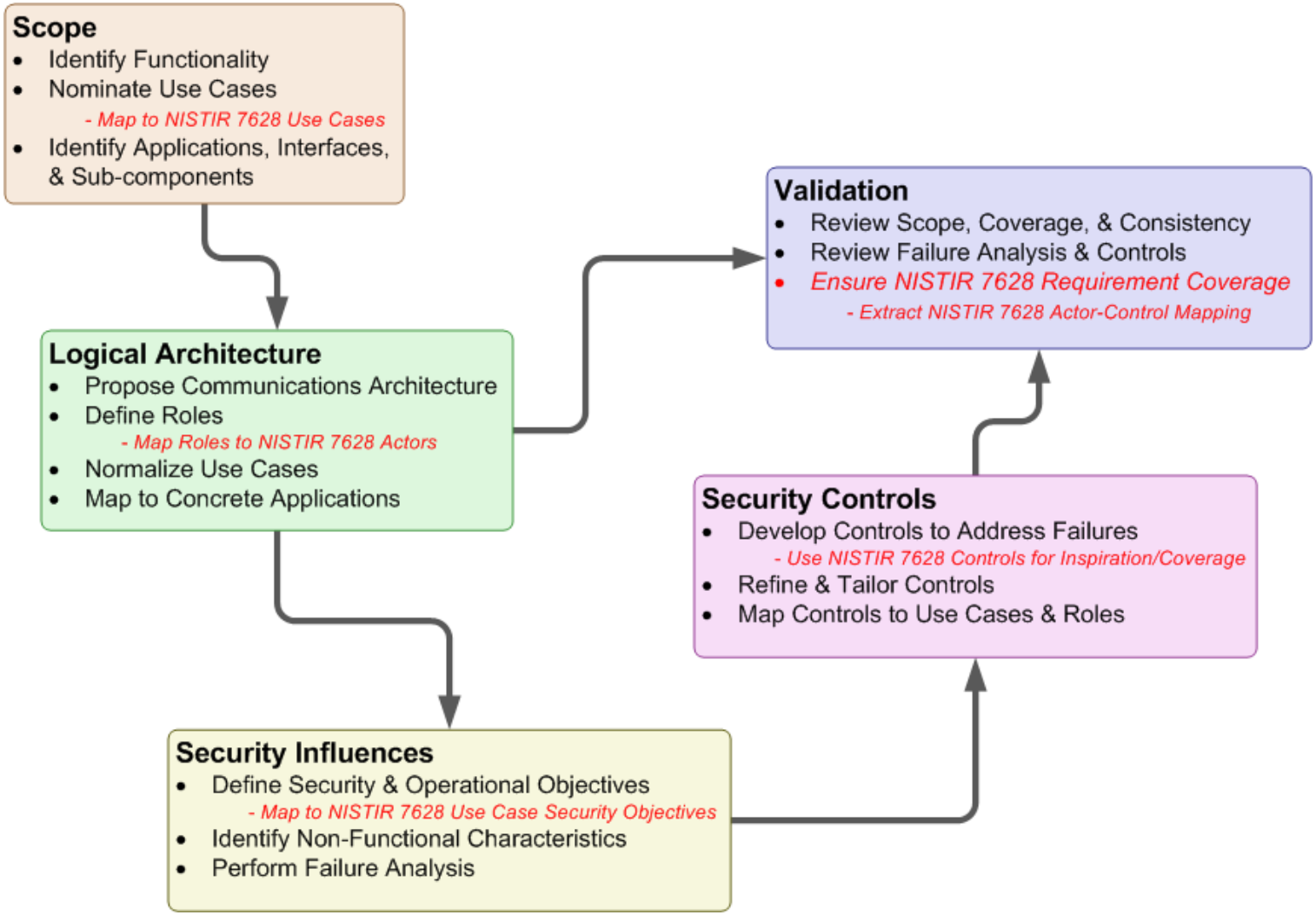
Use Case to Control Process



Basic Steps

1. Scope
   a) Nominate functionality (i.e., use case titles)
   b) Delineate real-world application/component coverage

Black Box

2. Logical Architecture
   a) Nominate logical architecture
   b) Define roles by functionality
   c) Refine use cases & logical architecture

