Analysis of Selected Electric Sector High Risk Failure Scenarios

National Electric Sector Cybersecurity Organization Resource (NESCOR)

December 2015

Version 2.0

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

Revision history

version	date	changes
0.2	2013.1.2	Initial skeleton for document
0.3	2013.1.22	Added Impact instructions from Section 5.2.2.1 of the 0.8 short failure scenarios document. Added 5.2.2.2, criteria for effects on likelihood and opportunity, for Difficulty of Steps. Updated table to reference these new sections. Added Appendix A, content from Section 3 FAILURE SCENARIO THREAT MODEL.
0.9	2013.7.24	Initial release outside of drafting team
1.0	2013.8.24	Initial public release.
2.0	2015.12.04	Revised all attack trees based on updated common attack trees Added generation failure scenarios updated common attack trees.

ACKNOWLEDGMENTS

The research was paid for by the Department of Energy (DOE) under the NESCOR grant.

Principal Investigator

A. Lee

The first version of this report was produced as a collaborative effort of industry experts, asset owners, and academia who participate in NESCOR technical working group (TWG) 1. This version was developed by utilities and EPRI staff.

NESCOR would like to acknowledge all TWG 1 members who provided feedback to the drafting team whose members were: Jordan Henry, Steve Harp, E. K. Lee, Carol Muehrcke, Charlie Payne, Elizabeth Sisley.

Version 2 was developed by EPRI and utility members, particularly Ameren and Luminant.

Related Documents:

1. *Cyber Security for DER Systems*, Version 1.0 July 2013
2. *NESCOR Guide to Penetration Testing for Electric Utilities,* Version 3.0
3. *Wide Area Monitoring, Protection, and Control Systems (WAMPAC), Standards for Cyber Security Requirements*, Oct 26, 2012
4. *Electric Sector Failure Scenarios and Impact Analyses,* Version 3.0, December 2015

Executive Summary

The National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group 1 (TWG1) developed the first version of this document using the failure scenarios included in the Failure Scenarios and Impact Analyses document. Information about potential cyber security failure scenarios is intended to be useful to utilities for risk assessment, planning, procurement, training, tabletop exercises and security testing. A cyber security failure scenario is a realistic event in which the failure to maintain confidentiality, integrity, and/or availability of sector cyber assets creates a negative impact on the generation, transmission, and/or delivery of power. Some of the scenario descriptions include activities that typically are not allowed by policies, procedures, or technical controls. These scenarios may be used to ensure that the applicable mitigation strategies are specified and implemented.

This document builds upon the previously published NESCOR document, "Electric Sector Failure Scenarios and Impact Analyses," referred to here as the "short failure scenario document." That prior document provides short descriptions of approximately 125 failure scenarios across the following domains of the electric sector:

1. Advanced Metering Infrastructure (AMI)
2. Distributed Energy Resources (DER)
3. Wide Area Monitoring, Protection, and Control (WAMPAC)
4. Electric Transportation (ET)
5. Demand Response (DR)
6. Distribution Grid Management (DGM)

These domains correspond to the those identified in the National Institute of Standards and Technology (NIST) Special Publication 1108, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0,* Office of the National Coordinator for Smart Grid Interoperability. In addition, there are failure scenarios in two additional domains, Generation (GEN) and a crosscutting category called “Generic,” which includes failure scenarios that may impact many of these functional domains.

The present document provides detailed analyses for a subset of the failure scenarios identified in the short failure scenario document. All analyses presented include an attack tree, which details in a formal notation, the logical dependencies of conditions that allow the failure scenario to occur. Several of the analyses also provide a detailed text write up for the scenario, in addition to the attack tree. Failure scenarios in the short failure scenario document were prioritized for inclusion in the present document, based upon level of risk for the failure scenario, the priorities of NESCOR utility members, and the priorities of the generation working team. This document includes the following:

- Text format analyses and attack trees for two AMI failure scenarios, one DGM failure scenario, and two GEN failure scenarios (Section 2)

- Attack trees for six additional AMI failure scenarios and two DR failure scenarios (Section 3)

- Common sub trees referenced by several attack trees (Section 4)

- A glossary that defines terminology related to less familiar potential mitigations called out in the failure scenario analyses (Appendix A)

- Rationale for selection of the specific failure scenarios in this document (Appendix B)

- A description of the template used for the detailed failure scenario text analyses and attack trees, and the rationale for use of this template (Appendix C)

- A threat model that defines a list of threat agents, which is referenced by the failure scenario analyses (Appendix D).

Information included in the present document for a particular failure scenario expands upon that provided in the short failure scenario document. For example, impact information is detailed per a list of standard impact categories, and potential mitigations are tied to specific conditions (nodes) in the attack tree. The purpose of the additional detail provided by the analysis in this document is to help a utility:

- To understand its particular points of susceptibility to a failure scenario,
- The potential impact should this scenario occur in their environment, and
- Which potential mitigations are appropriate for their mitigation strategy?

Examples of insights from the development of this document are:

- A set of pluggable "common sub trees" have been identified that appear in many failure scenarios attack trees. This not only simplifies tree development, but, more importantly, highlights specific opportunities for common mitigations across several failure scenarios.

- Analysis of the potential for an unintended mass meter disconnect depends upon both enforcement of business rules for legitimate meter disconnect as well as the architecture used to enforce these rules and carry out the disconnect action. (AMI.1 analysis)

- The impact of theft of power due to malicious meter reconfiguration might be minimized by a centralized configuration-check-and-reset capability not known to be used today. (AMI.32 analysis)

- Six unique methods are identified via which a threat agent may gain access to a distribution grid management system. (DGM.11 analysis)

This document does not include a comprehensive set of attack trees. The number of high priority failure scenarios analyzed in this document was determined by available schedule and resources; additional analyses may be added in the future.

1 Contents

Table of Figures

Table of Tables

1 INTRODUCTION AND CONTEXT

This document describes a set of detailed failure scenarios for the electric sector. These scenarios are based on the short failure scenarios. The original National Electric Sector Organization Resource (NESCOR) failure scenario documents did not include generation. This documents addresses that gap. Attack trees are provided for the scenarios included in this document. Appendix C describes the analysis presentation format/content and the rationale for its use.

A cyber security failure scenario is a realistic event in which the failure to maintain confidentiality, integrity, and/or availability of sector cyber assets creates a negative impact on the generation, transmission, and/or delivery of power. Previously, NESCOR published a compendium of electric sector failure scenarios with short descriptions, typically less than one page each. That document is titled "Electric Sector Failure Scenarios and Impact Analyses" [1]. An updated version of that document is also available. Some of the scenario descriptions include activities that typically are not allowed by policies, procedures, or technical controls. These scenarios may be used to ensure that the applicable mitigation strategies are specified and implemented. That document is referred to here as "the short failure scenario document," in contrast to the present document, which presents longer, more detailed, failure scenario analyses. Information about potential cyber security failure scenarios is intended to be useful to utilities for risk assessment, planning, procurement, training, tabletop exercises and security testing, as discussed in [1].

The present document expands upon the results in the short failure scenario document by providing detailed analyses for scenarios from that document. This version added two generation failure scenarios. The two scenarios were selected based on assessment made by the generation failure scenario team.

Although the failure scenarios in the present document are inspired by specific scenarios in the short failure scenario document, they are not necessarily limited to the scope defined by those original scenarios. Specifically, a benefit of the attack tree format is that it leads to the discovery of related scenarios and variations of scenarios. These are included in the present document where deemed useful, whether or not they appeared in the short failure scenarios document.

2
ELECTRIC SECTOR FAILURE SCENARIO ANALYSES

2.1 General

2.1.1 Scope

Included in this section are analyses of the following failure scenarios. Each analysis includes both a text description and an attack tree. Appendix B provides the rationale for selection of these failure scenarios for detailed analysis.

- AMI.1: Advanced Metering Infrastructure failure scenario - Mass Meter Disconnect by Authorized Individual
- AMI.32: Advanced Metering Infrastructure failure scenario - Threat Agent Performs Mass Meter Disconnect
- DGM.11: Distribution Grid Management failure scenario - Threat Agent Triggers Blackout via Remote Access to Distribution System
- GEN.1: Threat agent adds spurious trip parameters on remotely located plant support equipment and trips unit offline
- GEN.15: Plant tripped off-line through access gained through a compromised vendor remote connection

2.1.2 Attack Tree Notation Quick Start

The following generic example illustrates how to read an attack tree in this document. For more information, see Appendix C, which provides a complete description and rationale for both the text and attack tree formats used to present a failure scenario in this document. This format was initially presented in earlier versions of [1]; it has been moved to the present document and updated.

The common sub trees referenced by the attack trees in this document are included in Section 4. These are fragments of attack trees, which were found to be repeated across several scenarios, or several times within a single scenario. Hence it was more convenient to present them once in a parameterized fashion, and then invoke them using relevant parameters in specific instances.

2.1.3 Failure Scenario Template Graphic

A graphic format suitable for development as a PowerPoint slide has been developed by TWG1 to provide a visual representation that describes a failure scenario in a concise manner. The template information that is included in the diagram is noted in the last column of Table 8, Categories of Impact for a Specific Scenario. The graphical notation used is illustrated below and shows a modified annotated attack tree. Key aspects of this notation are:

- The tree is shown on each slide, with truncated branches represented by double lines around the numbered small hexagons. These branches are then shown on another slide.

- Each hexagon represents a condition in the sequence of conditions that make up a failure scenario. The leaves directly connected to and above a leaf represent the full conditions necessary for that lower leaf to occur. The conditions can be descriptions of several steps that must occur within a failure scenario.

- The tree is read from top to bottom, in terms of the sequence of conditions that occur. (This is a revision to the standard attack tree format – where the tree is followed from bottom to top. The objective was to provide a diagram that is easier to read.)

- A condition is labeled with the SOURCE that initiated that condition and the action (STIMULUS) that was initiated. A source is typically a human actor or a cyber component.

- The numbers that label each hexagon (condition) are ID's to enable a user to refer to specifics of the figure. They do not represent an ordering of condition. A double border indicates that the branch is truncated, and continues on another diagram.

- Connection of two conditions by a line means that the lower condition depends upon the higher condition.

- Connection by a dotted line means "OR", that is, a lower condition can occur if either one OR the other of the connected upper conditions occurs. If all upper conditions are required for a lower condition to occur, a solid line is used, representing "AND."

- At the bottom of the attack tree are two additional nodes – the first indicates what happens to the system after the failure scenario occurs (system response), represented with a rounded square, and the second describes the impact when this occurs, represented with an oval.

