has implications to different stakeholders and lifecycle phases—specifically from development, configuration, and operational perspectives. Though any given control may be written from one perspective, such as operational, its implications to other perspectives should not be overlooked. Procurement language, for example, should be written to ensure that development activities produce a system able to support configuration and operational requirements.

More concretely, the Detection.1 control requires that physical access to facilities be monitored and logged at all times. From an operational perspective, this speaks to the activities of performing logging and monitoring the logs. From a configuration perspective, this implies a need to setup systems such that logs are accessible to the personnel that will be monitoring them. From a development perspective, this implies a need for systems to be built in such a way that logs can be electronically generated, stored, and potentially shared or distributed.

The process for selecting recommended technical security controls is based on an analysis of the roles, use cases, and failures defined in this profile along with careful examination of the DHS

Catalog of Control Systems Security and other collections of security standards and best practices. The process looked something like the following (with natural iteration and review):

1. Examine reference material, looking for ideas that should be included in a recommended technical security control. Included controls should address one or more identified failures that are required by at least one role in the profile.
2. Customize the reference material, frequently by writing a new control. For example, many controls in the DHS catalog are complex, addressing several points and fitting in several categories; such controls were typically broken up. Additionally, most controls were made more specific. Each control includes references to the source material that inspired it.
3. Explicitly document the applicability of each control (to which roles), the justification for its inclusion (which failure it most directly mitigates), and the category to which it belongs.
4. Cluster the controls by category to facilitate examination for overlap and gaps. In some cases multiple controls were combined into a single, simpler control. In other cases, a gap was identified and a new control was drafted. Gaps were also identified through a cross-check to ensure that all failures were addressed by at least one technical control.

The results of this process are documented in Table 6 and Table 7. Table 6 defines the technical controls themselves. It includes

- Control ID: This ID is composed of the control's category and a sequence number within that category.
- Short Name: This is a short string that summarizes the intent of the control in a unique string.
- Definition: This is the text that defines the control itself.
- Reference(s): This is the list of outside controls or standards on which a control is (to some extent) based. Most references are to controls in the DHS Catalog of Control Systems Security.

Technical Security Controls for Distribution Management Security

Control ID	Short Name	Definition	Reference(s)
Detection.1	Facility Access Monitoring/Logging	Physical access to facilities (such as control centers, data centers, and substation control buildings) containing DM system cyber components shall be monitored and logged at all times.	DHS 2.4.4
Detection.2	Cabinet Access Monitoring/Logging	Physical access to cabinets and/or enclosures containing DM system cyber components shall be monitored and logged at all times. Mechanisms utilized to monitor entry to cabinets shall be capable of	DHS 2.4.21

Control ID	Short Name	Definition	Reference(s)
		operating in the event of a local power outage.	
Detection.3	Electronic Log Format	All physical access logs should be retained in electronic form suitable for long term storage and retrieval.	DHS 2.4.8
Detection.4	Power Source Monitoring/Logging	The state of the primary and alternate power sources for all critical control system components shall be monitored at all times, and all interruptions of these power sources shall be logged.	DHS 2.4.9
Detection.5	Location of Mobile Components	DM system cyber components which are not permanently installed (such as applications loaded on laptop computers or other mobile devices) shall be tracked and monitored. Current location of these mobile devices shall be electronically available at all times.	DHS 2.4.17
Detection.6	Fire Detection	Fire detection devices/systems shall be deployed in all facilities housing centralized assets. 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.	DHS 2.4.11
Detection.7	DM Systems Inventory	An inventory of DM systems and devices shall be maintained which includes information that uniquely identifies each component, such as manufacturer, type, serial number, version number, and location.	DHS 2.6.2
Detection.8	Baseline Configuration	A baseline configuration shall be established for each DM system or device including the approved software/firmware installed, currently approved patch levels, and configuration settings.	DHS 2.6.2
Detection.9	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.	DHS 2.6.4, 2.6.6
Detection.10	Current Configuration	A designated system or systems shall daily or on request obtain current version numbers, installation date, configuration settings, and patch levels on all elements of a DM system, compare these with inventory and configuration databases, and log all discrepancies.	DHS 2.6.4, 2.6.6

Control ID	Short Name	Definition	Reference(s)
Detection.11	Communication Integrity	The <role> employs a standard integrity-protection mechanism on all transmissions to facilitate detection of unauthorized modification of information. Latency induced from the use of hashing or signature mechanisms must not degrade the operational performance of the <role>.	DHS 2.8.8
Detection.12	System/Device Deficiency	Annually identify DM system/devices, including legacy devices that fail to meet the organization's security requirements.	DHS 2.10.2
Detection.13	System Assessment	Conduct vulnerability assessments and penetration tests on at least an annual basis and after any significant infrastructure or application change.	DHS 2.10.3
Detection.14	Remote Access Monitoring/Logging	Monitor and log all remote interactive sessions to all DM system components including all administrative and maintenance activities.	DHS 2.10.9
Detection.15	Testing Updates	Updates to firmware and software systems must be tested and scanned for malicious code prior to deployment for effectiveness and potential side effects in a standalone environment that is as close as possible to the actual architecture and components.	DHS 2.14.2
Detection.16	Integrity Check	There shall be maintained 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 30 days. Acceptable technologies shall be specified by FIPS 186.	DHS 2.14.3, 2.14.7
Detection.17	Firmware/Configuration Authenticity	Firmware or configuration file downloads to field devices shall have cryptographically signed message payloads. Firmware and configuration files shall not be accepted if not properly signed. Acceptable technologies shall be specified by FIPS 186.	DHS 2.14.3
Detection.18	End Point Security	End point security mechanisms shall be used to detect and eradicate malicious code.	DHS 2.14.3

Control ID	Short Name	Definition	Reference(s)
		Application white listing is another viable means of protecting against malware.	
Detection.19	Intrusion Detection	The organization shall run an intrusion detection system that detects anomalous events. Sources of anomalous events can be the network or data logs. Such systems have false positives so the alarms generated by the intrusion detection systems shall be screened by an experienced person to determine its validity prior to any responsive action being taken.	DHS 2.14.4, 2.8.26
Detection.20	Configuration File Integrity	Configuration files should include standard integrity protection techniques (for software, usually digital signatures)and the integrity of the file should be checked whenever it is read by an application.	DHS 2.14.7
Detection.21	Manual Input Checking	The control system employs mechanisms to check manual input for accuracy, completeness, validity, and authenticity.	DHS 2.14.10
Detection.22	Message Delay Detection	All messages should be time stamped and the recipient should verify that the message arrived within a time window to meet its design or process requirements. Anomalous delays shall be logged and reported.	DHS 2.14.11
Detection.23	Device Self Test	Failures of field applications, sensors, or actuators should be detected through the use of built-in self-tests in the applications, sensors, and actuators. Tests shall include calibration parameters of the device and must be executed on startup or on demand and the results reported and logged.	DHS 2.14.11
Detection.24	Heartbeat	The system scans or validates the current communications state (including proper response) of all devices and applications on a daily basis.	
Detection.25	Automated Account Management	The organization shall employ automated mechanisms for account management including creating an audit trail of account creation, modification, disabling, and termination.	DHS 2.15.3
Detection.26	Identifier Management	The organization shall assign unique identifiers for individuals and devices utilizing unique identifiers (e.g. MAC, IP address)	DHS 2.15.4

Control ID	Short Name	Definition	Reference(s)
Detection.27	Inappropriate User Activity	The organization shall monitor for inappropriate user activity and reviews and analyzes system audit records using automated mechanisms for indications of inappropriate or unusual activity on at least a monthly basis.	DHS 2.15.6, 2.15.3
Detection.28	Previous Logon Notification	The control system notifies the user, upon successful logon, of the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.	DHS 2.15.19
Detection.29	IDS Architecture	Place IDS/IPS devices and DM protocol-aware application firewalls between network segments to monitor and alert for malicious traffic passing between DM network segments.	DHS 2.8.7, 2.8.5
Detection.30	Physical Access Indications	All events relating to physical access to DM system cyber components shall be immediately visible to utility operations personnel (e.g. system operator).	DHS 2.4.21
Detection.31	Sufficient Error Message Content	Error messages shall provide information necessary for corrective action	DHS 2.14.11
Detection.32	Message Validation	Message recipients must validate application protocol fields[3] for logical and expected values including source, destination, time stamps, and state indicators.	
Protection.1	Physical Access Authentication	A minimum of two factor authentication shall be employed for unescorted physical access to facilities containing DM components wherever technically feasible.	DHS 2.4.2, 2.4.3
Protection.2	Limited Control Center Access	Physical access to general user DM system cyber components located within control center facilities should be limited to only those necessary for user input and output (such as workstations, display boards, and printers). Physical access to all other DM system cyber components (such as servers hosting applications and information repositories) should be limited within the control center facility. This can be accomplished by segregating these components within a room internal to the control center facility, the use of lockable enclosures or cabinets, or other similar	DHS 2.4.3, 2.8.18

[3] This control is implemented at OSI layer 4 and above.

Control ID	Short Name	Definition	Reference(s)
		mechanism.	
Protection.3	Limited Field Component Access	Physical access to all field DM system cyber components shall be controlled at all times. This shall be accomplished by the installation of the component with a lockable cabinet. The mechanism utilized for physical access to the cabinet shall provide unique credentials per user which shall be authorized on a per cabinet basis. Periodic re-authorization shall be required which will automatically expire by default if no re-authorized is performed. This would preclude the use of a standard mechanical lock and key mechanism.	DHS 2.4.21, 2.8.18
Protection.4	Emergency Power Shutoff	Emergency power shutoff capability shall be protected from unauthorized activation within facilities containing concentrations of DM system cyber components such as control center and data center facilities.	DHS 2.4.8
Protection.5	Power Sources and Cables	Power sources and power cables for DM system cyber components should be physically protected from damage or unauthorized manipulation.	DHS 2.4.20
Protection.6	Component Location	DM system cyber components should be located as to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	DHS 2.4.20, 2.8.18
Protection.7	Control Center Location	Primary and alternate control center facilities should be geographically dispersed to the extent that a single natural or manmade disaster should not be expected to adversely affect both sites.	DHS 2.4.15
Protection.8	EMI/Surge Protection	DM system cyber components located within, on, or nearby power distribution equipment or facilities shall be resistant to EMI and heavy electrical surges that can be expected within an electrical substation or electrical distribution feeder circuit. Purchasing equipment that meets IEEE 1613 or IEC 61850-3 specifications will satisfy this requirement.	
Protection.9	Factory Default Credentials	All factory default identification and authentication credentials on DM components and applications shall be changed upon installation.	DHS 2.6.10
Protection.10	Management/Configuration	The management/configuration port or	DHS 2.8.2,

Control ID	Short Name	Definition	Reference(s)
	Isolation	function for <role> shall be physically (air-gapped network) or logically (separate VLAN not routed to other networks) separated from non-management/configuration data. Management and configuration will also use separate authentication credentials from the credentials used by <role>.	2.8.3, 2.8.4
Protection.11	Security Function Isolation	Security devices and functionality (devices implementing security controls) will be physically (air-gapped network) or logically (such as securely tunneled) separated from the data and functionality of the <role>. Security devices and functionality can exist on management networks however the authentication for these devices and functionality will use separate multi-factor credentials.	DHS 2.8.2, 2.8.3, 2.8.4
Protection.12	Quality of Service	Network links between <role> and <role> will use Quality of Service, or similar resource reservation control mechanisms. These control mechanisms will ensure that lower-level functions, such as system health or diagnostics, do not overwhelm higher-priority functions such as command and control.	DHS 2.8.6
Protection.13	Communication Confidentiality	1. The <role> employs FIPS 140-2 compliant cryptographic mechanisms to prevent unauthorized disclosure of sensitive information during transmission. Sensitive information will be classified by an organization in accordance with DHS control 2.9.4 (information classification) and 2.9.11 (automated labeling). 2. Latency induced from the use of cryptographic mechanisms must not degrade the operational performance of the <role>.	DHS 2.8.9, 2.9.4, 2.9.11
Protection.14	Remote Interactive Sessions	All remote user-interactive sessions to field deployed devices shall be encrypted using FIPS 140-2 compliant mechanisms, including all administrative and maintenance activities.	DHS 2.10.9
Protection.15	Cryptographic Keys	When cryptography is required, and employed within the distribution management system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting backup procedures. A formal	DHS 2.8.11, 2.8.9, 2.8.8