White Box

3. Security Constraints
   a) Define security & operational objectives
   b) Perform failure analysis

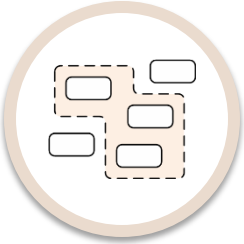
Justification

4. Security Controls
   a) Define controls (including recommended network segmentation)
   b) Map and tailor controls to roles
5. Validation

Reqmts

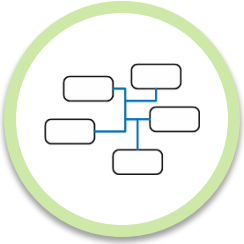
Process Notes: Scope

- Why is this important?
  - First point of entry for new audiences
  - Will likely dictate whether the document gets broad review and engagement
- What does it do?
  - End users must be able to figure out if this document applies to them or not
  - Need an easy and clear “yes” or “no” answer
  - Should not have to understand the rest of the document
- What is the approach?
  - Define functionality covered in real-world terms
  - Provide examples using real-world terminology



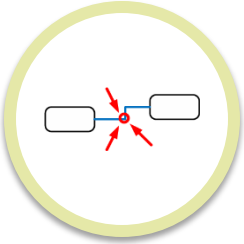
Process Notes: Logical Architecture

- Why is this important?
  - Lack of coverage for functionality is the root of security vulnerabilities
  - Lack of coverage is rarely intentional
    - Ambiguity in terminology
    - Changes in functionality over time
- What does it do?
  - Provides abstract (vendor-neutral) representation of the system to bind controls
  - Removes ambiguity about functionality covered
- What is the approach?
  - Define roles in terms of functionality
  - Describe relationships between the roles
  - Define the functionality in terms of use cases
    - Use a normalized format that facilitates verification of coverage

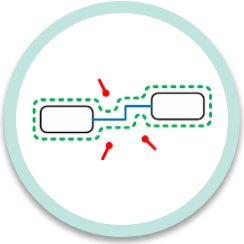


Process Notes: Security Constraints

- Why is this important?
  - Security ultimately has a cost
  - How do we know we are investing in the right place?
- What does it do?
  - Provides justification for selection of controls
  - Provides traceability for ***when*** (not if) system functionality changes
  - Provides a means to quantifiably claim coverage
- What is the approach?
  - Define objectives for system operation
    - What the system should do
    - What the system should **NOT** do
  - Define failures the system should prevent
    - Bind to functionality (avoidance is one means of mitigating risk)
    - Look at both common and functionality-specific failures

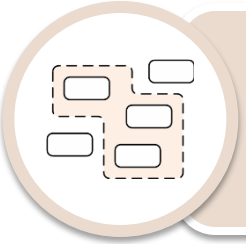


Process Notes: Security Controls



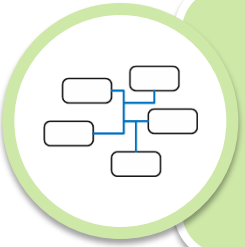
- Why is this important?
  - Actions and requirements must be precisely defined
- What does it do?
  - Provides actionable guidance for the end user
  - Establishes a context to link high-level objectives to low-level security mechanisms
- What is the approach?
  - Generate controls
    - Brainstorm controls from failures
    - Normalize controls into approachable and useful organization for the end user
  - Map to logical architecture
    - System (i.e., network segmentation)
    - Roles
  - Adapt controls to specific context for each role
    - (e.g., consider resource constraints, access requirements, maintenance…)