Common Sub Trees are a simplification technique that represents those subsets used in many attack trees, and is represented as a hexagon with double outlines as shown. Creating modular subsets simplifies the specific attack trees by allowing those common details to be documented in their own trees. The specific trees then instantiate a Common Sub Tree with the pertinent context of how it is being referenced.

- The Common Sub Tree has a common name, such as Threat Agent Obtains Credentials, but also include the context, "for system or function". The specific attack tree will then specify which system or function is referenced.

- The mitigation documented on the specific attack tree will state "See Common Sub Tree Threat Agent Obtains Credentials for <system or function>".

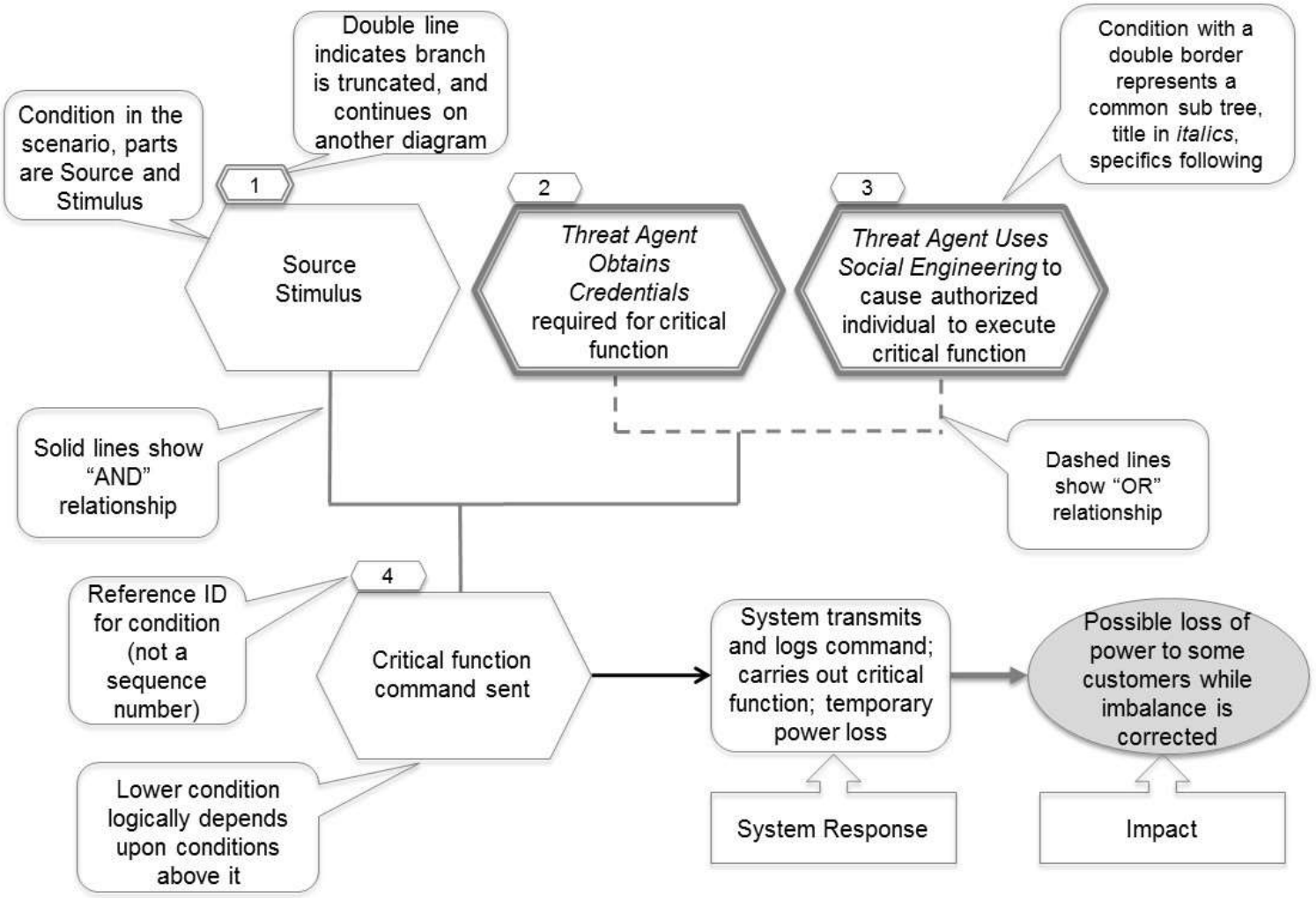

Figure 1
Graphical Notation for Annotated Attack Tree Format

2.2 AMI.1 Authorized Individual Issues Unauthorized Mass Remote Disconnect

2.2.1 Describe Scenario

Description: An authorized individual (defined as an individual who legitimately has privileges to remotely disconnect meters) issues a command or commands that causes the disconnect of a massive number of meters within a short time period.

Assumptions:

- A two-stage meter disconnect process is in place, where business rules such as billing status of a meter and criticality of service are verified before implementing a requested disconnect.
- The user interface provides a warning if a request puts the number of meters disconnected over some threshold in a specified period of time. Stronger enforcement is possible but is not assumed.
- AMI management has implemented a separate role that permit remote meter disconnect requests and credentials are required to access functions under this role.
- Installation of software on the host system for the disconnect function is allowed for users logging in remotely from outside the utility enterprise, only if the users access the system using a virtual private network (VPN) and use strong authentication.
- A log of commands executed by users is kept that can be reviewed to determine which users performed the commands. This log is well-protected against modification or access by unauthorized individuals.

Variants of the scenario: The command to disconnect a large number of meters may be issued intentionally or unintentionally, under circumstances such as the following.

- **Using authorized software:** An authorized insider that is disgruntled, or is social engineered by others, takes the action to disconnect a large number of meters in a short period of time, using authorized software. The insider is able to do so without invoking system protections. This could occur because controls built into the system that limit disconnections of meters due to business rules or power system restrictions can be overridden, or have themselves been modified by an authorized or unauthorized individual, from inside or outside the network where these

configurations reside.

- **Using unauthorized software:** Unauthorized software is installed that directly executes a mass meter disconnect, bypassing the two-stage process. Social engineering is then used to cause an authorized individual to execute this software, and it may be assumed to look authentic. The disconnect can occur because the unauthorized software bypasses power system restrictions that limit disconnections of meters. Installation of malicious software may be carried out by an insider or an outsider that has accessed the utility enterprise network. The outsider may have gained VPN access or direct access to this network.

Physical location for carrying out scenario:

- The authorized individual that triggers this scenario would need to have either direct or remote network access to the systems that host disconnection functions.

- Given the assumptions above, unauthorized software could only be directly installed remotely from outside the utility enterprise network if the threat agent was able to gain VPN access. It is also feasible that advanced malware that performs this install could be transmitted from a remote source without gaining VPN access.

Threat agent(s) and objectives (if applicable, from Table 9 in Appendix D):

- Most likely threat agents, with objective to create disorder:
  - Malicious criminals,
  - Recreational criminals,
  - Terrorists.
- Other threat agents:
  - Activist groups, to protest differences with utility,
  - Economic criminals, for financial gain using extortion against a utility or paid by one of threat agents in the “most likely” list.

Relevant vulnerabilities:

- **Inadequate background checks on employees:** Background checks mitigate the variants of this scenario in which insiders intentionally carry out the meter disconnection, change the configuration that controls disconnect cross-checking, or install unauthorized software to be executed by themselves or other insiders. Background checks might disclose

economic or malicious criminal background, a propensity for revenge against an employer, or susceptibility to certain types of social engineering such as bribery or extortion. Such checks are particularly important for those employees that have responsibility for the cyber systems.

- **Weak enforcement of disconnect thresholds:** A warning that can be overridden in real time by an operator is useful under most circumstances, but is a weak deterrent if the operator has been subjected to social engineering.

- **Configuration that determines checks to be performed before disconnection, is inadequately protected:** For example, the number of meters that can be disconnected in a specific time frame might be modifiable by an individual with operator privileges, and thus susceptible to change by an insider who can also perform the disconnect. Likewise, this configuration might be inadequately protected from outsider access, such as when it is modifiable from a web server on a network with insufficient perimeter controls.

- **Inadequate integrity** controls on field tool or third party installations of software that can control meters.

- **System architecture provides application programming interface (API) for meter disconnection that bypasses power system restrictions.**

  The above two vulnerabilities contribute to the variant of this scenario that rely upon installation of unauthorized software.

Relationship to the National Institute of Standards and Technology Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*, **logical reference model actors:** Software and commands for implementing meter disconnect reside within the Operations domain Actor 29-SCADA or the Distribution domain Actor 16-Field Crew Tools. There may also be third parties that can disconnect meters. In this case the commands reside in the Service Provider domain under 41-Aggregator/Retail Energy Provider, 43-Energy Service Providers or 44-Third Party.

2.2.2 Analyze Impact

a) Possible temporary voltage or frequency fluctuations due to load dropped,

b) Loss of power and customer service situation with customers whose meters are disconnected,

c) Abets criminal or terrorist activity in the area where disconnects occurred,

d) If this failure was caused by installation of unauthorized software, there would be a cost to identify the unauthorized software, remove it, and install the correct software.

The table below shows those general categories of impacts that are most relevant to this scenario, as they relate to the discussion above.

Table 1
Impact Categories for AMI.1

	Impact category	Text reference
1	Public safety concern	[b] [c]
2	Workforce safety concern	
3	Ecological Concern	
4	Financial Impact of Compromise on Utility (excluding #5)	[b]
5	Cost to return to normal operations	[d]
6	Negative impact on generation capacity	
7	Negative impact on the energy market	
8	Negative impact on the bulk transmission system	
9	Negative impact on customer service	[b]
10	Negative impact on billing functions	
11	Damage to goodwill toward utility	[b]
12	Immediate macro economic damage	[b]
13	Long term economic damage	
14	Loss of privacy	
15	Loss of sensitive business information	

Detectability of occurrence:

- There is no common method in use that would immediately pinpoint the occurrence of this scenario.

- The following impacts of this scenario would indicate some failure, but would not provide the cause for these impacts, which might have many different causes.

    - Customer reports of power loss, often handled in an Outage Management System, will indicate a failure to be investigated.

    - However, an Outage Management System is not aware of disconnects, since the disconnected meters still have power.

    - If voltage or frequency fluctuations occurred, a utility would detect these in the time frame supporting by their monitoring of these parameters.

    - Distribution feeder data might be investigated in these cases, and provide clues to the problem if the meters were on the same feeder.