Control ID	Short Name	Definition	Reference(s)
		written policy shall be developed to document the practices and procedures relating to cryptographic key establishment and management.	
Protection.16	Least Privilege	Users, process and service integrations such as connections to a database, and all other active elements in a system shall follow the principle of least privilege. Each process or service within a system will be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks.	2.8.19, DOD-5200.28-STD
Protection.17	Communication Integrity	A cryptographically strong digital signature mechanism shall be used to verify the validity/identity of a command in conformance with IEC 62351 and FIPS-186.	DHS 2.8.20
Protection.18	Addressing	DNS services shall not be deployed in a control system environment. Addressing shall be performed using static IP and/or host tables. In some circumstances, centralized DNS can be appropriate for a control system environment. If DNS services are implemented, use at least two authoritative DNS servers on different network subnets.	DHS 2.8.21
Protection.19	Fail in Known State	Devices and applications shall fail to a known state that meets the system requirements set by the organization for safety and security.	DHS 2.8.24
Protection.20	Startup in Known State	Devices and applications shall start up in a known state that is safe and/or secure (e.g., device attestation) in accordance with system requirements set by the organization.	
Protection.21	Automated Labeling	The control system automatically labels information in storage, in process, and in transmission based on its classification and the binding between the label and information is maintained as the information moves throughout the system. Information classification should be based on: 1. Access control requirements 2. Special dissemination, handling, or distribution requirements 3. System security policy requirements	DHS 2.9.11, 2.9.4

Control ID	Short Name	Definition	Reference(s)
Protection.22	Mobile Code	Mobile/active code technologies such as JavaScript, ActiveX, Flash, Java Applets, etc. may only be executed on or accepted from components deployed on DM Control Systems Server or User Networks.	DHS 2.8.16
Protection.23	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.	DHS 2.6.7
Protection.24	No Internet Access	No internet or e-mail access shall be allowed from a system implementing DM. No access to the internet on a DM system, even if through a proxy or through a firewall.	DHS 2.14.3
Protection.25	Minimal Error Message Content	Error messages shall not reveal potentially harmful (e.g., exploitable) information	DHS 2.14.11
Protection.26	Account Management	The organization shall manage system accounts (including central and field devices) by identifying authorized users, providing role-based access, and promptly deactivating inactive and terminated users.	DHS 2.15.3
Protection.27	Authenticator Management	The organization shall manage system authenticators for devices and users by verifying the identity of the user/device receiving the authenticator, reviewing the strength of authenticator mechanism for the intended use, establishing lifetime restrictions and reuse conditions for authenticators, and establishing means for users and devices to safeguard authenticators (certificates, passwords, and/or physical tokens).	DHS 2.15.5
Protection.28	Authenticator Distribution	The organization shall employ a secure mechanism to remotely distribute authenticators (certificates, passwords, and/or physical tokens).	DHS 2.15.5
Protection.29	Access Enforcement	The organization shall enforce access	DHS 2.15.7

Control ID	Short Name	Definition	Reference(s)
		control policies for users and devices based on identity, role, and attributes, utilizing mechanisms like access control lists and cryptography.	
Protection.30	Logical Access Authentication	A minimum of two-factor authentication is required for logical access to all critical DM components.	DHS 2.15.7
Protection.31	User Identification and Authentication	Acceptable methods of multi-factor authentication for users are a combination of two or more independent types of authentication -- what you know (passwords), what you have (physical security tokens), and what you are (biometrics) -- for local, network, and remote access.	DHS 2.15.10
Protection.32	Device Identification and Authentication	The organization shall employ cryptographic-based bi-directional identification and authentication (e.g. TLS) for device to device communication.	DHS 2.15.12
Protection.33	Authenticator Feedback	The organization shall obscure the feedback of authentication information during the authentication process.	DHS 2.15.13
Protection.34	Cryptographic Module Authentication	The DM system components shall employ cryptographic module authentication for authenticating users and devices.	DHS 2.15.14
Protection.35	Information Flow Enforcement	The organization enforces the flow of information within the DM system based on applicable policy. Organizations shall place software or hardware firewalls at designated network segment boundaries that serve as choke points for filtering information across field and central devices.	DHS 2.15.15
Protection.36	Password Management	The system provides the necessary capabilities to enforce the use of strong passwords, in accordance with FIPS 112, and to protect passwords from potential exposure. This includes: 1. Ensuring that passwords never cross component boundaries in the clear. 2. Ensuring that all stored passwords are encrypted in accordance with FIPS 140-2 or hashed using 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	DHS 2.15.16

Control ID	Short Name	Definition	Reference(s)
		tools, source code, scripts, aliases, or shortcuts. 4. Supporting the enforcement of password complexity policies (minimum and maximum length, combination of lower/upper case, numerals, and special characters). 5. Providing the ability to expire passwords at defined intervals and minimize reuse 6. Protecting the password store from unauthorized modification. 7. Changing default passwords	
Protection.37	Concurrent Session Management	The use of concurrent sessions for any user, device, or application shall be limited to the minimum necessary for proper operation of the DM system.	DHS 2.15.18
Protection.38	Session Lock	The system shall: 1. Prevent further user access to the system by initiating a session lock after an organization-defined time period of inactivity or upon receiving a request from a user 2. Retain the session lock until the user reestablishes access using appropriate identification and authentication procedures. 3. Provide capability of limiting session lockouts for critical systems requiring immediate access in emergency conditions.	DHS 2.15.21
Protection.39	Remote Session Termination	The system terminates a network connection at the end of a session or after an organization-defined time period of inactivity.	DHS 2.15.22
Protection.40	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 maintenance functions. The system prevents the automated execution of code located on portable media.	DHS 2.15.25
Protection.41	Wireless Encryption	All wireless communications shall use a FIPS certified method of link-layer encryption in addition to any encryption already required by other controls.	DHS 2.25.26
Protection.42	Public Network Restriction	No DM system shall connect to or pass	DHS 2.8.7,

Control ID	Short Name	Definition	Reference(s)
		data through any Public Network. DM functionality may only be communicated through Private Networks.	2.8.5
Protection.43	WAN Communication Outage	DM field systems must be able to carry out all critical/essential functionality without any connection beyond its local network. (For example, a field segment should be able to carry out normal functionality if communications to the DM Control Systems Server segment is lost.)	DHS 2.8.7, 2.8.5
Protection.44	Traffic Control and Filtering	Control and filter all traffic passing between network segments using “deny unless specifically permitted” policies. Restrict permit rules to the smallest number of endpoints, workstations, devices, and services possible.	DHS 2.8.7, 2.8.5
Protection.45	Non-adjacent Network Restrictions	Prohibit all direct communication (without additional, appropriate security controls) between devices/systems in non-adjacent network segments.	DHS 2.8.7, 2.8.5
Protection.46	Internet and e-mail Restrictions	No system, workstation, or device in any DM network should have access to the Internet. This includes workstations in the DM Control Systems User Network. Utility employees whose primary workstations are in these Internet-restricted network segments should be provided secondary non-DM accessible systems for Internet and email access.	DHS 2.8.7, 2.8.5
Protection.47	Centralized Authentication	Authentication servers for the DM systems shall be separate from authentication servers used for corporate and business systems. The DM authentication system should be placed in the DM Control System Server Network and should not have any trust relationships with other non-DM centralized authentication systems.	DHS 2.8.7, 2.8.5
Protection.48	Secure Coding Practices	DM software components shall be developed in accordance with secure coding standards (e.g., the CERT C secure coding standard) or avoidance of cataloged coding flaws and weaknesses (e.g., the NIST SAMATE Reference Dataset or the MITRE Common Weakness Enumeration). Compliance can be demonstrated through code inspections or use of static analysis tools.	DHS 2.8.5, 2.5.8
Protection.49	Message Identities	Every message shall include the identity of	

Control ID	Short Name	Definition	Reference(s)
		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. Data link layer (layer 2) and/or Network layer (layer 3) addressing is not sufficient by itself to meet the requirement of this control.	
Protection.50	Data Point State Indicators	Every message containing data about the state of the system (e.g., sensor or field application data) shall include a time stamp and state indicator (e.g., DNP3 quality flag) for each data point.	
Protection.51	No Shared Accounts	Additionally, each account within a system must be tied to an individual (no shared accounts) for proper auditing, management, and tracking. Where ever possible, SuperUser accounts, Administrator or Root, should be disabled and/or removed.	DHS 2.8.19 DOD-5200.28-STD
Protection.52	Application Layer Security	Device applications, within operating systems like Windows and Linux, shall provide application layer security in addition to the inherent protections offered by the device's operating system.	DHS 2.8.19 DOD-5200.28-STD
Protection.53	Separate Keys for Separate Functions	Field devices will use separate encryption keys based on functionality. For example, the key used for performing volt/VAR reads from a field device will be different than the key used for firmware updates.	DHS 2.8.19 DOD-5200.28-STD
Reaction.1	Access Revocation - Central	Revocation of access credentials for all control and data center facilities shall be carried out within 24 hours of the revocation approval.	DHS 2.4.2, 2.4.3
Reaction.2	Access Revocation - Field	Revocation of access credentials for all substation and outdoor cabinets shall be carried out within 7 days of the revocation approval.	DHS 2.4.2, 2.4.3
Reaction.3	Physical Access Correlation	Physical access events which cannot be correlated to approved access shall be immediately evaluated for potential risk to the power system and corrective action taken in a time frame appropriate to the posed risk.	DHS 2.4.21
Reaction.4	Unscheduled or Unapproved Activity	Any unscheduled or unapproved activity detected within the DM system shall be immediately evaluated for potential risk to	DHS 2.15.6

Control ID	Short Name	Definition	Reference(s)
		the power system and corrective action taken in a time frame appropriate to the posed risk.	
Reaction.5	Emergency Access	In the event of emergency the organization shall be able to provide audited, controlled, manual override of automated access control mechanisms.	DHS 2.15.7, 2.15.11
Reaction.6	Unsuccessful Access Attempts	The system: 1. Enforces a limit of an organization-defined number of consecutive invalid access attempts by a user during an organization-defined time period 2. Automatically locks the account/node for an organization-defined time period and delays the next login prompt according to an organization-defined delay algorithm or until released by an administrator when the maximum number of unsuccessful attempts is exceeded.	DHS 2.15.20
Reaction.7	End Point Isolation	If a compromised device is detected, it shall be isolated from the rest of the DM system to prevent further compromise and minimize system impact.	
Recovery.1	Alternate Power Source	A long-term alternate power supply for the critical DM system cyber components located at primary and alternate control facilities shall be provided that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.	DHS 2.4.9
Recovery.2	Backup Power Requirement	DM system cyber components essential for system restoration shall be capable of operating for a minimum of 1 hour upon loss of primary power source. This requirement can be met by the use of a UPS, battery backup, or alternate power source	DHS 2.4.9
Recovery.3	Operations Continuity	The DM system shall be architected in such as way as the loss of the primary control facility or critical DM system elements shall not prevent the functionality or operability of the DM system.	DHS 2.4.15
Recovery 4	Rebuild System	The organization shall be capable of rebuilding the system from the securely maintained images of the DM components in the event of compromised device or network.	DHS 2.12.17

Table 6 - Technical Security Controls

Table 7 maps each technical security control against the failures it addresses and the roles that are required to implement it. The table includes:

- Control ID and Short Name: These are references to the control as defined in Table 6. The short name is included as reminder of the general intent of the control.
- Failure(s): This is a list of the failures from Table 1 that the control addresses. Failures included in this list are those most directly addressed by the control. Mitigation of a failure can often indirectly address several other failures, but such secondary effects are not listed.