Document Essentials



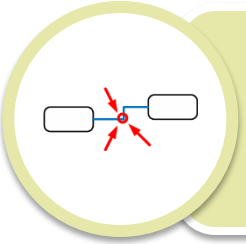
Scope

- Functionality Covered
- Applications, Interfaces, & Sub-Components
- Explicit Examples



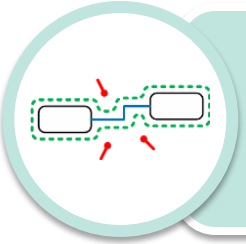
Logical Architecture

- Communications Architecture
- Roles
- Use Cases
- Mapping to Concrete Applications



Security Considerations

- Contextual & Operational Assumptions
- Security Principles
- Failure Analysis



Security Controls

- Network Segmentation
- Control Definitions
- Mapping of Controls to Roles & Segments

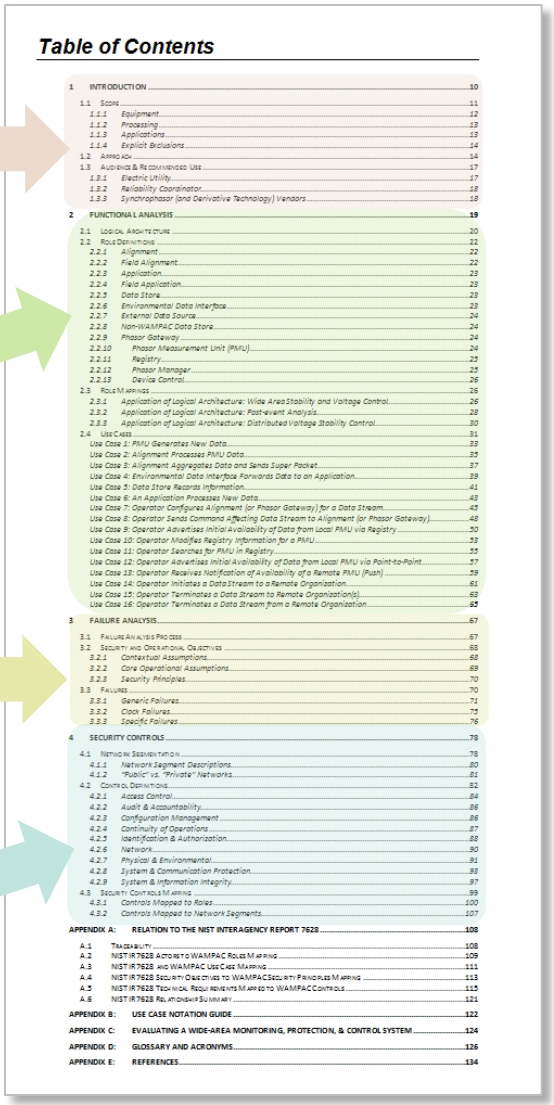


Table of Contents

1 INTRODUCTION 10
1.1 Scope 11
1.1.1 Equipment 12
1.1.2 Processing 13
1.1.3 Applications 13
1.1.4 Explicit Exclusions 14
1.2 Approach 14
1.3 Audience & Recommended Use 17
1.3.1 Electric Utility 17
1.3.2 Reliability Coordinator 18
1.3.3 Synchrophasor (and Derivative Technology) Vendors 18
2 FUNCTIONAL ANALYSIS 19
2.1 Logical Architecture 20
2.2 Role Definitions 21
2.2.1 Alignment 22
2.2.2 Field Alignment 22
2.2.3 Application 23
2.2.4 Field Application 23
2.2.5 Data Store 23
2.2.6 Environmental Data Interface 23
2.2.7 External Data Source 24
2.2.8 Non-WAMPAC Data Store 24
2.2.9 Phasor Gateway 24
2.2.10 Phasor Measurement Unit (PMU) 24
2.2.11 Registry 25
2.2.12 Phasor Manager 25
2.2.13 Device Control 26
2.3 Role Mappings 26
2.3.1 Application of Logical Architecture: Wide Area Stability and Voltage Control 26
2.3.2 Application of Logical Architecture: Post-event Analysis 28
2.3.3 Application of Logical Architecture: Distributed Voltage Stability Control 30
2.4 Use Cases 31
Use Case 1: PMU Generates New Data 33
Use Case 2: Alignment Processes PMU Data 35
Use Case 3: Alignment Aggregates Data and Sends Super Packet 37
Use Case 4: Environmental Data Interface Forwards Data to an Application 39
Use Case 5: Data Store Records Information 41
Use Case 6: An Application Processes New Data 43
Use Case 7: Operator Configures Alignment (or Phasor Gateway) for a Data Stream 45
Use Case 8: Operator Sends Command Affecting Data Stream to Alignment (or Phasor Gateway) 48