    - Advanced software integrity checks might alert for the presence of unauthorized software, but would not indicate the impact of that software.

    - Otherwise, discovery of unauthorized software would be a manual operation that would commence once this possibility was suspected.

Diagnosing unauthorized software may be more difficult on third party or field equipment.

The following methods used today also might provide clues but would not pinpoint the problem:

- Meter disconnection reports. These events occur in volume, reporting is infrequent and these reports are not routinely individually assessed.

- Data from meters is logged by the AMI head end, including disconnects. However this data is not typically analyzed today (in real time) for this type of event. An example of analysis done today relates mainly to reconnection when bills have not been not paid, and is done infrequently.

Recovery timeline: Recovery consists of:

- Addressing any voltage and frequency fluctuations after the effects of the disconnection
    - The length of time to address voltage and frequency fluctuations will be dependent upon the level of these fluctuations, which in turn depends upon the number of meters disconnected.

- Restoring the disconnected meters to service
    - Reconnection of the meters should take less than an hour.

- If applicable, restoring the correct software.
    - Restoration should take a few hours once the unauthorized software is identified, but may take longer if downloading signed software is required.

2.2.3 Analyze Factors that Influence Probability of Occurrence

Difficulty to achieve attack conditions:

Condition numbers used here are shown in the figures below.

For *Condition (2)*, social engineering of an employee may be expensive and there is a risk of disclosure by an employee if the attempt fails.

For *Conditions (8)* and *(9),* penetration of a network and a host on that network are generally of moderate difficulty if basic controls are in place.

In *Conditions (15) and (17),* the difficulty to install unauthorized software that actually works, will depend upon the complexity of the interfaces of this component with other software on which it depends, and the extent to which public or insider knowledge about the software is known to the threat agent. This is likely to be technically difficult and also detectible with the appropriate controls. The level of security control implemented may

differ among the operations, distribution and service provider domains where this scenario may take place.

No other conditions in this scenario are difficult to achieve, though they are detectible using logs per the **Assumptions** information.

Potential for multiple occurrences: If the utility is able to find the cause for this failure, it is unlikely to occur multiple times. Logging of user names associated with commands will assist in finding the cause for the cases of a disgruntled or social engineered employee. If the cause is unauthorized software, this will be more difficult to diagnose unless specific controls are in place. In that case, there may be multiple occurrences until the utility analyses the problem.

Likelihood relative to other scenarios:

- **A disgruntled or social-engineered employee** has many options open for disruptive actions. A disconnect action that can be tracked directly to a specific employee via a command or reconfiguration log entry is most likely not the most attractive option.

- **For a malicious criminal or terrorist**, the impact of a single attack of this kind is likely insufficient to be worth the effort. If a method were devised to repeatedly execute this attack, such a method could be of interest to these threat agents. This could happen if unauthorized software was installed and remained undetected. Another potential use of this attack by these threat agents would be to mask or intensify the impact of other criminal or terrorist activity occurring in the area where the meters have been disconnected.

- The impact of this attack might meet the goals of a **recreational criminal**. They would likely target third party systems that may have less security controls than the utility itself.

2.2.4 Mitigation

Potential mitigations:

Limit events, specifically the max number of disconnects permitted*:* The system could enforce a hard-coded or configurable maximum number of disconnects over a specified time period. Override may not be permitted, or may only be permitted under a two person rule. If this value is configurable, access to modify the configuration is also protected, from both outsiders and unauthorized

insiders. In particular only individuals with special privileges would be able to access and modify the value. (Condition 3)

Require two-person rule: The system could request confirmation by a second individual before implementing a large number of disconnects. (Condition 3)

Require application whitelisting: Install an *application whitelisting* product on the system that runs the software that ultimately sends the command for disconnection. This solution prevents unauthorized software from executing even if it is successfully installed. (Condition 6)

Check software file integrity, generate alert: Real time or periodic checks on the integrity of critical files such as the disconnect software and threshold configuration files can alert to unauthorized changes. (Conditions 15, 17)

Require strong host password or other credentials for the platform that hosts the disconnect software; *harden platform* that hosts this software. (Condition 12)

If a VPN connection is permitted to the network for the platform that hosts the disconnect software, *create policy* for changing VPN passwords, and *maintain patches* in VPN software. (Condition 12)

Mitigations related to gaining network access, here these apply to the networks hosting the disconnect interface, disconnect software and disconnect threshold configuration (Conditions 8, 13):

- Enforce least privilege to limit individuals with privilege to the network and connected networks
- Isolate network
- Enforce restrictive firewall rules for access to network
- Design for security by limiting connection points to networks that are widely accessible and by limiting number of hosts on same network
- Require authentication to the network
- Enforce least privilege for individuals with access to hosts on the network
- Detect unusual patterns of usage on hosts and network

In this failure scenario, the threat agent may obtain legitimate credentials to modify the disconnect threshold configuration and to modify the disconnect software. General mitigations that apply are found in the common sub tree "*Threat Agent Obtains Legitimate Credentials for* <system or function>." (Conditions 9, 14)

In this failure scenario, social engineering can be used to convince an authorized individual of the need to disconnect a number of meters, or to obtain credentials that permit modifying the configured disconnect threshold or the disconnect

software (Conditions 2, 9, 14). General mitigations related to social engineering apply as shown in the common sub tree "*Threat Agent Uses Social Engineering.*" Potential applications of these mitigations specific to this failure scenario are:

- *Define policy* that must be followed in order to validate a request received to disconnect a large number of meters, or to modify the disconnect threshold (Condition 2)

- *Require multi-factor authentication* such as using a token with a PIN for critical changes such as disconnect software install and disconnect threshold configuration change. It is more difficult to use social engineering to obtain these types of credentials. (Conditions 9, 14)

Verify personnel via background checks*:* Individuals with a criminal background would not be given critical responsibilities, such as the capability to directly implement a meter disconnection request, change the configuration of disconnection-related checks or install software that supports meter operations. (Condition 1)

Organizations involved in scenario and recovery:

- Utility operations, utility field service or third party operations for sending of disconnect command

- IT for software installation or reinstallation at recovery

- Distribution Operations for rebalancing of system load

- Customer Service for interface with affected customers.

2.2.5 References

Source scenario(s): AMI.1 in the present document covers all situations under AMI.1 in [1], except the case of a terminated employee, since they are not “authorized.”

Publications: None identified.

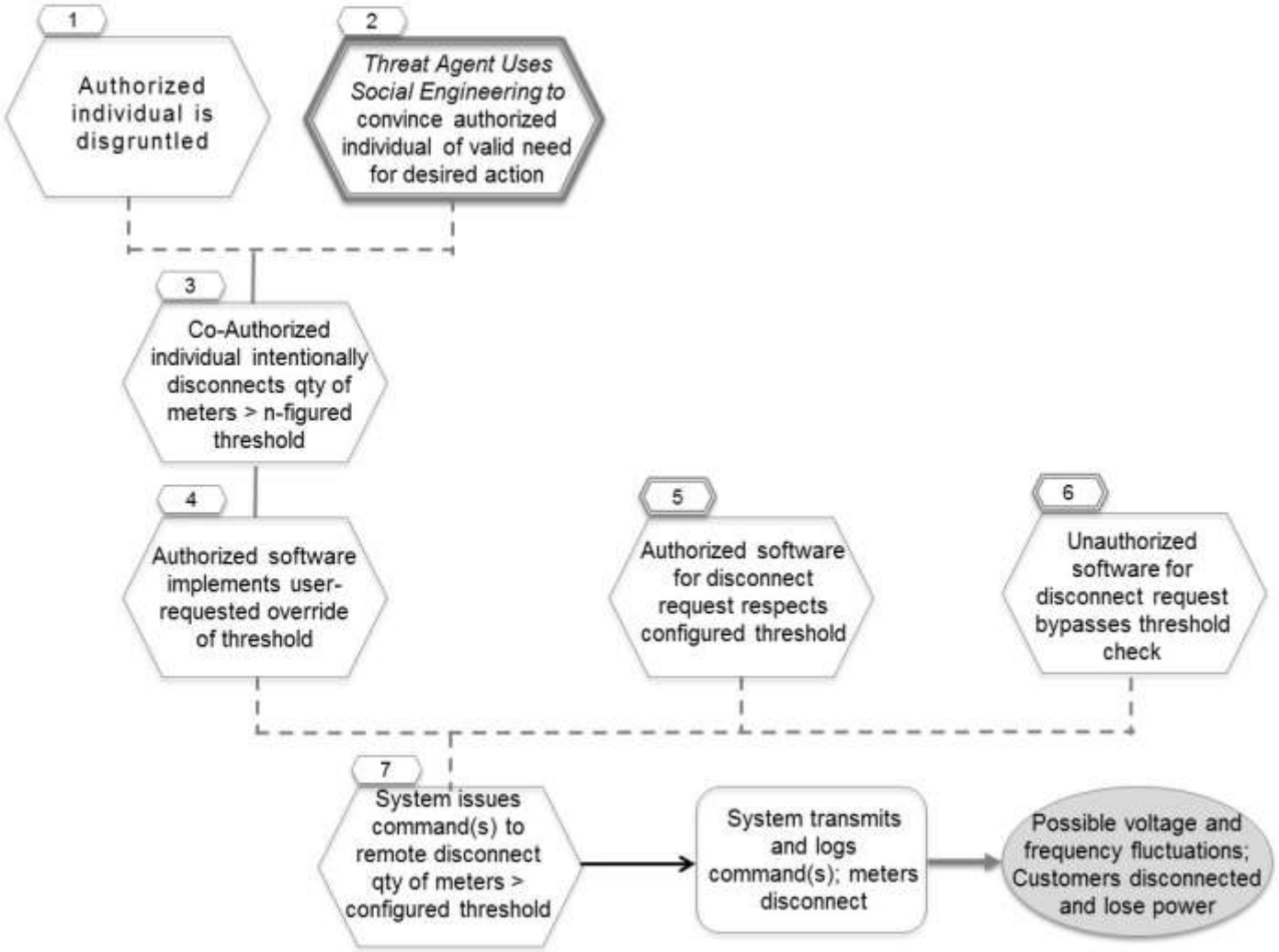

Figure 2
Mass Meter Remote Disconnect by Authorized Individual (1/3)