  For example, mitigating failure 21 (<Role> is physically accessed by unauthorized personnel) could indirectly mitigate failures such as failure 11 (<Role> does not respond to a message in a timely fashion) for cases where the unauthorized physical access took <Role> offline.
- Roles: The remaining columns list the roles from Section 2.1. An "X" in a role's column indicates that that role must implement the security control.

Control ID	Short Name	Failures	Actuator	Sensor	Field Application	Information Repository	Control Authority	Central Application	External Application
Detection.1	Facility Access Monitoring/Logging	21	X	X	X	X	X	X	X
Detection.2	Cabinet Access Monitoring/Logging	21	X	X	X				
Detection.3	Electronic Log Format	21	X	X	X	X	X	X	X
Detection.4	Power Source Monitoring/Logging	19	X	X	X	X	X	X	X
Detection.5	Location of Mobile Components	13, 20			X				
Detection.6	Fire Detection	22				X	X	X	X
Detection.7	DM Systems Inventory	20	X	X	X	X	X	X	
Detection.8	Baseline Configuration	20	X	X	X	X	X	X	X
Detection.9	Self Identification	20	X	X	X	X	X	X	
Detection.10	Current Configuration	20			X			X	
Detection.11	Communication Integrity	13	X	X	X	X	X	X	X
Detection.12	System/Device Deficiency	20	X	X	X	X	X	X	X
Detection.13	System Assessment	13, 20	X	X	X	X	X	X	X
Detection.14	Remote Access Monitoring/Logging	13	X	X	X	X	X	X	
Detection.15	Testing Updates	20	X	X	X	X	X	X	
Detection.16	Integrity Check	20	X	X	X	X	X	X	
Detection.17	Firmware/Configuration Authenticity	18, 20	X	X	X				

Control ID	Short Name	Failures	Actuator	Sensor	Field Application	Information Repository	Control Authority	Central Application	External Application
Detection.19	Intrusion Detection	13, 16, 14, 15	X	X	X	X	X	X	
Detection.20	Configuration File Integrity	20	X	X	X	X	X	X	
Detection.21	Manual Input Checking	2, 7, 8, 9			X	X	X	X	X
Detection.22	Message Delay Detection	10, 12	X	X	X	X	X	X	
Detection.23	Device Self Test	19	X	X	X				
Detection.24	Heartbeat	19	X	X	X	X	X	X	
Detection.25	Automated Account Management	13			X	X	X	X	X
Detection.26	Identifier Management	13	X	X	X	X	X	X	X
Detection.27	Inappropriate User Activity	13			X	X	X	X	X
Detection.28	Previous Logon Notification	13			X			X	
Detection.29	IDS Architecture	13			X	X	X	X	X
Detection.30	Physical Access Indications	21	X	X	X	X	X	X	X
Detection.31	Sufficient Error Message Content	3, 4, 5	X	X	X	X	X	X	
Detection 32	Message Validation	8, 9, 10	X	X	X	X	X	X	X
Protection.1	Physical Access Authentication	21			X	X	X	X	X
Protection.2	Limited Control Center Access	21				X	X	X	X
Protection.3	Limited Field Component Access	21	X	X	X				
Protection.4	Emergency Power Shutoff	21				X	X	X	X

Control ID	Short Name	Failures	Actuator	Sensor	Field Application	Information Repository	Control Authority	Central Application	External Application
Protection.5	Power Sources and Cables	21	X	X	X	X	X	X	X
Protection.6	Component Location	21	X	X	X	X	X	X	X
Protection.7	Control Center Location	22				X	X	X	X
Protection.8	EMI/Surge Protection	22	X	X	X				
Protection.9	Factory Default Credentials	13, 20	X	X	X	X	X	X	
Protection.10	Management/Configuration Isolation	20	X	X	X	X	X	X	X
Protection.11	Security Function Isolation	20	X	X	X	X	X	X	X
Protection.12	Quality of Service	20	X	X	X	X	X	X	X
Protection.13	Communication Confidentiality	13	X	X	X	X	X	X	X
Protection.14	Remote Interactive Sessions	13	X	X	X				
Protection.15	Cryptographic Keys	13	X	X	X	X	X	X	X
Protection.16	Least Privilege	13	X	X	X	X	X	X	X
Protection.17	Communication Integrity	2, 7						X	X
Protection.18	Addressing	2, 7	X	X	X	X	X	X	X
Protection.19	Fail in Known State	17	x	x	X	X	X	X	X
Protection.20	Startup in Known State	17	x	x	x	x	X	x	x
Protection.21	Automated Labeling	13	X	X	X	X	X	X	X
Protection.22	Mobile Code	13	X	X	x	X	X	X	X
Protection.23	Disabling Unnecessary Communication Services	13	X	X	X	X	X	X	
Protection.24	No Internet Access	13			X	X	X	X	

Control ID	Short Name	Failures	Actuator	Sensor	Field Application	Information Repository	Control Authority	Central Application	External Application
Protection.25	Minimal Error Message Content	13	X	X	X	X	X	X	
Protection.26	Account Management	13			X	X	X	X	X
Protection.27	Authenticator Management	13			X	X	X	X	X
Protection.28	Authenticator Distribution	13			X	X	X	X	X
Protection.29	Access Enforcement	13			X	X	X	X	X
Protection.30	Logical Access Authentication	13			X	X	X	X	X
Protection.31	User Identification and Authentication	13			X	X	X	X	X
Protection.32	Device Identification and Authentication	13	X	X	X				
Protection.33	Authenticator Feedback	13	X	X	X	X	X	X	X
Protection.34	Cryptographic Module Authentication	13			X	X	X	X	X
Protection.35	Information Flow Enforcement	13			X	X	X	X	X
Protection.36	Password Management	13						X	
Protection.37	Concurrent Session Management	13	X	X	X	X	X	X	
Protection.38	Session Lock	13			X			X	
Protection.39	Remote Session Termination	13	X	X	X	X	X	X	
Protection.40	Portable Device Attachment	13			X			X	
Protection.41	Wireless Encryption	13	X	X	X	X	X	X	
Protection.42	Public Network Restriction	13	X	X	X	X	X		
Protection.43	WAN Communication Outage	13	X	X	X				

Control ID	Short Name	Failures	Actuator	Sensor	Field Application	Information Repository	Control Authority	Central Application	External Application
Protection.44	Traffic Control and Filtering	13				X	X	X	X
Protection.45	Non-adjacent Network Restrictions	13	X	X	X	X	X	X	X
Protection.46	Internet and e-mail Restrictions	13			X	X	X	X	
Protection.47	Centralized Authentication	13	X	X	X	X	X	X	X
Protection.48	Secure Coding Practices	14, 15, 16, 17	X	X	X	X	X	X	X
Protection.49	Message Identities	7	X	X	X	X	X	X	X
Protection.50	Data Point State Indicators	12, 11, 6, 1	X	X	X	X	X	X	
Protection.51	No Shared Accounts	13	X	X	X	X	X	X	X
Protection.52	Application Layer Security	13			X	X	X	X	X
Protection.53	Separate Keys for Separate Functions	13	X	X	X				
Reaction.1	Access Revocation - Central	21				X	X	X	X
Reaction.2	Access Revocation - Field	21	X	X	X				
Reaction.3	Physical Access Correlation	21	X	X	X	X	X	X	X
Reaction.4	Unscheduled or Unapproved Activity	13			X	X	X	X	X
Reaction.5	Emergency Access	14, 15, 22	X	X	X	X	X	X	X
Reaction.6	Unsuccessful Access Attempts	13			X			X	
Reaction.7	End Point Isolation	13	X	X	X	X	X	X	X

Control ID	Short Name	Failures	Actuator	Sensor	Field Application	Information Repository	Control Authority	Central Application	External Application
Recovery.1	Alternate Power Source	22				X	X	X	X
Recovery.2	Backup Power Requirement	22	X	X	X				
Recovery.3	Operations Continuity	22				X	X	X	X
Recovery.4	Rebuild System	23	X	X	X	X	X	X	X

Table 7 – Technical Security Controls Mapped against Failures and Roles

Appendix A: Use Case Notation Guide

The use cases presented in Section 2.3 of this document include activity diagrams that graphically depict the flow of information/data and activities performed by roles in order to complete the use case. An example is shown in Figure below.

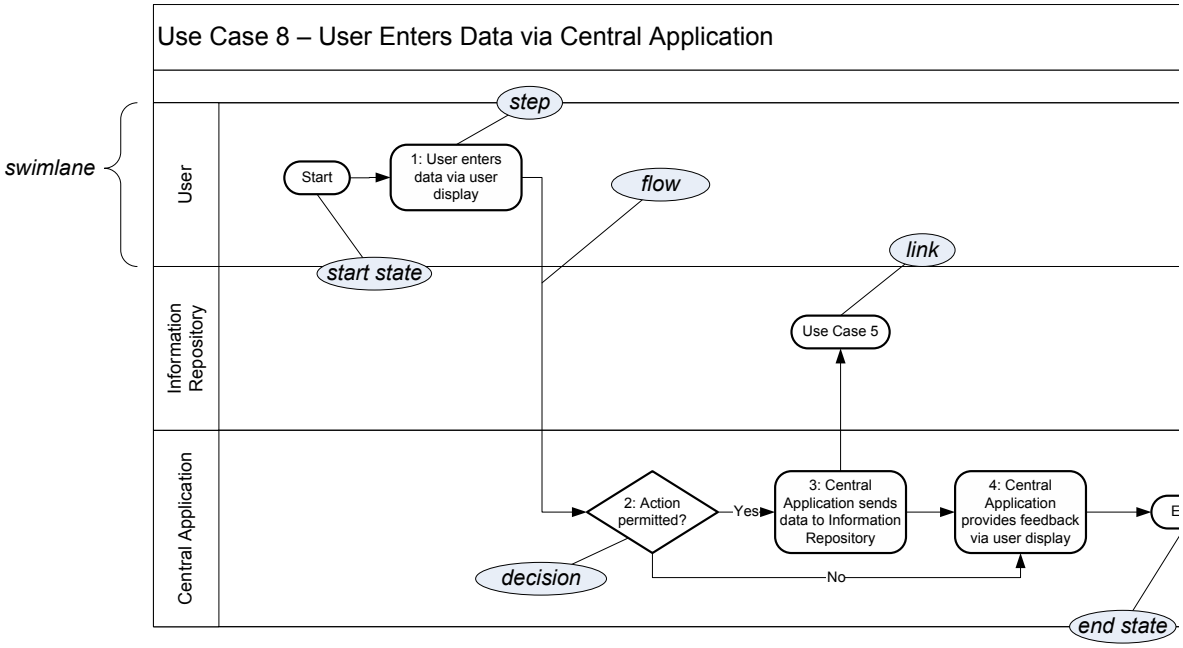

Figure 7 – An Annotated Activity Diagram

This example is annotated to point out key features of the notation.

1. Activity diagrams are organized around *swimlanes*. A swimlane is a horizontal region used to represent the activities of a particular role. For example, Figure contains three swimlanes, one each for the User, Information Repository, and Central Application roles.
2. A swimlane contains *steps* that indicate the activities performed by its role during the use case. A step is represented by a rounded box, is numbered, and includes a short description of the work performed during that step.
3. Steps are ordered across a use case by indicating the *flow* of activities using arrows. A flow points from one step to the step that follows it. Flows can cross swimlanes, typically indicating a communication between the roles represented by the swimlanes.
4. In addition to a general step, there are several special kinds of steps:
    a. A *begin state* is a step labeled "Start" that indicates where a use case begins.
    b. A *decision* is a step in which a role makes a decision as to what step should follow. Flows coming from a decision step are labeled (often with "yes" or "no") to indicate the condition (relative to the decision) under which each flow should be followed; if a flow from a decision step is not labeled, then its condition is considered to be always satisfied. Typically only one flow out of a decision step is followed.
    c. An *end state* is a step labeled "End" that indicates the completion of the use case.
    d. A *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.
5. All steps, except for an end state or link, must have at least one outgoing flow. If a non-decision step has multiple outgoing flows, this indicates a split in the flow. Multiple paths will proceed independently in the use case following such a split.
6. Dashed arrows represent *optional flows*. An optional flow indicates a flow that may or may not always happen in a use case, usually based on variation in the implementation or configuration of a role. For example, if some Field Applications always log their activities with an Information Repository but others do not, then an optional flow would be used to indicate that a Field Application may update an Information Repository. Individual implementations would have to determine whether to exercise optional flows.
7. A use case ends when all of its steps have been completed and all remaining flows lead to a terminal—an end state or a link.
8. If multiple flows lead to a common step, this represents a choice of paths for reaching that step; no synchronization is implied.