Use Case 9: Operator Advertises Initial Availability of Data from Local PMU via Registry 50
Use Case 10: Operator Modifies Registry Information for a PMU 53
Use Case 11: Operator Searches for PMU in Registry 55
Use Case 12: Operator Advertises Initial Availability of Data from Local PMU via Point-to-Point 57
Use Case 13: Operator Receives Notification of Availability of a Remote PMU (Push) 59
Use Case 14: Operator Initiates a Data Stream to a Remote Organization 61
Use Case 15: Operator Terminates a Data Stream to Remote Organization(s) 63
Use Case 16: Operator Terminates a Data Stream from a Remote Organization 65
3 FAILURE ANALYSIS 67
3.1 Failure Analysis Process 67
3.2 Security and Operational Objectives 68
3.2.1 Contextual Assumptions 68
3.2.2 Core Operational Assumptions 69
3.2.3 Security Principles 70
3.3 Failures 70
3.3.1 Generic Failures 71
3.3.2 Clock Failures 73
3.3.3 Specific Failures 76
4 SECURITY CONTROLS 78
4.1 Network Segmentation 78
4.1.1 Network Segment Descriptions 80
4.1.2 "Public" vs. "Private" Networks 81
4.2 Control Definitions 82
4.2.1 Access Control 84
4.2.2 Audit & Accountability 86
4.2.3 Configuration Management 86
4.2.4 Continuity of Operations 87
4.2.5 Identification & Authorization 88
4.2.6 Network 90
4.2.7 Physical & Environmental 91
4.2.8 System & Communication Protection 92
4.2.9 System & Information Integrity 97
4.3 Security Controls Mapping 99
4.3.1 Controls Mapped to Roles 100
4.3.2 Controls Mapped to Network Segments 107
APPENDIX A: RELATION TO THE NIST INTERAGENCY REPORT 7628 108
A.1 Traceability 108
A.2 NIST IR 7628 Actors to WAMPAC Roles Mapping 109
A.3 NIST IR 7628 and WAMPAC Use Case Mapping 111
A.4 NIST IR 7628 Security Objectives to WAMPAC Security Principles Mapping 113
A.5 NIST IR 7628 Technical Requirements Mapped to WAMPAC Controls 115
A.6 NIST IR 7628 Relationship Summary 121
APPENDIX B: USE CASE NOTATION GUIDE 122
APPENDIX C: EVALUATING A WIDE-AREA MONITORING, PROTECTION, & CONTROL SYSTEM 124
APPENDIX D: GLOSSARY AND ACRONYMS 126
APPENDIX E: REFERENCES 134