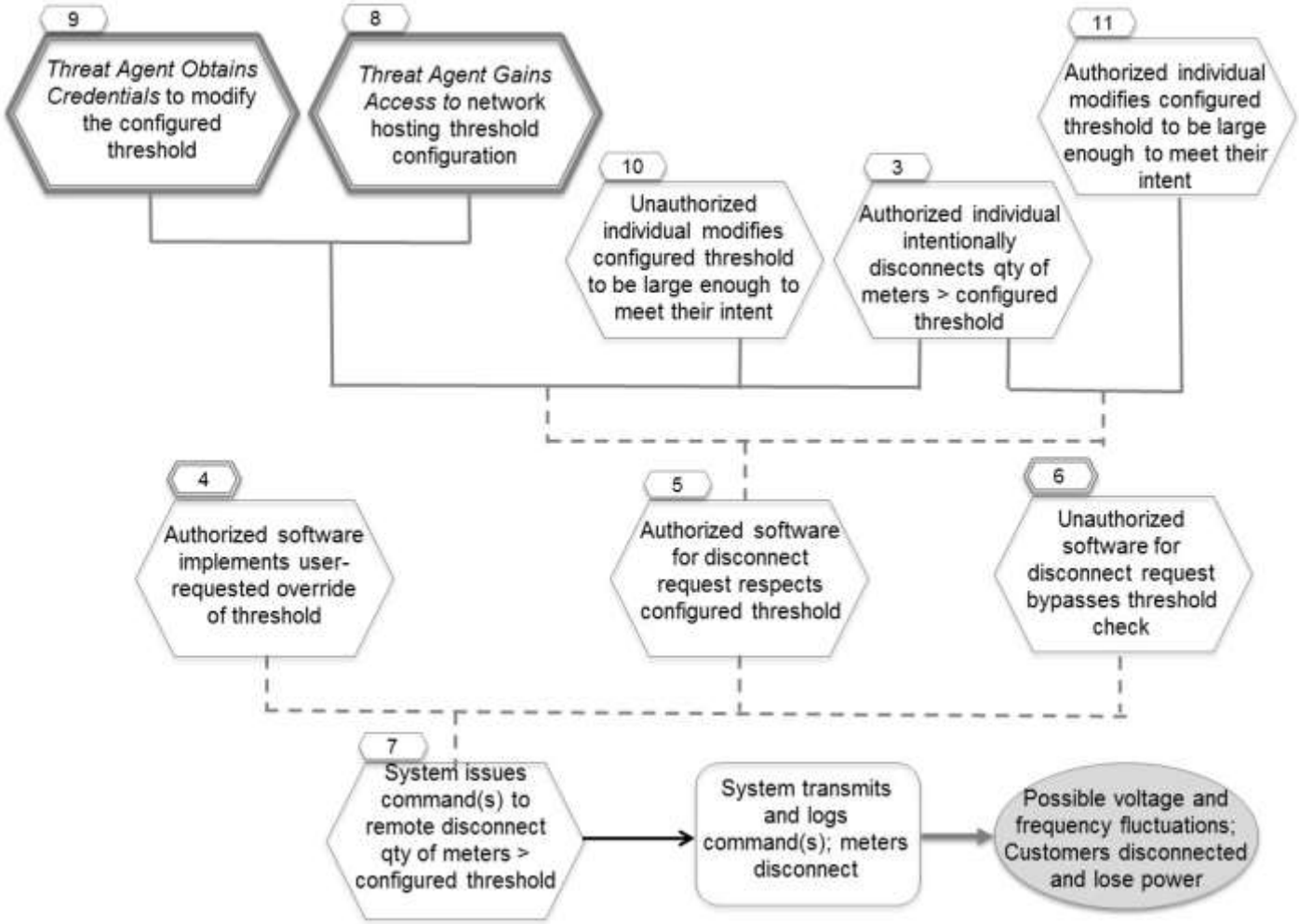

Figure 3
Mass Meter Remote Disconnect by Authorized Individual (2/3)

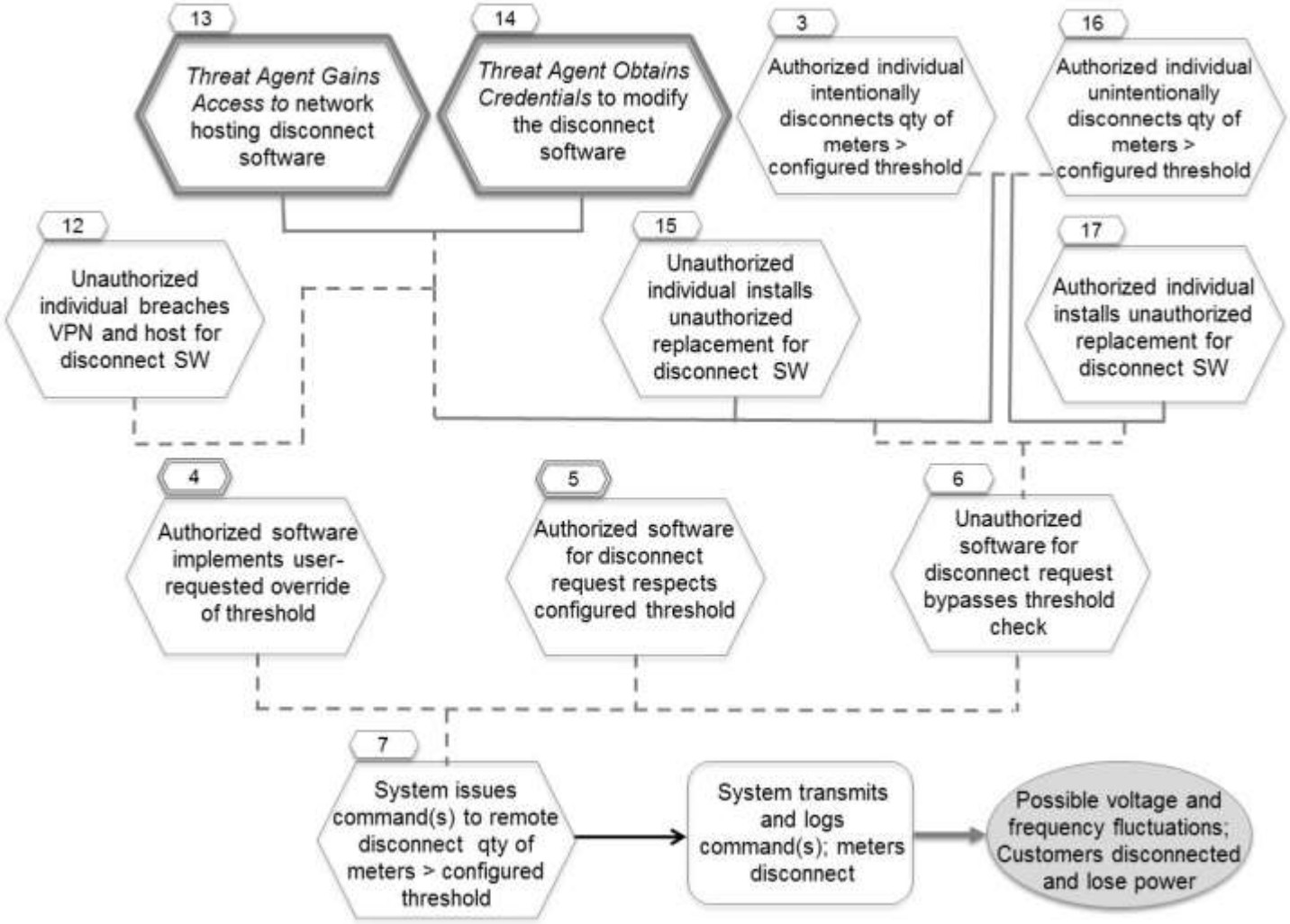

Figure 4
Mass Meter Remote Disconnect by Authorized Individual (3/3)

2.3 AMI.32 Power Stolen by Reconfiguring Meter via Optical Port

2.3.1 Describe Scenario

Description: Many smart meters provide the capability of re-calibrating the settings via an optical port, which may be misused by economic thieves who offer to alter the meters for a fee, changing the settings for recording power consumption and often cutting utility bills by 50-75%. This requires collusion between a knowledgeable criminal and an electric customer, and will spread because of the ease of intrusion and the economic benefit to both parties.

Assumptions:

- Smart meters have an optical port, and provide the capability of re-calibrating the settings that determine how much power is recorded and reported by the meter.
- Both insiders and outsiders have a strong motivation in financial gain.
- There is sufficient information and tools available to teach outsiders how to do this attack.
- Threat agent has physical access to meter.

Variants of the scenario: Reconfiguring the meter's settings for recording power consumption require one of the following types of software and tools:

- **Using authorized software/tools:** An authorized insider that is disgruntled, or is social engineered by others, takes the action to alter meters for a fee, using authorized software. The insider uses vendor software installed on a laptop to speak to the meter, an opticoupler cable from the vendor, and the authorized C12.18 password to access the correct configuration table in the meter.
- **Using unauthorized software/tools:** An unauthorized outsider takes the action to alter meters for a fee, and can use open source software (such as Termineter) installed on a laptop to speak to the meter, and build an opticoupler cable.

Physical location for carrying out scenario:

- The individual that triggers this scenario would need to have physical access to the meter's optical port on the customer premises.

Threat agent(s) and objectives (from Table 9 in Appendix D):

- Most likely threat agents, with objective for financial gain:

- Economic criminals, who may be current or former employees of the meter manufacturer or the utility, or knowledgeable outsiders, to carry out the attack against the target meter,
- Home residents, the buyer of the power recorded by the target meter,
- Business owners, the buyer of the power recorded by the target meter.

Relevant vulnerabilities:

- Inadequate background checks on employees: Background checks mitigate the variants of this scenario in which insiders intentionally change the configuration that records power consumption. Background checks might disclose economic or malicious criminal background, a propensity for revenge against an employer, or susceptibility to certain types of social engineering such as bribery or extortion. Such checks are particularly important for those employees that have responsibility for the cyber systems.

- Weak credentials needed to change the meter settings: Using a shared password across each utilities full deployment.

- Configuration that determines how power consumption is recorded, is inadequately protected: For example, most smart meters offer the capability to re-configure the settings that record and report power usage, via the optical port.
- The C12.18 password is easily obtained by using a logic probe on a meter from that utility region, if the password is stored unencrypted.

- Inadequate protection of the password on field tool or third party installations of software that can reconfigure meters. This allows non-authorized employees to steal the C12.18 password.

Relationship to NISTIR 7628 logical reference model actors: Software and commands for implementing meter re-configurations reside within the Distribution domain Actor 16-Field Crew Tools. There may also be third parties that can reconfigure meters. In this case the commands reside in the Service Provider domain under 41-Aggregator/Retail Energy Provider, 43-Energy Service Providers or 44-Third Party. The meters themselves are Actor 8-Meter.