Appendix B: Evaluating a Distribution Management System

This document can be used to evaluate a proposed DM deployment. The security controls and the failure analysis are based on the definition of uses cases and roles. In different DM deployments, the use cases and roles will be mapped to different elements of the actual deployment (as illustrated in Section 2.2). For example, a sensor may or may not be controlled by a field application. An architectural analysis of a proposed deployment against this document, then, has the following steps.

1. Map the proposed deployment to the roles in Section 2.1. For every operational element of the proposed deployment (not including communications infrastructure), determine what control authorities and information repositories exist, which applications are central applications and which are field applications, and what types of sensors and actuators exist in the proposed deployment.

2. For each use case, use the mapping generated in step 1 to determine which elements are involved in the use case. Typically, each use case will have multiple instantiations, each with their own elements involved. For example, some sensors will be controlled by field applications and others will not, resulting in an impact on the instantiation of the use cases involving sensors.

3. For each instance of each use case, determine the possible failures, per role and per step. This information comes from Table 2 in Section 3.2. Then determine the controls that mitigate each possible failure using the mapping in Table 7.

4. For each element of the proposed DM deployment, determine the recommended controls for that element. This involves mapping each element to the appropriate use cases and use case steps, proceeding through possible failures and determining the recommended controls. This is the information gathered in steps 1-3 above.

5. For each element of the proposed DM deployment and each recommended control for that element, determine how the control is implemented or how the failure being mitigated by the recommended control is being mitigated by an alternate control.

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 C: 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.[4]

AMI: Automated or advanced metering infrastructure. Utility infrastructure with two-way communications for metering and associated systems allowing delivery of a wide variety of services and applications to the utility and customer.

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.

Actuator: Within a distribution management system, an actuator is a device which performs physical actions. Examples include reclosers and switches.

Application: Within a distribution management system, an application refers to software programs designed to manage and operate physical devices.

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 distribution management resources.

CIS: Customer Information System

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

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.[5]

Central Application: Back office applications which provide supervisory control over other applications and physical devices.

Control Authority: An application or set of applications that assert primary control over subordinate applications and/or physical devices.

DA: Distribution automation, a general term referring to a class of technology that lets electric utilities monitor and remotely control their power distribution networks with two-way computer networking and computerized data handling.

DG: Distributed generation, power generation that happens on the premises of the end user.

DHS: Department of Homeland Security

DM: Distribution Management is the process of managing the physical devices used to distribute of electrical energy.

DOD: Department of Defense

DR: 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.

DM Control System Server Network: Any system that directly communicates with and controls field deployed devices or provides centralized critical operational/support functions (i.e., systems implementing Control Authority, Information Repository, or automated Central Application functionality) is deployed in a DM Control Systems Server Network Segment.

DM Control System User Network: Workstations and devices that provide interactive access to Central Applications in the DM Control Systems Server Network (i.e., systems providing a human-machine interface for Central Application functionality) are deployed in DM Control Systems User Network Segments.

DM Field Network: Field deployed devices (i.e., devices implementing the Field Application, Sensor, and Actuator functionality) and supporting network devices are deployed in a DM Field

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

Network Segment. A typical DM implementation will have multiple DM Field Network Segments.

ERP: Enterprise Resource Planning. Information system used to manage assets, financial resources, and human resources.

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

FEP: A front-end processor.

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.[6]

Fault: A defect in a circuit which causes some level of equipment or system failure.

Feeder: The distribution legs from electrical substations.

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

Field Application: Software applications that reside on devices in DM Field Network Segments.

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.

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

HAN: Home area network, the network in the home created by BPL or another technology and that may need to be able to interact with a DR, AMR or other external application, service or system.

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.

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.

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

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.

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.

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.

IT: Information Technology.

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

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

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.

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.[7]

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)

Non-DM Utility Network: Utility systems that provide other enterprise functions (i.e., systems providing External Application functionality), control systems unrelated to DM, and interfaces to control systems owned by other utilities are deployed in Non-DM Utility Network Segments. Example systems include AMI, ERP, CIS, Generation and Transmission management systems, or corporate business systems. This type of network is intended to include all types of utility networks outside of the scope of DM.

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

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

Open SG: Open Smart Grid.[8]

Private Network: In networking this refers to networks using private IP space as defined by RFC 1918. Within distribution management 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 distribution management this refers to networks not owned, operated, or controlled by the utility or retail electric provider.

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.

Recloser: A device used on medium-voltage power distribution circuits to control the flow of power. A circuit breaker which can automatically re-close the breaker after it has been opened because of a fault.

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.

RFP: Request for Proposal.

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

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

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

SGIP: Smart Grid Interoperability Panel[9]

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.

Smart meter: A utility meter for electricity, natural gas or water, usually, that uses two-way communications technology (see AMI).

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

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

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

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.[10]

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.

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).[11]

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.

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.

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

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.

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

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

Appendix D: References

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

Institute of Electrical and Electronics Engineers, Inc. (2003). *IEEE Std 1613-2003, Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations,* New York, New York.

International Electrotechnical Commission. (2002, January)., *IEC 61850-3 Communication Networks and Systems in Substations - Part 3: General Requirements*

International Electrotechnical Commission, *IEC 62351 - Information Security for Power System Control Operations*

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. Federal Information Processing Standards (FIPS) [as listed below, available at http://csrc.nist.gov/publications/PubsFIPS.html]. Gaithersburg, Maryland.

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

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

FIPS 112 Password Usage, May 1985

FIPS 180 Secure Hash Standard, October 2008

Appendix E: Magnified Use Cases

The Use Case diagrams are repeated below at a scale of one diagram per page for printing and review purposes.

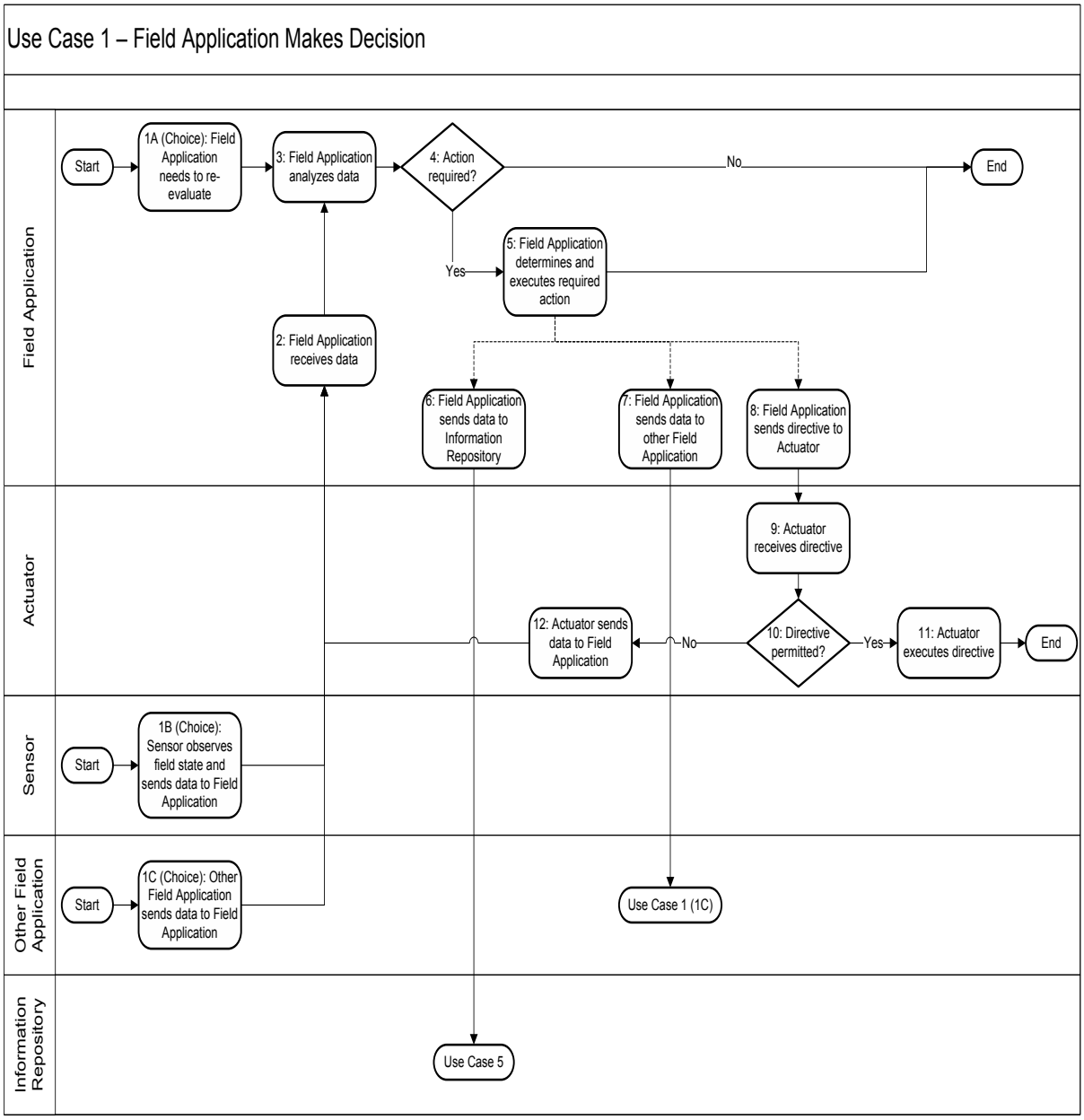

Diagram: Use Case 16 – Field Application Makes Decision

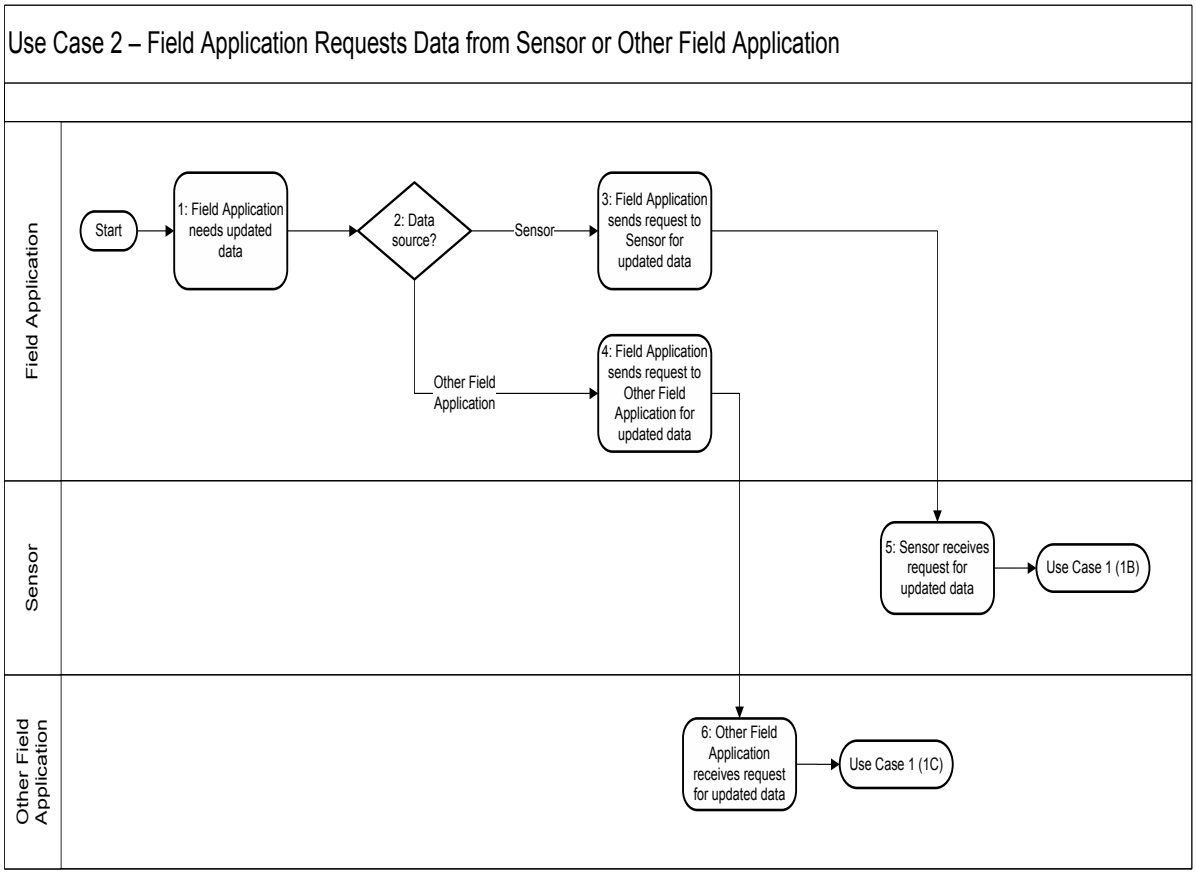

Diagram: Use Case 17 – Field Application Requests Data from Sensor or Other Field Application