For Each Use Case You Need To Think About

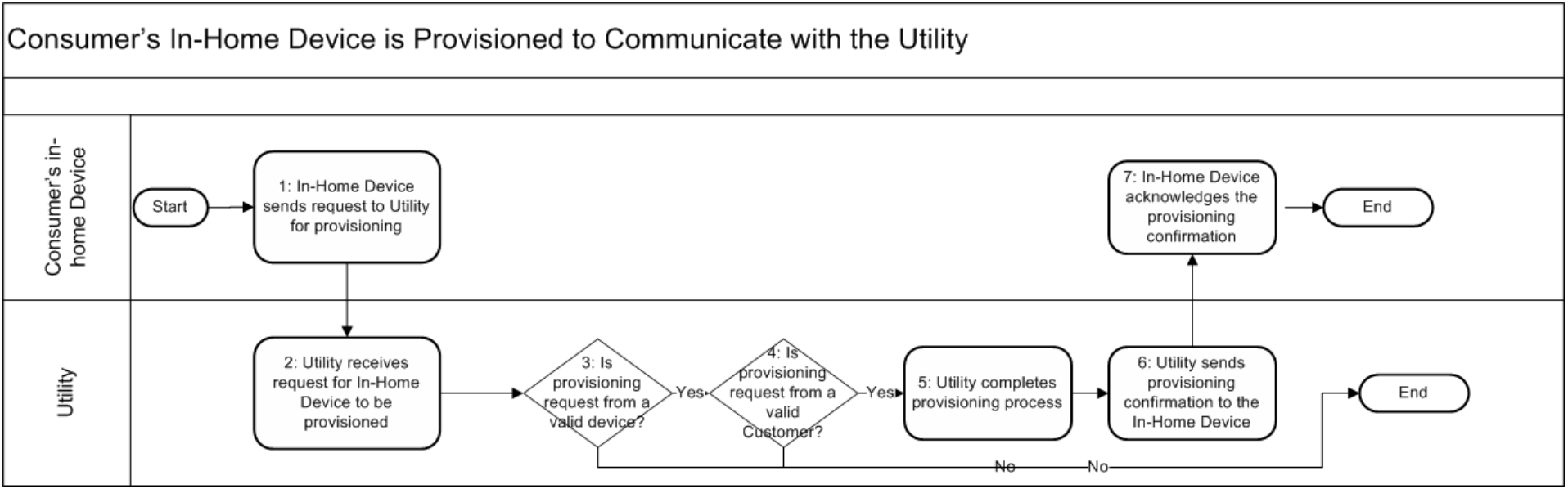
- Preconditions
- Minimal Guarantees
- Success Guarantees
- Trigger

Use case 1 - Customer’s In Home Device is Provisioned to Communicate With the Utility

Use case 1 - Summary

- Scenario: Customer’s In Home Device is Provisioned to Communicate With the Utility
- Description: This scenario describes the process to configure a customer’s device to receive and send data to utility systems. The device could be an information display, communicating thermostat, load control device, or smart appliance.

Use case 1 – Business Flow



Use Case 1 – SG Characteristics

- Characteristics
  - Enables active participation by consumers
  - Accommodates all generation and storage options
  - Enables new products, services and markets
- Potential Stakeholder issues
  - Customer device standards
  - Customer data privacy and security

Use Case 1 – SG CyberSecurity Objectives

- To protect passwords
- To protect key material
- To authenticate with other devices on the AMI system

Use case 1 – Potential Transactions

- Registration of the customer device
- Authentication of the customer device
- Receiving information from the utility
- Sending information to the utility
- Receiving a command from the utility
- Recording information on the device

Use case 1 – Potential Information

- Customer ID
- Customer authentication
- Device location information
- Device ID
- Device type
- Device configuration
- Device authentication information
- Logging information
- Time of day

Use case 1 – Potential Failures With (1)

- Send Data
  - Sends to wrong place
  - Sends wrong data
  - Sends corrupted data
  - Spurious send
  - Not authorized to send
  - Sends data late (not timely)
- Receive data
  - Not from authorized sender/from wrong sender
  - Receives wrong data
  - Receives corrupted data
  - Spurious receive
  - Does not receive timely data
  - Data is inappropriately rejected

Use case 1 – Potential Failures With (2)