2.3.2 Analyze Impact

Impact:

a) Loss of revenue due to under billing

- The FBI said the losses incurred by the Puerto Rican electric utility described in the articles under "Publications" below, could reach $400 million annually,
- A series of hacks perpetrated against so-called “smart meter” installations over the past several years may have cost a single U.S. electric utility hundreds of millions of dollars annually, the FBI said in a cyber intelligence bulletin obtained by KrebsOnSecurity.[1]

b) The cost of accurate detection is considerable, since each meter’s settings must be examined to determine if they have been tampered,

c) The cost of resetting the meter configurations, if done remotely, either via the headend or through communication devices capable of talking with the meter, would not be that high for an individual meter. However, a high number of meters would increase that cost.

The table below shows those general categories of impacts that are most relevant to this scenario, as they relate to the discussion above.

Table 2
Impact Categories for AMI.32

	Impact category	Text reference
1	Public safety concern	
2	Workforce safety concern	
3	Ecological Concern	
4	Financial Impact of Compromise on Utility (excluding #5)	[a]
5	Cost to return to normal operations	[b] [c]
6	Negative impact on generation capacity	
7	Negative impact on the energy market	
8	Negative impact on the bulk transmission system	
9	Negative impact on customer service	[a]
10	Negative impact on billing functions	[a]
11	Damage to goodwill toward utility	
12	Immediate macro economic damage	
13	Long term economic damage	
14	Loss of privacy	
15	Loss of sensitive business information	

Detectability of occurrence:

- Per security blogger Brian Krebs[1], The FBI stated "The altered meter typically reduces a customer's bill by 50 percent to 75 percent. Because the meter continues to report electricity usage, it appears be operating normally. Since the meter is read remotely, detection of the fraud is very difficult. A spot check of meters conducted by the utility found that approximately 10 percent of meters had been altered."

Diagnosing invalid settings may be more difficult on third party equipment, due to the utility's probable lack of access to third party passwords, software, and tools.

The following methods used today might provide clues but would not pinpoint the problem:

- Historical usage trends could show significant changes in electricity use, although there are valid reasons for changes such as
  - Change in number of residents,
  - Installation of energy saving appliances,
  - Improved weatherization, etc.

Recovery timeline: Recovery consists of:

- Restoring the meters to accurate recording of energy consumption
  - Resetting of the meters should take less than an hour, and can be done remotely.

2.3.3 Analyze Factors that Influence Probability of Occurrence

Difficulty of achieving conditions:

Condition numbers used here are shown in the figure below.

For *Condition (1)*, the outsider can easily obtain the C12.18 password off the hardware of any single meter from that utility region by using a logical probe. Particularly if there is a shared password across a utility's full deployment, the password would be easy to discover. It can also be obtained from any field

[1] http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/

technician, or off the field technician's laptop that usually has it saved in the software configuration.

For *Condition (2)* software and tools are easy and cheap to obtain or build, and instructions are now on the Internet. An optical probe can be built for $30 using instructions available online.

No other conditions in this scenario are difficult to achieve, though they are hard to detect.

Potential for multiple occurrences: This attack has already been discovered to be widespread in one major US utility, covering about 10% of installed smart meters. Some instances of the same attack have also been reported in other regions.

Likelihood relative to other scenarios:

"These individuals are charging $300 to $1,000 to reprogram residential meters, and about $3,000 to reprogram commercial meters," the alert states.[1]

- **A disgruntled employee** has many options open for disruptive actions. A reconfiguration action that can be tracked directly to a specific employee via a command or reconfiguration log entry is probably not the most attractive option. The ease of access via unauthorized tools along with the ability to gain economic value via collusion with customers is a strong motivator.

- An **economic criminal** can gain easy access meters to perform this attack, and the financial motivation is strong.

- For a **malicious criminal or terrorist**, the impact of a single attack of this kind is probably insufficient to be worth the effort. The long-term economic damage to the utility is unlikely to be a sufficient motive.

- The impact of this attack might meet the goals of a **recreational criminal**.

2.3.4 Mitigation

Potential mitigations:

See common sub tree *Threat Agent Obtains Legitimate Credentials* (Condition 1)

Require multi-factor authentication: for firmware updates (Conditions 2, 4, 5)

Detect unusual patterns: of energy usage on smart meters (all utilities have some type of revenue protection scheme, but these may not be sufficient) (Condition 6)

Check software file integrity (digital signatures) on code files to validate firmware updates before installation*:* Real time or periodic checks on the integrity of critical files such as configuration parameters that impact recording and reporting of power consumption can alert to unauthorized changes. (Condition 6)

- In this failure scenario, the threat agent may obtain legitimate credentials to modify charging/reporting parameters on meter via optical port. General mitigations that apply are found in the common sub tree "*Threat Agent Obtains Legitimate Credentials for* <system or function>", with applicable conditions to that sub tree numbered: *Design for security* by using strong passwords (Condition 2)

- *Design for security* by not recording passwords in log files (Condition 3)

- *Test for malware* on user workstations (Condition 4)

- *Design for security* by not sending passwords in the clear over the network (Condition 4)

- *Encrypt communication paths* on the network (Condition 4)

- *Protect against replay* on the network (Condition 4)

- *Design for security* by using strong security questions and protect answers (Condition 5)

- *Require multi-factor authentication* such as using a token with a PIN (Condition 6)

- *Define policy* regarding reporting and revocation of missing tokens (Condition 6)

Organizations involved in scenario and recovery:

- Utility operations, utility field service or third party operations for configuring the meter's power consumption settings.

- Customer Service for interface with affected customers.

2.3.5 References

Source scenario(s): AMI.32 in [1] is the short version of this detailed scenario.

Publications:

- **http://www.nbcnews.com/id/47003851/ns/technology_and_science-security/t/smart-meter-hacks-cost-hundreds-millions-annually-fbi-says/**

- **http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/**

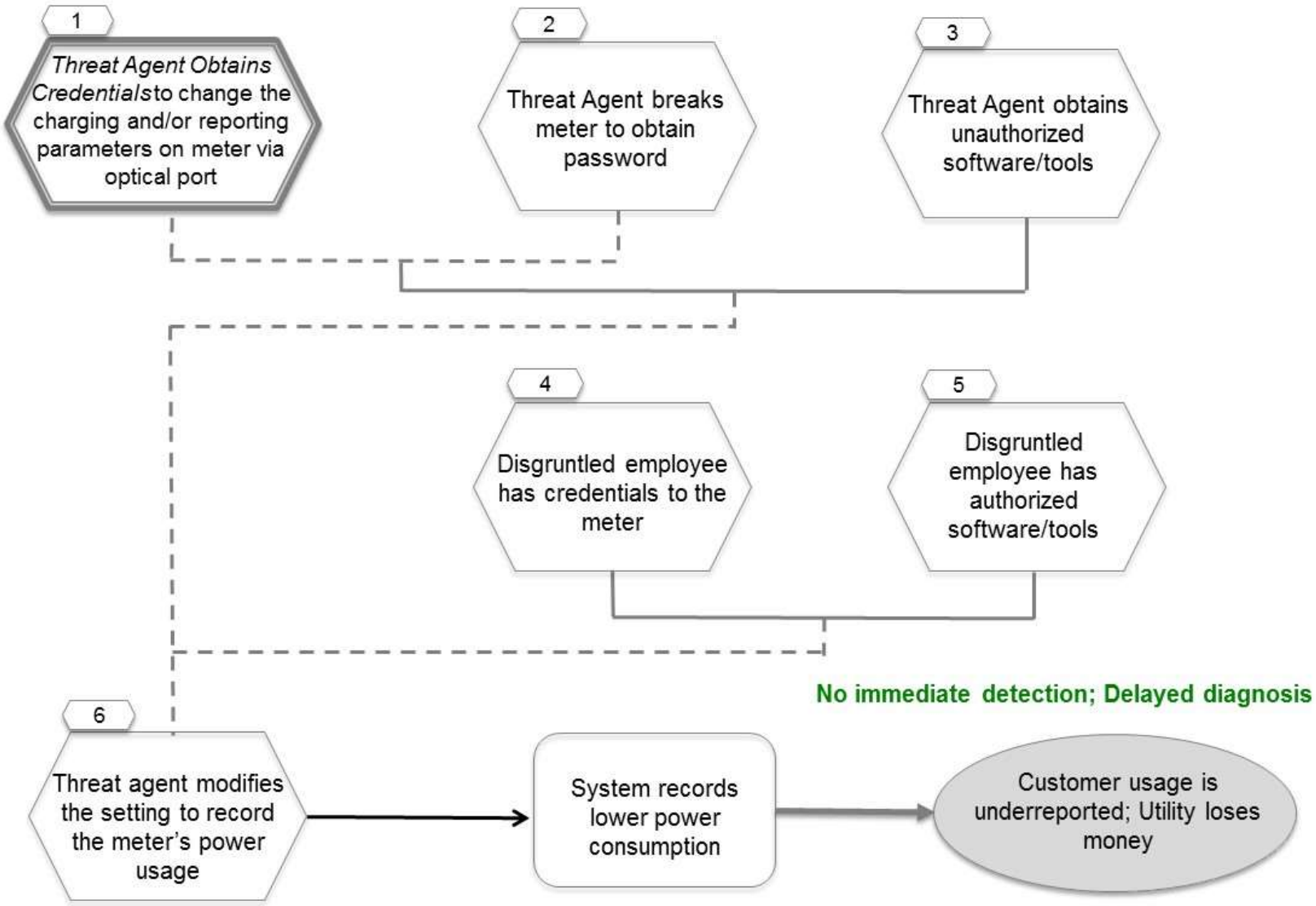

Figure 5
Power Stolen by Reconfiguring Meter via Optical Port

2.4 DGM.11 Threat Agent Triggers Blackout via Remote Access to Distribution System

2.4.1 Describe Scenario

Description: A threat agent performs reconnaissance of utility communications, an electrical infrastructure, and ancillary systems to identify critical feeders and electrical equipment. The threat agent gains access to selected elements of the utility distribution management system (DMS) - that includes all distribution automation systems and equipment in control rooms, substations, and on pole tops - via remote connections. After gaining the required access, the threat agent manufactures an artificial cascade through sequential tripping of select critical feeders and components, possibly causing automated tripping of distribution level generation sources due to power and voltage fluctuations. A blackout of varying degree and potential equipment damage ensues. Remote connections to the DMS might be established using a variety of methods or combination of methods.