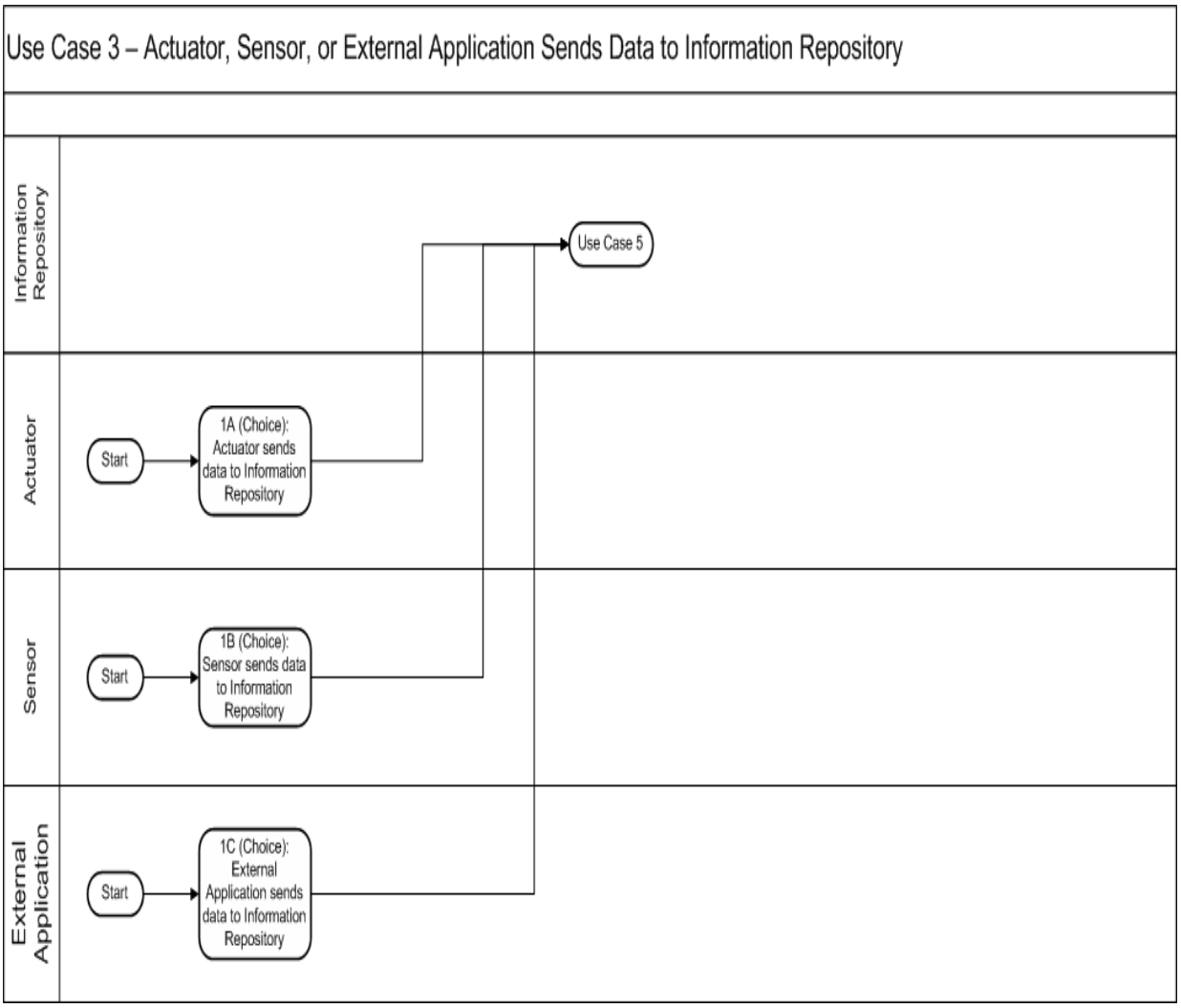

Diagram: Use Case 18 – Actuator, Sensor, or External Application Sends Data to Information Repository

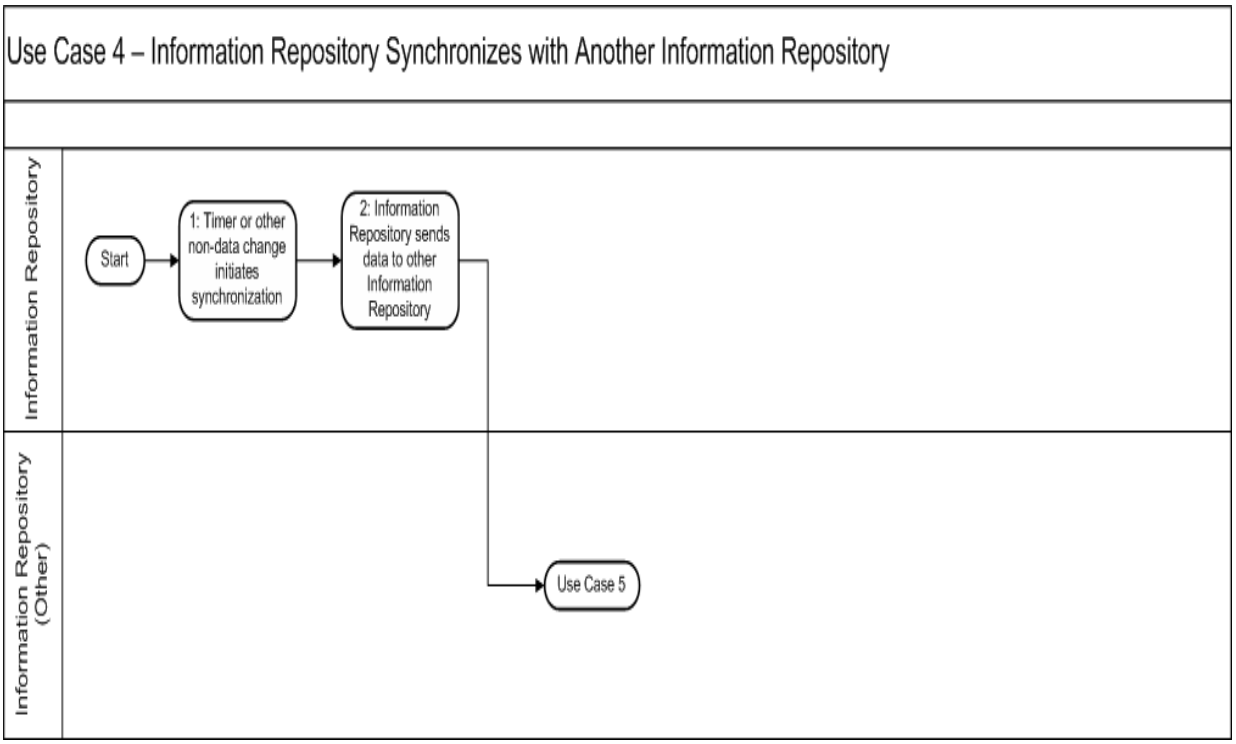

Diagram: Use Case 19 – Information Repository Synchronizes with Another Information Repository