- Store data
  - Allows unauthorized access and manipulation
  - Storage corrupted
  - Storage exhaustion
- Process data
  - Does not execute in a timely fashion (resource starvation)
  - Mis-configured
  - Subverted to execute wrong code

Use case 1 – Potential Failures With (3)

- Potential specific failures
  - Communication interruption – verbal, email and other non-energy use information
  - Does not act on a authenticated command
  - Acts on a authenticated command against local policy
  - Stolen credentials used to authorize command
  - Processes unrecognized command
  - Processes unauthenticated command
  - Fails to execute action based on changes to its operational parameters, its data, or its internal state
  - Processes an incorrectly formatted message
  - Does not respond to a message in a timely fashion
  - Fails to execute action in a timely fashion after receiving a legitimate message

Use case 1 – Potential Failures With (4)

- Potential specific failures
  - Need to have graceful failure (fail safely)
  - Default failure configuration (e.g. DR)
  - Fails to protect information or resources against authorized access
  - Fails to accept authorized and valid message
  - Fails to execute action based on changes to its operational parameters, its data, or its internal state
  - Executes wrong action based on changes to its operational parameters, its data, or its internal state
  - Accepts corrupted configuration file
  - Hardware, facilities or both fail and prevent proper operation
  - Failure to provide adequate protection against reasonable expectations for harm due to natural phenomenon, such as earthquakes, hurricanes, tornadoes, and electromagnetic interference
  - Failure to provide recovery mechanisms essential for the restoration of a failed or compromised system

Use case 1 – Potential Controls for Each Failure

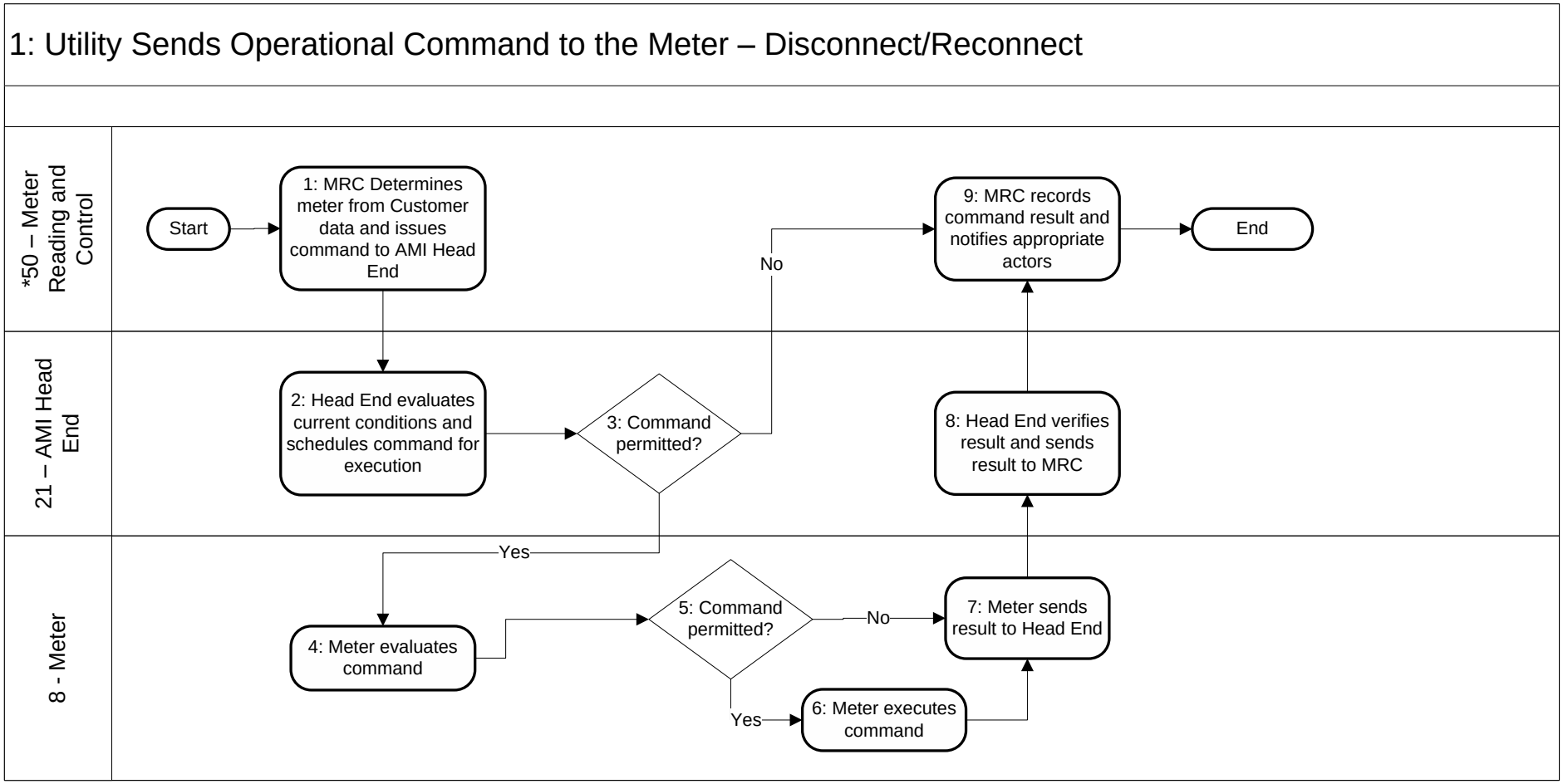
- Define at least one control for each failure
- Create a mapping back and forth to ensure every failure has a control and for every control we can indentify at least one failure