Assumptions:

- Remote connections for vendor access are tightly controlled (using a VPN) and physically disconnected manually when not in use; however, no formal procedure exists for disconnecting vendor access and unintentional sustained connections do occur

- DMS/supervisory control and data acquisition (SCADA) network is segregated from any corporate or public networks; however, DMS/SCADA is not completely air-gapped since a one-way connection exists to the corporate LAN for data gathering purposes

- Some DMS/SCADA communications run over leased fiber cables and communication equipment that are shared with other entities. Communications are segregated either by devoting fiber strands to entities or through use of VLANs

- Electrical infrastructure information (e.g., distribution system and substation one-line diagrams, equipment information, equipment location, etc.) and DMS/SCADA system documents (e.g., networking diagrams, communication equipment, communication protocols, etc.) are considered proprietary and protected from unauthorized disclosure; however, this information resides on corporate systems and networks that are more accessible from public networks

- Data logging is performed on DMS/SCADA systems, recording, at a minimum, the time and user's identity of all log-ins and control commands initiated (e.g., breaker close, connecting capacitor banks, configuration changes, etc.)

- Network intrusion detection is not present on the control system network; however, it is present on the corporate network

- Some utility linemen and communication personnel have laptops that permit connections to DMS/SCADA field equipment, communication devices (switches, head-ends, etc.), and DMS systems over the control system network (not from public networks)

- Company computers and systems require password authentication; however, complexity requirements are moderate and two factor authentication is not used

- Distribution management system communications are unencrypted and defense in depth practices have not been implemented

- The DMS/SCADA system is monitored 24/7 by dedicated control system personnel

- The control system network is flat

- Distribution system is largely radial, though some tie lines do exist at the end of select laterals

Variants of the scenario: Remote connections for reconnaissance and execution of this attack can be obtained by a number of methods.

- A disgruntled or socially engineered employee provides remote access to the DMS for the threat agent or directly carries out the attack

- Using a lost, stolen, or otherwise acquired utility linemen's laptop to access the DMS directly: requires company laptop configured for employee remote connections to DMS, username and password to unlock computer, username and password for access to the DMS (if different from the computer), access to physical communication channel (e.g., switch port, wireless connection, etc.)

- Compromising an active or unintentionally connected remote maintenance connection used for vendor DMS application maintenance: requires knowledge of when the remote vendor connection is active, capability to access the

connection, credentials for log-in or some way to subvert credentials/connection

- Taking advantage of an accidental bridged connection to the internet due to DMS misconfiguration: requires knowledge of an accidental DMS internet connection (possibly through a port scan that was not detected by cybersecurity countermeasures), administrator privileges on the DMS (possibly requiring a stolen username and password or introduction of malware)

- Subverting distribution control communications directly: requires intimate knowledge of utility communication protocols, skilled and clever means of subversion (e.g., breaking encryption or authentication, access to physical communication medium (fiber, copper, wireless spectrum, etc.)

- Implanting, swapping, or otherwise covertly implementing removable media into the DMS system via a control system employee. The removable media contains malware to facilitate remote unauthorized DMS access. This requires sophisticated malware on removable media, detailed knowledge of the DMS system, and clever means of getting removable media into the DMS system

- Supply chain attack on DGM equipment (i.e., relays, RTUs, servers, communication equipment, etc.) that installs rootkits on the devices to facilitate outside access to DGM network and equipment: requires physical access to devices during design, manufacturing, storage, or transportation, custom developed malware

- Subversion of TCP/IP layers on shared networking equipment (e.g., changing VLAN configurations on communication equipment) to gain access to DGM network: requires physical access to shared networking communication equipment, login credentials to obtain privileged access networking on equipment

Physical location for carrying out scenario:

- Physical access to the communication infrastructure will be required (e.g., fiber cables, copper land lines, wireless, etc.) for direct subversion of communications

- Access to manufacturing, commissioning, storage, or transportation facilities (e.g., factories, warehouses, etc.) will be required for supply chain attacks,

- Physical access to shared networking facilities (e.g., switching stations, area distribution nodes, etc.) is likely required for attack on shared communication infrastructure, though remote connections to shared equipment may be possible

depending on the service provider

- Physical access to vendor communication or datacenter facilities may be required for subversion of vendor communications

- If the conditions are right, this attack could also be carried out remotely over the Internet

Threat agent(s) and objectives

- Most likely threat agents, with the objective to create disorder:
    - Malicious criminals or criminal groups
    - Recreational criminals
    - Activist groups, to protest differences with utility
    - Terrorists
    - Nation States
- Malicious criminals, with the objective to camouflage or enable other criminal activity,
- Other threat agents:
    - Economic criminals, for financial gain using extortion against a utility or paid by one of threat agents in the “most likely” list

Relevant vulnerabilities:

- Inadequate protection of linemen and maintenance personnel company laptops used for remote connections to DMS from loss, theft, or abuse, and from misuse when not under control of authorized individuals, These company laptops are used for remote connection to the DMS,
- Weak protection of specific control system access information
- Weak authentication on SCADA/DMS systems and equipment
- Weak passwords
- Inadequate protection of proprietary infrastructure and SCADA/DMS information,
- Human error in control center configuration (e.g. Ethernet cable plugged into wrong port)
- Violation of DGM security policies (e.g., plugging in USB drives in DMS computer)
- Remote access to DMS/SCADA for vendors to perform application maintenance and troubleshooting

- Distribution control communications sent in cleartext
- Lack of defense in depth in DGM network
- Distribution networks are more radial in nature than meshed, making network reconfiguration to restore power more difficult
- Weak physical security of communication and personnel equipment, including access to shared communication hardware and facilities
- Little to no review of communication logs
- Little to no forensics capability in DGM network
- Sharing communication equipment and infrastructure with other entities

Relationship to NISTIR 7628 logical reference model functions: The Operations domain function 27-Distribution Management System is the suite of application software that supports electric system operations, including online three-phase unbalanced distribution power flow, switch management, and volt/VAR management. The DMS also communicates with the Operations domain function 29-SCADA, providing the threat agent with access to that software and commands for controlling compliant devices. These devices are represented as Distribution domain function 15-Distribution RTUs or IEDs.

2.4.2 Analyze Impact

Impact:

[a] Loss of customer power might spread to entire service area

- Depending on the sequence of the feeders tripped, timing of attack, severity of cascading effects (if any), and utility response, power loss can range from a select feeder supplying a town, portions of a suburb, a large city, or a large geographic area

[b] Possible customer and utility equipment damage

- Voltage sags and swells could damage customer electronic equipment
- Shifting electrical load might overload transformers and switchgear or blow fuses,
- Oscillatory behavior might damage distribution level generation

[c] Loss of customer or employee private information

- Utility employee names, home address, date of birth, vehicle registration plate number, email address, social security numbers, etc.

[d] Disclosure of the names of personnel, proprietary utility documents or information

- Precise location of critical feeders
- Manufacturer and model numbers of equipment
- Network architecture of DMS communications
- Installed operating systems and software, version numbers, patch levels
- Password requirements and cyber security countermeasures
- Policy and procedure documentation

The table below shows those general categories of impacts that are most relevant to this scenario, as they relate to the discussion above.

Table 3
Impact Categories for DGM.11

	Impact category	Text reference
1	Public safety concern	
2	Workforce safety concern	
3	Ecological Concern	
4	Financial Impact of Compromise on Utility (excluding #5)	[a]
5	Cost to return to normal operations	[a] [b]
6	Negative impact on generation capacity	
7	Negative impact on the energy market	
8	Negative impact on the bulk transmission system	
9	Negative impact on customer service	[a] [b]
10	Negative impact on billing functions	
11	Damage to goodwill toward utility	[a]
12	Immediate macro economic damage	[a]
13	Long term economic damage	
14	Loss of privacy	[c]
15	Loss of sensitive business information	[d]

Detectability of occurrence:

- Detection of reconnaissance of DMS/SCADA and infrastructure information residing on corporate and control system networks may be possible given the presence of a network intrusion detection system (IDS) on the corporate side, the small landscape of the control system network, and data logging conducted on both; however, adversaries may conduct reconnaissance of electrical infrastructure by visually inspecting utility infrastructure (e.g., driving to substations and estimating line capacities, identifying equipment, etc.) which is more difficult to detect

  - Control systems that support the DMS are highly deterministic, so anything out of the ordinary would likely be detected and investigated

- A breaker trip, as well as the type of trip (e.g., manual trip, directional overcurrent trip, undervoltage trip, etc.) can usually be detected very quickly by control system personnel monitoring the DMS; however, the root cause of the trip (e.g., (fallen tree branch, equipment damage, intentional sabotage, etc.) takes more investigation, such as deploying trucks to survey feeders and equipment, connecting to relays to view logged events, etc.

- Software alterations and malware on DGM control equipment would be difficult to detect, especially those introduced in the supply chain

- In the case of reduced situational awareness, customers may notify utility of any loss of power due to an attack by telephone

- If privileged access to relays is obtained by adversary, logs from relays could be wiped or alerts to the control center may be disabled, making detectability more difficult

Recovery timeline: Typical recovery consists of:

- First 1-3 hours from disturbance (Preparation Actions)
  - Determination of information that is required to reconstruct the sequence of events, including attribution
  - Review standard restoration plans
  - Evaluate the post-disturbance system
  - Analyze the CIS, monitor the DMS and dispatch maintenance workers to determine the cause and extent of the outage
  - Develop strategy for rebuilding the distribution network
  - Supply critical loads with the initial sources of power available

- 1 - 24 hours from disturbance (System Restoration)
  - Damaged components (if any) are repaired or replaced
  - Skeleton distribution paths are energized
  - Collect information and impound equipment as necessary

- Post Recovery
  - Review data logs on DMS, relays, phasor measurement units (PMUs), and communication equipment to determine:
    - sequence of events

- how attacker gained access
- mitigations to prevent attack from happening again

2.4.3 Analyze Factors that Influence Probability of Occurrence

Difficulty of conditions:

Condition numbers used here are shown in Figures 6-9 below.

For *Condition (2) and Condition (11)*, social engineering of an employee may be expensive and there is a risk of attribution if the attempt fails; however, social engineering of employees is not difficult.

For *Condition (7),* acquiring a company control laptop through theft may be trivial if the hardware is left unattended (e.g., being left in a company vehicle over lunch); however, if laptops and control equipment are left in locked boxes when unattended, acquisition is more difficult. Acquiring a company control laptop and credentials from a willing utility employee (or one that is amenable to coercion) can be easily accomplished through social engineering, bribery, blackmail, persuasion, or by force.