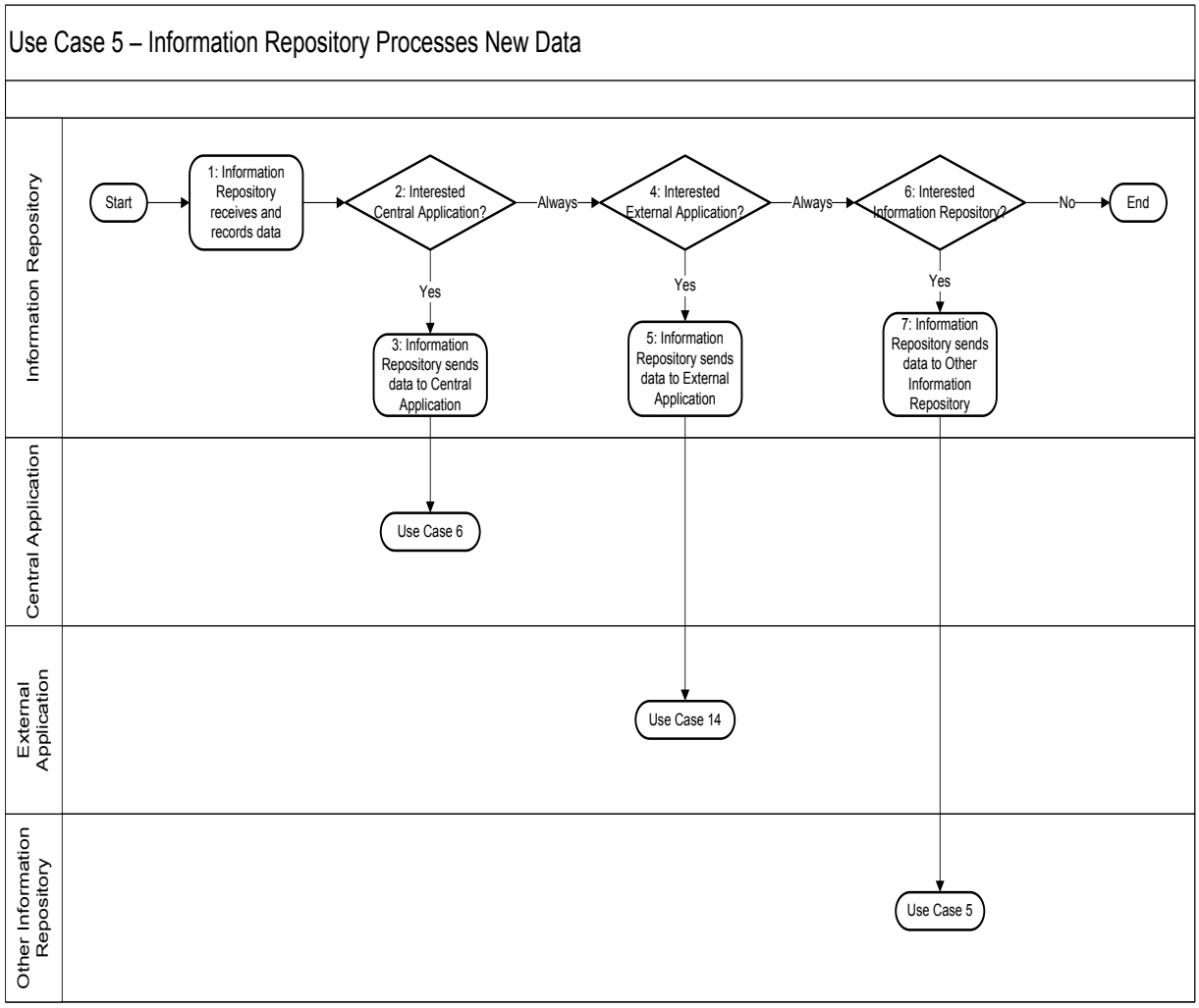

Diagram: Use Case 20 – Information Repository Processes New Data

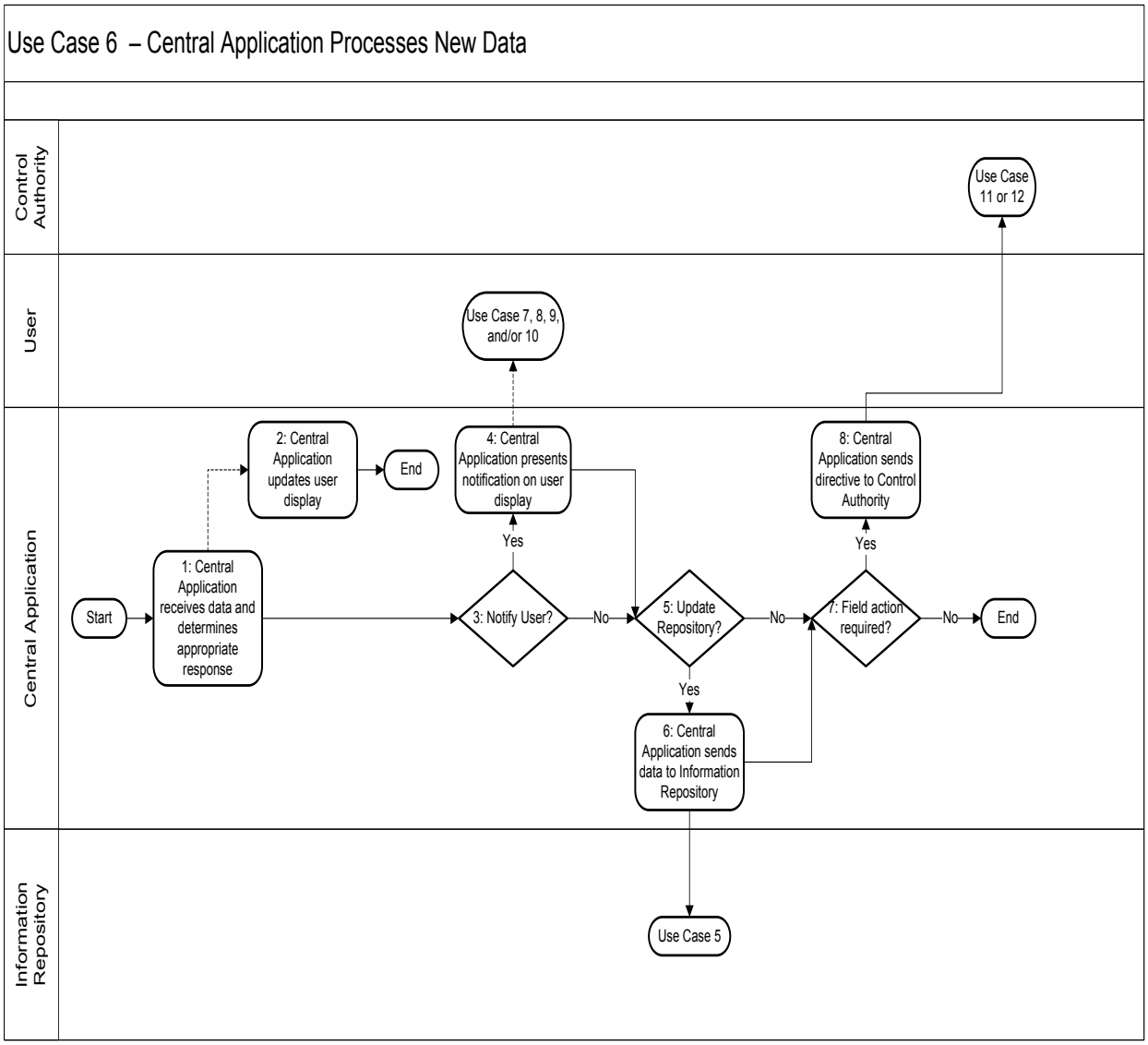

Diagram: Use Case 21 – Central Application Processes New Data

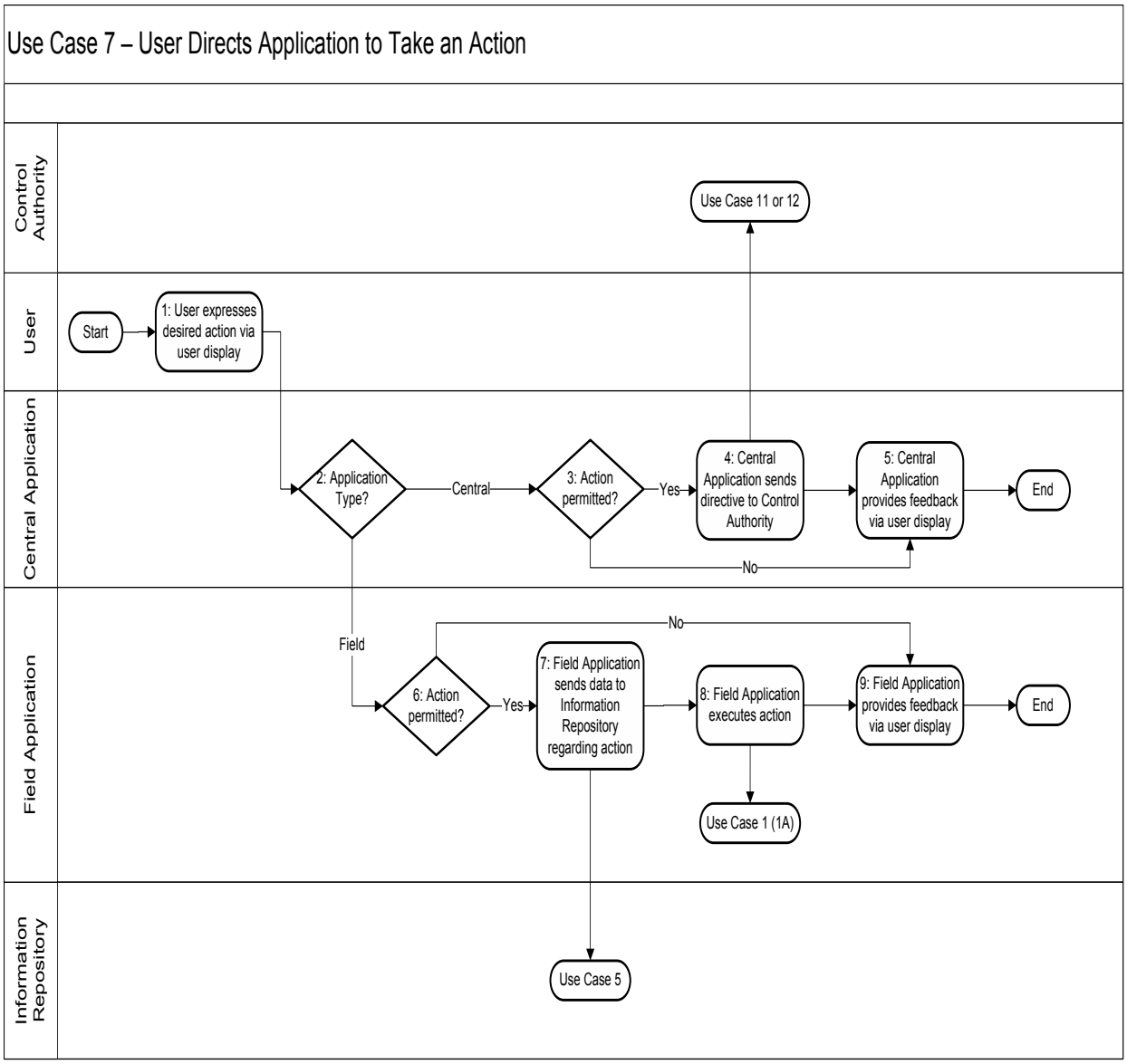

Diagram: Use Case 22 – User Directs Application to Take an Action

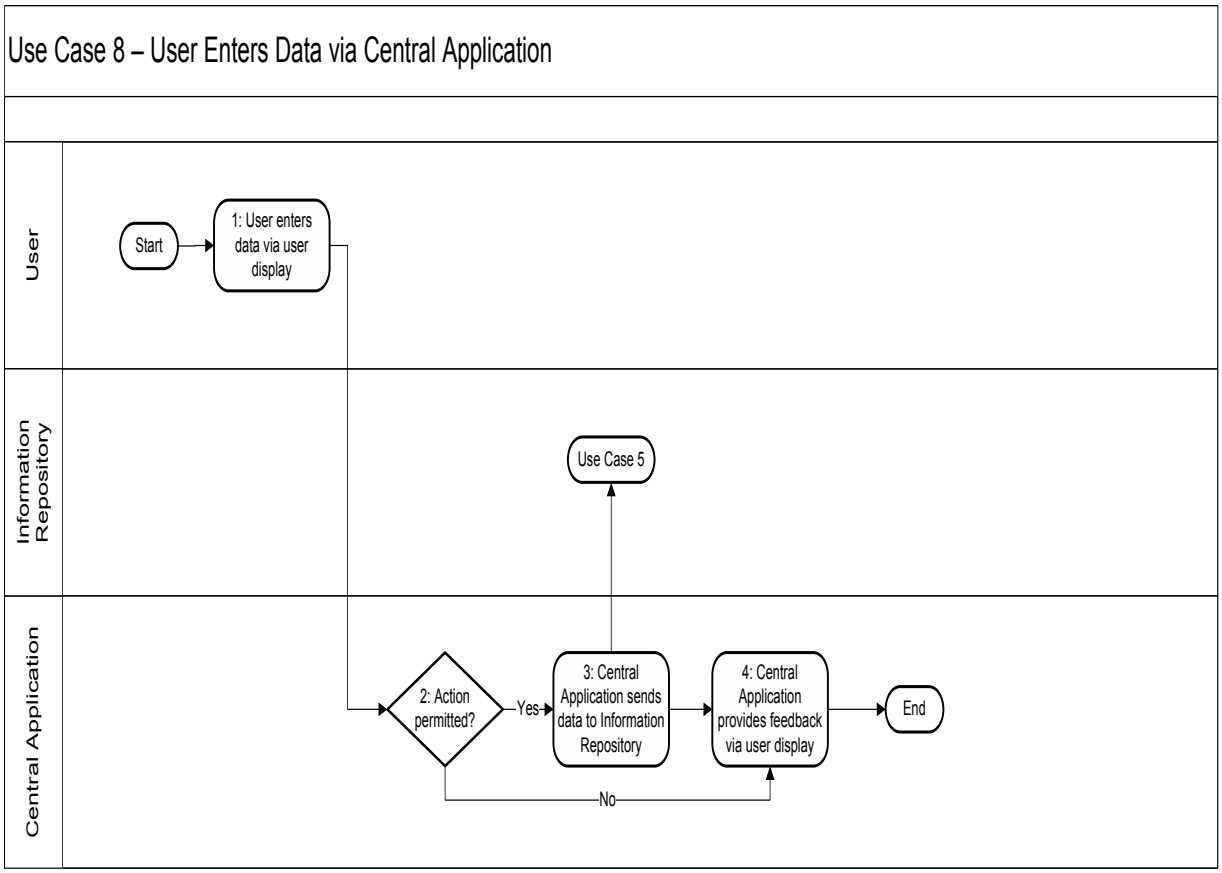