Use case 2 - Remote Connect/Disconnect of Meter

Use case 2 - Summary

- Scenario: Remote Connect/Disconnect of Meter
- Description: Traditionally, utilities send a metering service person to connect or disconnect the meter. With an AMI system, the connect/disconnect can be performed remotely by switching the remote connect/disconnect (RCD) switch for the following reasons:
  - Remote Connect for Move-In
  - Remote Connect for Reinstatement on Payment
  - Remote Disconnect for Move-Out
  - Remote Disconnect for Nonpayment
  - Remote Disconnect for Emergency Load Control
  - Unsolicited Connect / Disconnect Event

Use case 2 – Business Flow



Use Case 2 – SG Characteristics

- Characteristics
  - Optimizes asset utilization and operate efficiently
  - Operates resiliently against attack and natural disasters
- Potential Stakeholder issues
  - Customer data privacy and security
  - Retail Electric Supplier access
  - Customer data access
  - Customer Safety

Use Case 2 – SG CyberSecurity Objectives

- Integrity of control commands to the RCD switch is critical to avoid unwarranted disconnections or dangerous/unsafe connections. The impact of invalid switching could be very large if many meters are involved
- Availability to turn meter back on when needed is important
- Confidentiality requirements of the RCD command is generally not very important, except related to non-payment

Use case 2 – Potential Transactions

- Valid registration of device/meter
- Authentication of the device/meter
- Receiving information from the utility
- Sending information/confirmation to the utility
- Receiving a command from the utility
- Recording information on the device

Use case 2 – Potential Information

- Customer ID
- Customer authentication
- Device location information
- Device/Meter ID
- Device/Meter type
- Device/Meter configuration
- Device/Meter authentication information
- Logging information
- Time of day
- Command information from device/meter and utility
- Response to the command from device/meter and utility

Use case 2 – Potential Failures With

- Sending information
  - Authorization
  - Authentication
  - Disclosure
  - Availability
  - Logging / Auditing
  - Communication links – down, delay, etc
- Receiving information
- Information storage
- Communication method
- The information itself

Use case 2 – Potential Controls for Each Failure

- Define at least one control for each failure
- Create a mapping back and forth to ensure every failure has a control and for every control we can indentify at least one failure