For *Condition (8),* knowing the exact moment that a vendor remote connection was inadvertently left connected will generally require substantial time and patience, depending on the frequency of remote vendor connections and the likelihood of control system personnel to forget to physically disconnect remote connections, but it is not difficult.

For *Condition (9),* scanning the utility network for accidental bridged connections to the Internet or corporate networks is, by itself, trivial; however, actually finding such a connection is exceptionally rare.

For *Condition (10),* connecting to the DMS by directly subverting the DMS communications is generally difficult, but can range in difficulty depending on the mix of communication mediums used. For example, subverting wired communications is more difficult than wireless communications, since access to the communication medium may be more difficult for wired communications.

For *Condition (11),* stealing or cracking employee credentials can be accomplished quickly and easily with the right password cracking equipment. If passwords are stored in databases as a hash, acquiring the hash values in the databases is moderately difficult.

For *Condition (12),* compromising an active remote vendor VPN connection for the purpose of a man-in-the-middle (MITM) attack is likely very difficult. Such an activity would require advanced capabilities and a high level of skill and knowledge.

For *Condition (4),* altering relay settings on its own is a very trivial task, given that relay software and user manuals are readily available by manufacturers, often at no cost. More difficult, is obtaining relay passwords (if they exist) that are not default passwords.

For *Condition (19),* spoofing telemetry data is moderately difficult, given the knowledge and skill required; however, many infrastructure measurement devices can be easily altered by physical stimuli if physical access to the devices can be achieved.

No other Conditions in this scenario are difficult, though they are detectible using logs per the **Assumptions** information.

Potential for multiple occurrences: If this attack can be achieved once, it can be done multiple times; however, depending on the attack vector, lessons learned will make repeat occurrence on the same system less likely.

Likelihood relative to other scenarios:

- **A disgruntled or social-engineered employee** carrying out the attack is perhaps a utility's most vulnerable means of attack since the insider threat is difficult to defend against; however, this scenario is less likely to occur since logging and the immediate detection of breaker trips would limit the impact of the attack.

- **For a malicious criminal or terrorist**, the impact of a single attack is likely severe enough to warrant considerable interest. The higher level of skill and resources required for this attack is commensurate with established criminal or terrorist groups that have vast resources and highly skilled members. Additionally, the possibility of a large geographic area losing power might support a terrorist or criminal group agenda of causing significant financial harm.

- This attack might meet the goals of a **recreational criminal**. It is a challenge with a clear objective, and the attacker will remain anonymous; however, the difficulty

of the attack and the high level of skill and resources required would generally limit their involvement.

2.4.4 Mitigation

Potential mitigations:

- *Require strong passwords* with complexity requirements or *require two-factor authentication* for company devices and systems (Condition 14, 16)
- *Require strong passwords* that are different for each relay (Condition 18)
- *Train personnel* (operations and maintenance employees) on handling and protecting company computing devices securely, requirements on storing devices, and reporting instructions in cases of loss, theft, and system recovery activities (Condition 7)
- *Restrict remote access* of vendor connections (e.g. physically disconnect remote connections when not in use or incorporating timed physical disconnects of remote connections) (Condition 8)
- *Restrict remote access* of vendors by installing patches and updates via physical media mailed by vendor, instead of allowing remote vendor access (Condition 16)
- *Encrypt* communication paths for distribution control communications (Conditions 8, 10, 11, 14, 16, 19)
- *Restrict physical access* to communication equipment in shared locations (Conditions 10, 19)
- *Require intrusion detection* on the DGM networks and hosts (Condition 16)
- *Minimize functions* on control system equipment by disabling all unused ports (Conditions 9, 10)
- *Check integrity* of firmware, applications, patches and updates (Condition 17)
- *Verify personnel* by performing thorough background checks on employees (Condition 1)
- In this failure scenario, social engineering can be used to convince an authorized individual of the need to take a specific DMS/SCADA action, or for a threat agent to obtain network access and DMS credentials (Conditions 2, 11, 13). General mitigations related to social engineering apply as shown in the common sub tree "*Threat Agent Uses Social Engineering.*"
- The following mitigations have not been mapped to a specific condition in the attack tree in this draft:

- *Define policy* that requires prior notification and mutual consent of all participating for all modifications to be made on any shared communication devices *Require two-person rule* to verify correct DMS configuration
- *Isolate networks* (distribution control networks) by segmenting the distribution control network itself
- Mitigations related to loss of proprietary business information during this occurrence of this scenario:
  - *Train personnel* to protect company information and documents from unauthorized disclosure
  - *Define policy* on handling sensitive information. This includes substation one-line diagrams, equipment information, communication architectures, protection schemes, load profiles, etc.

Organizations involved in scenario and recovery:

- Utility operations, utility field service or third party operations for sending disconnect command
- IT for closing off access to attacker
- Distribution Operations for rebalancing of system load
- Customer Service for interface with affected customers

2.4.5 References

Source scenario(s): DGM.11 in [1].

Publications: None.

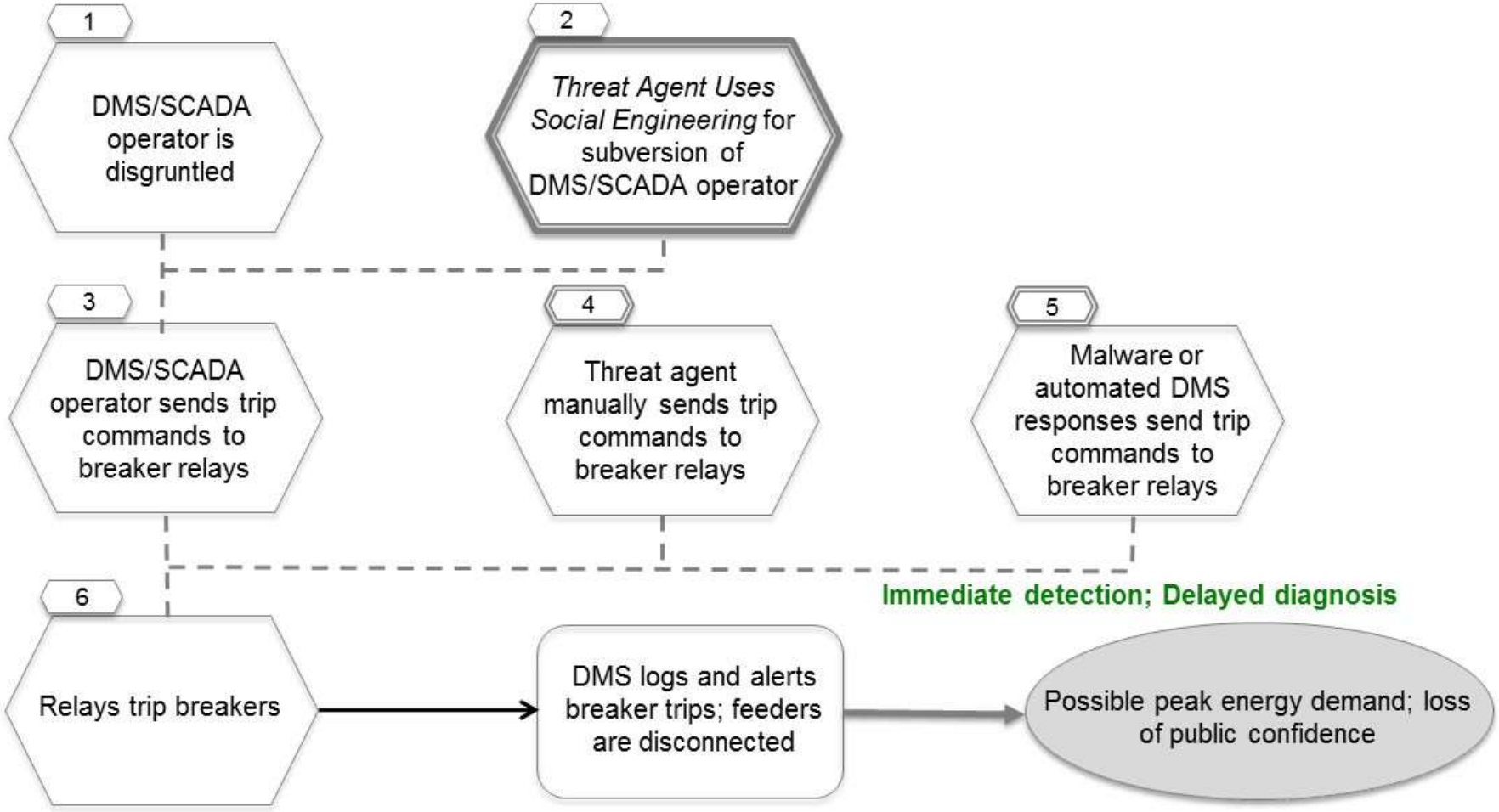

Figure 6 -
Threat Agent Triggers Blackout via Remote Access to Distribution System (1/4)