Diagram: Use Case 23 – User Enters Data via Central Application

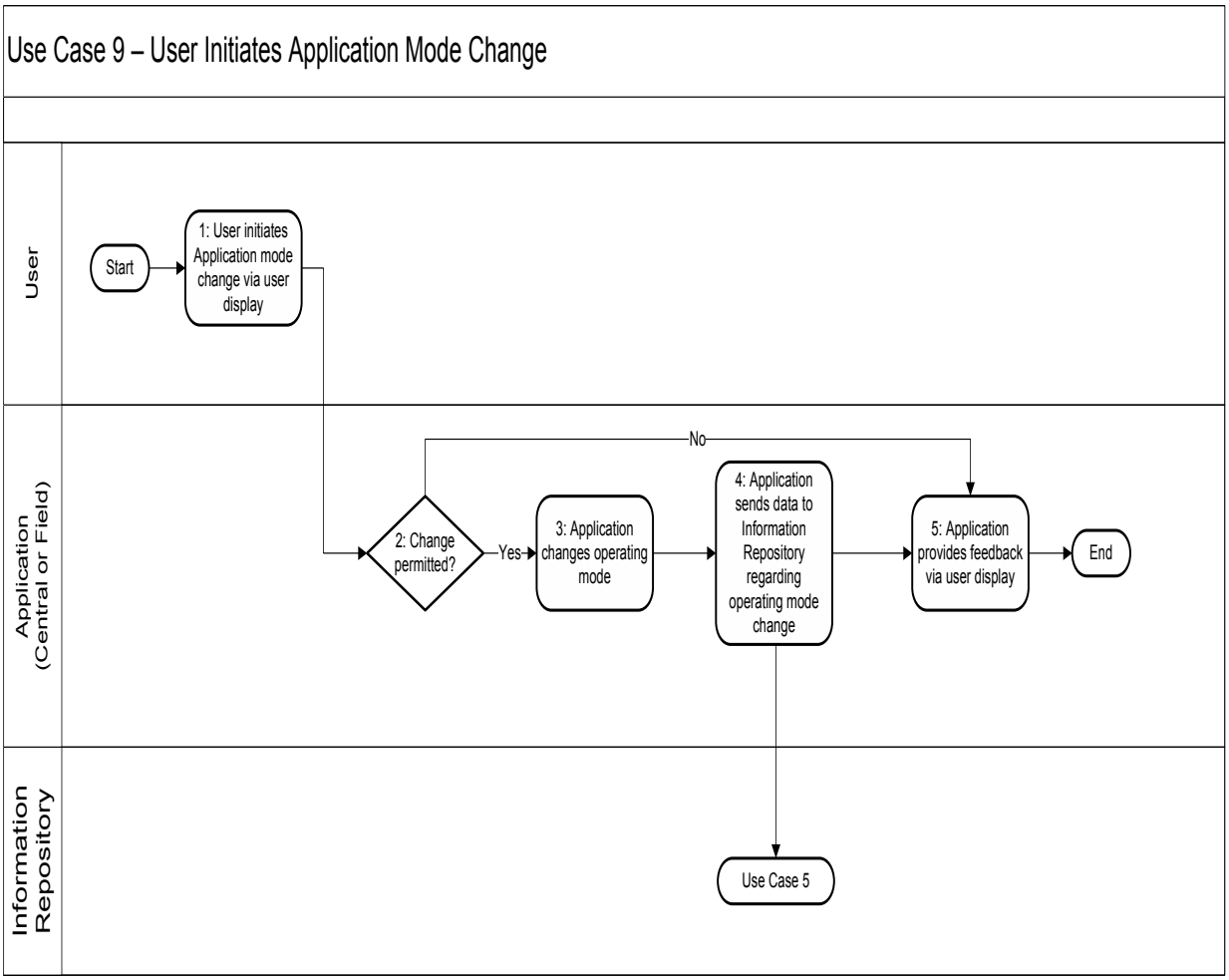

Diagram: Use Case 24 – User Initiates Application Mode Change

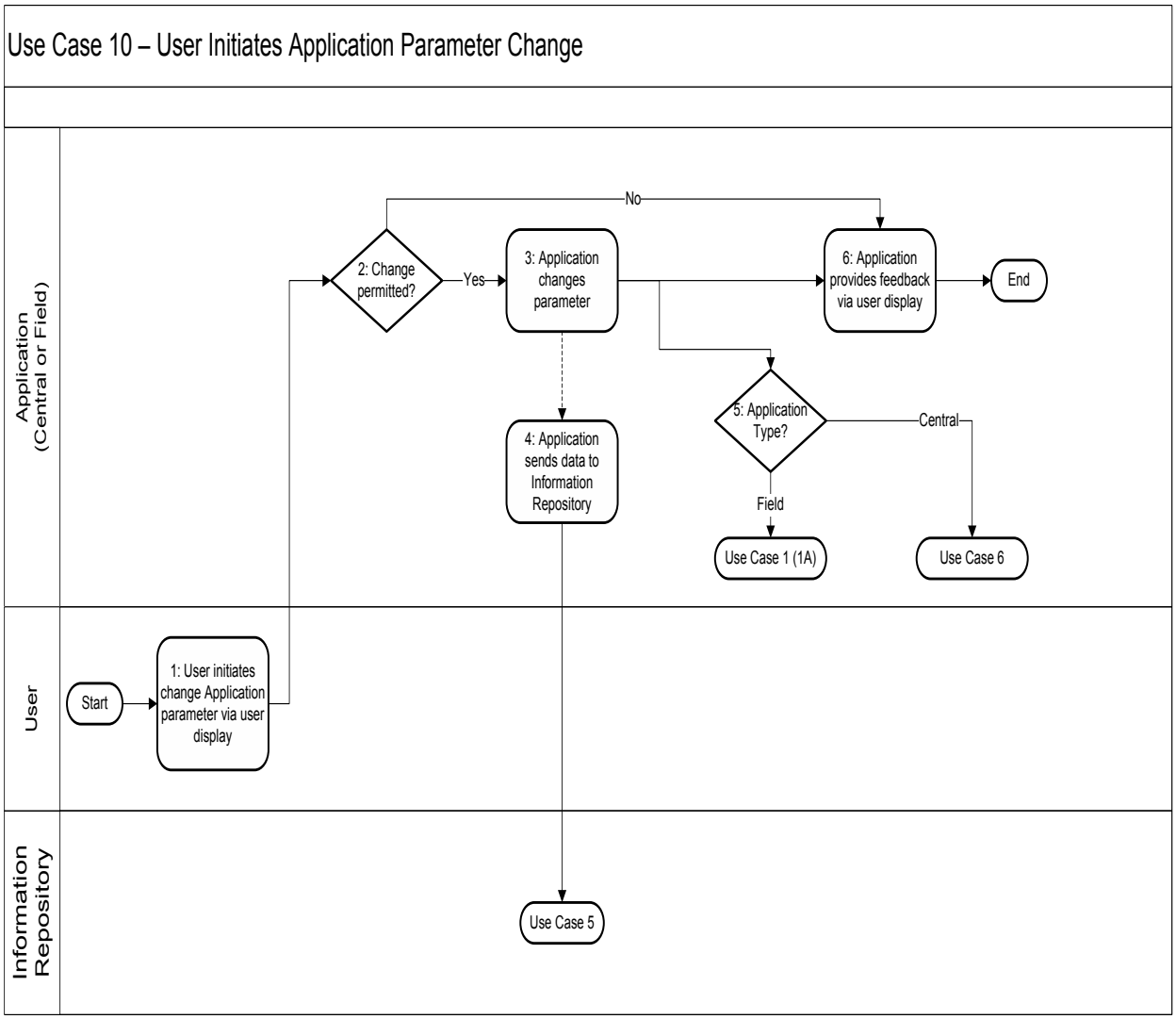

Diagram: Use Case 25 – User Initiates Application Parameter Change

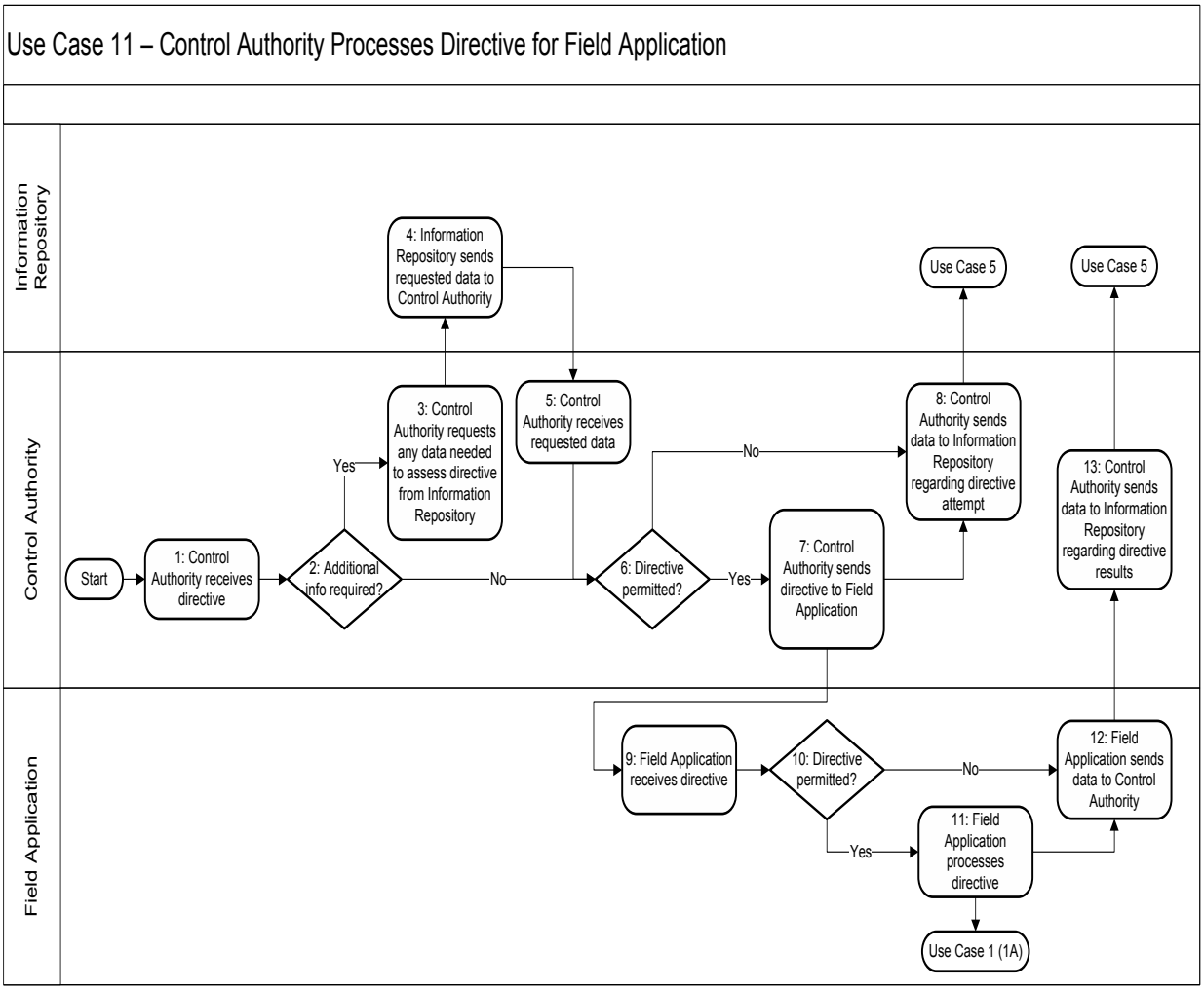

Diagram: Use Case 26 – Control Authority Processes Directive for Field Application

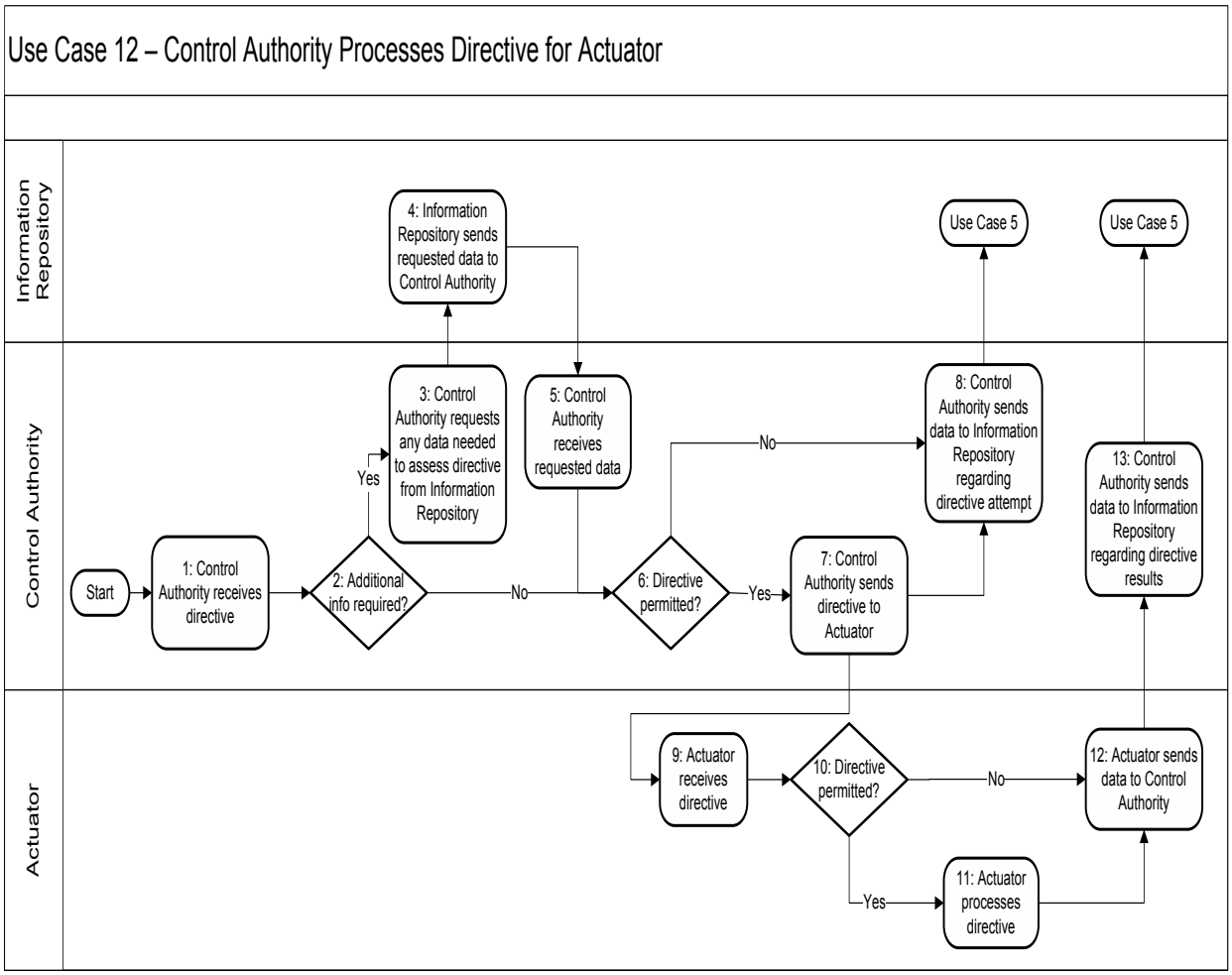

Diagram: Use Case 27 – Control Authority Processes Directive for Actuator

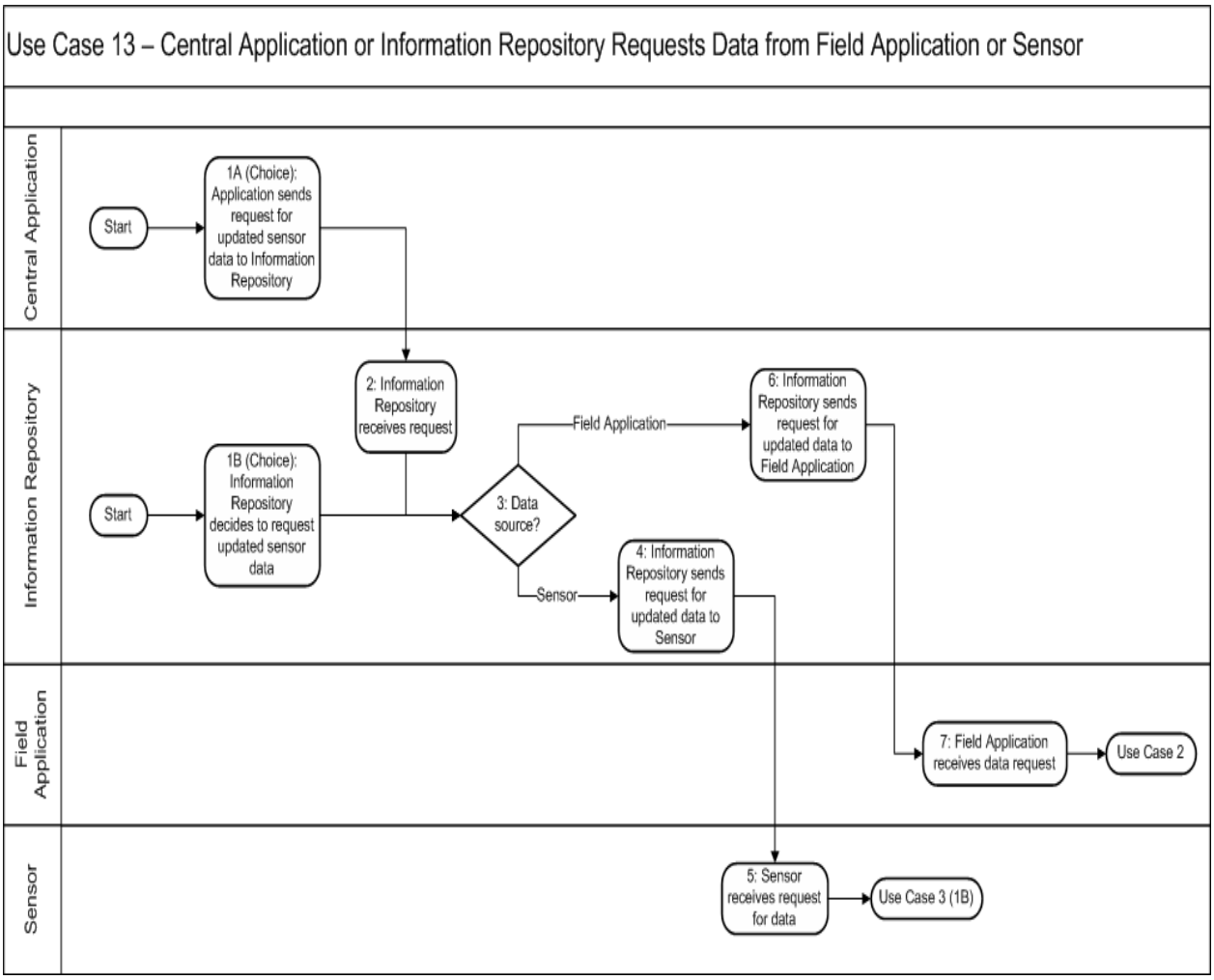

Diagram: Use Case 28 – Central Application or Information Repository Requests Data from Field Application or Sensor

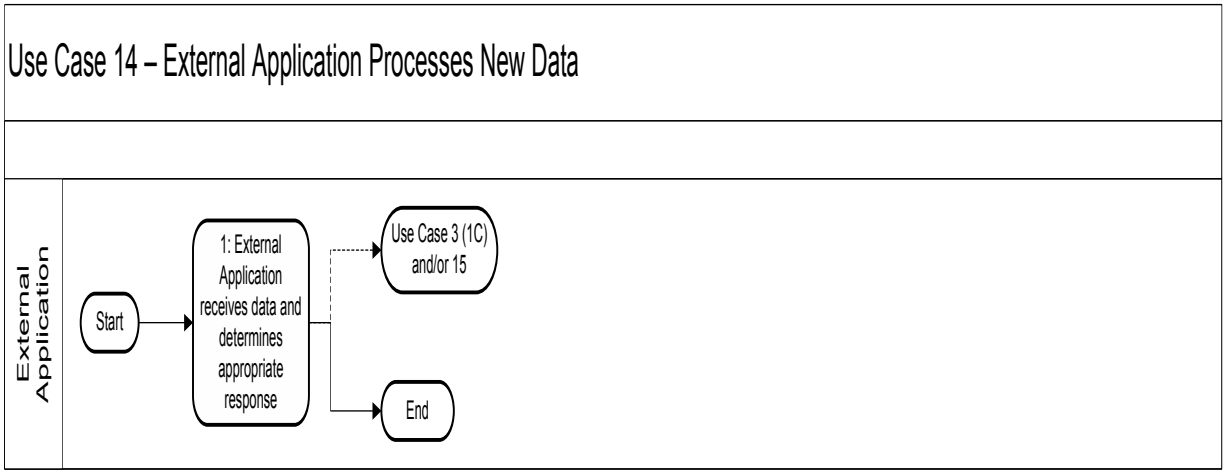

Diagram: Use Case 29 – External Application Processes New Data

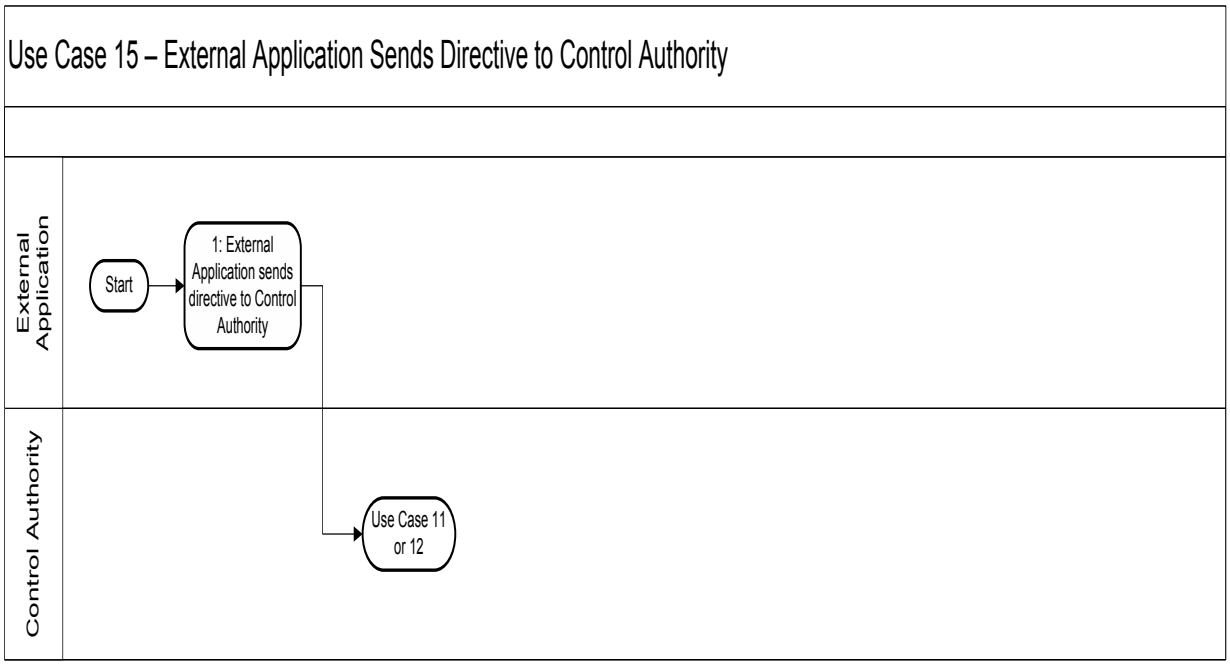

Diagram: Use Case 30 – External Application Sends Directive to Control Authority