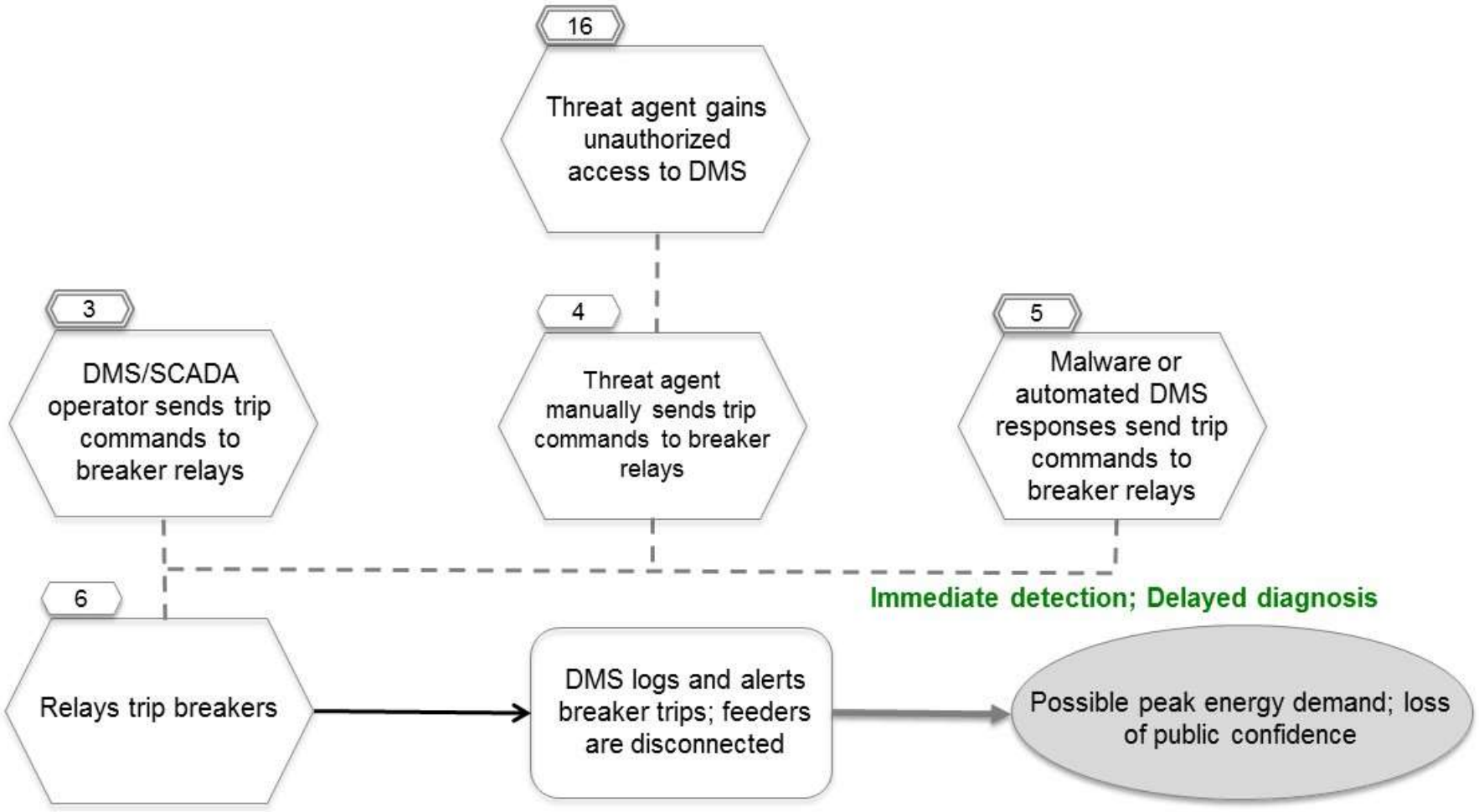

Figure 7
Threat Agent Triggers Blackout via Remote Access to Distribution System (2/4)

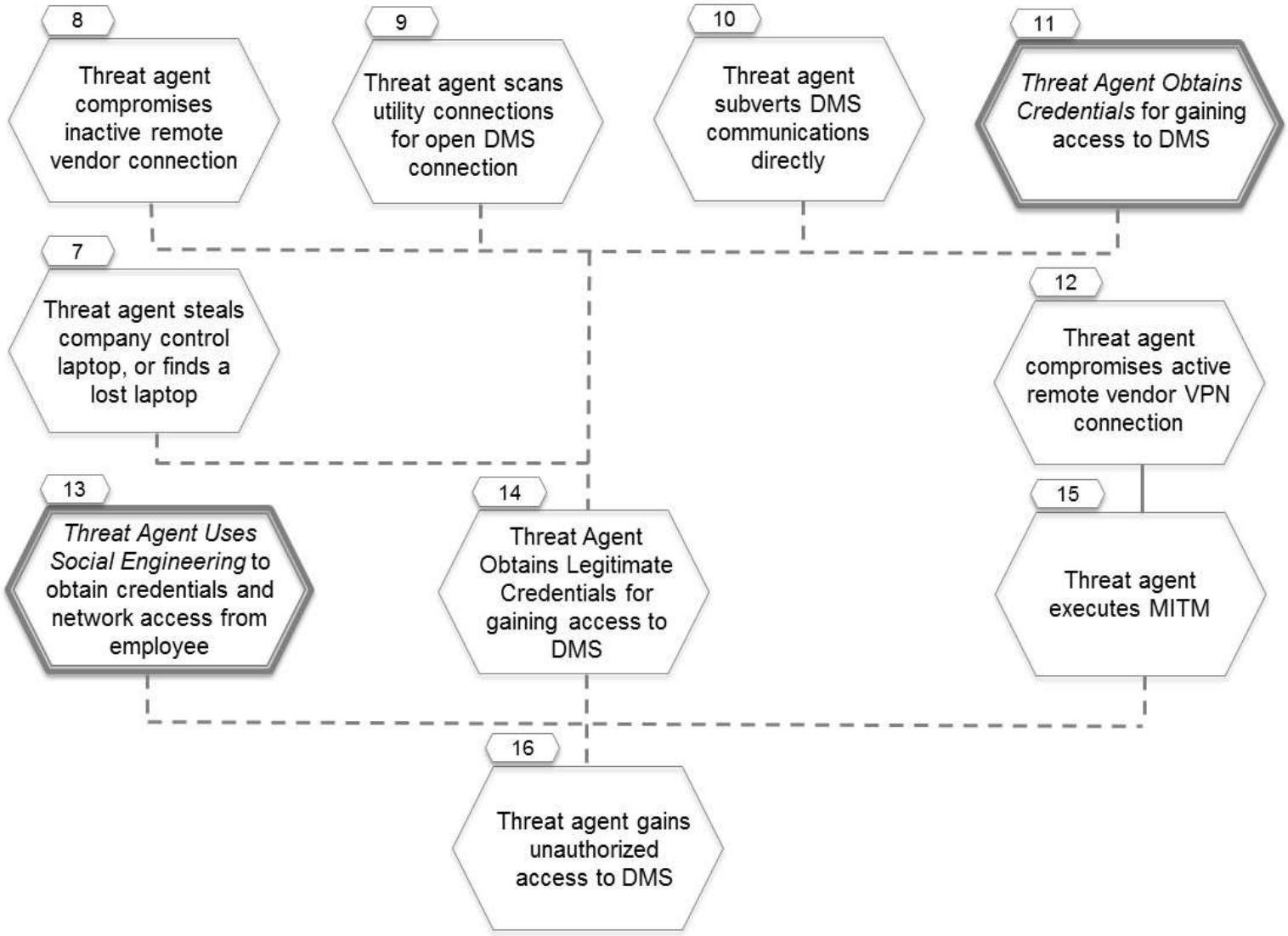

Figure 8
Threat Agent Triggers Blackout via Remote Access to Distribution System (3/4)

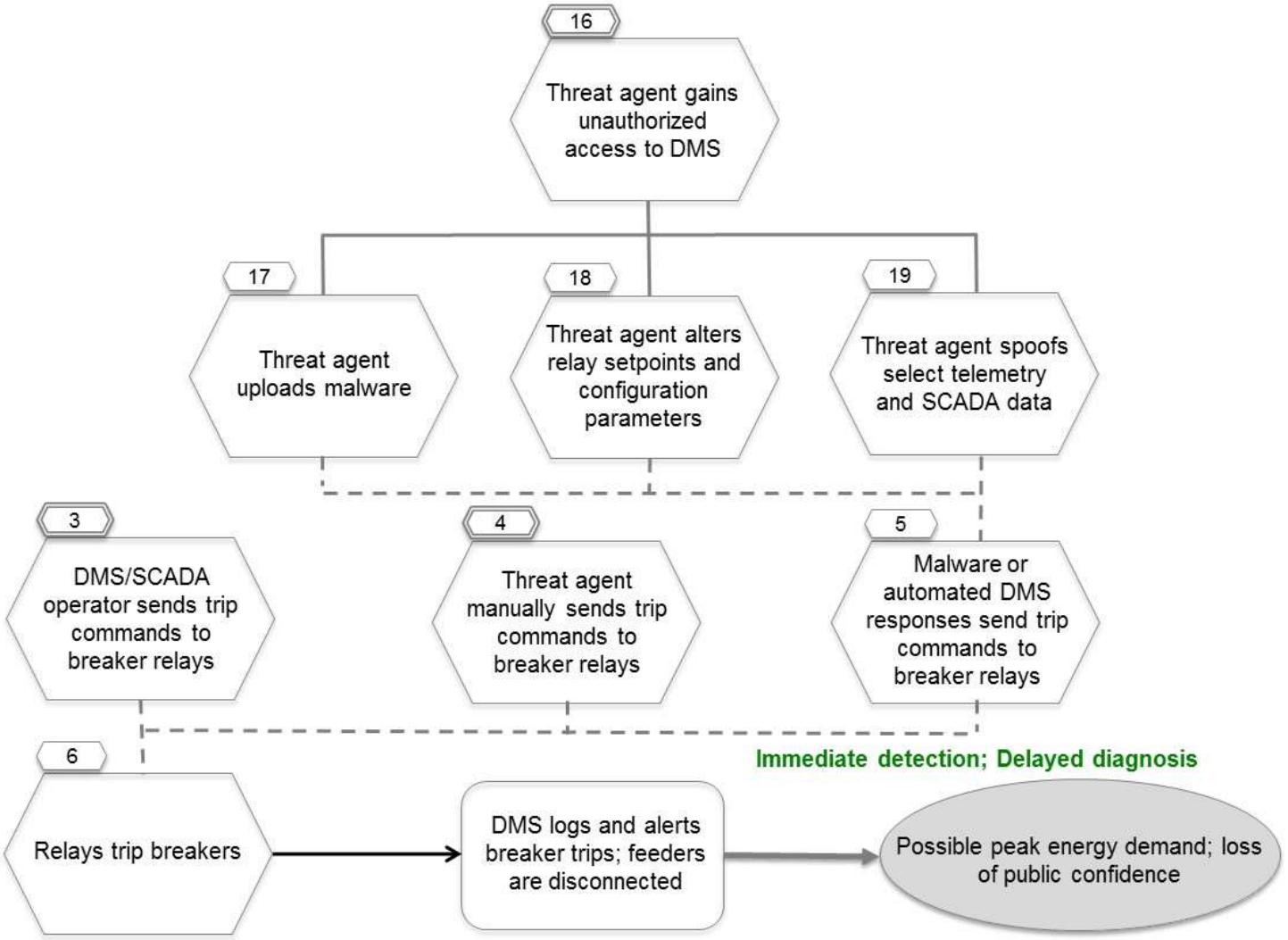

Figure 9
Threat Agent Triggers Blackout via Remote Access to Distribution System (4/4)

2.5 GEN.1 Threat agent adds spurious trip parameters on remotely located plant support equipment and trips unit offline

2.5.1 Describe Scenario

Description: A threat agent gains physical access to a river water pump house, connects a laptop to the local controls network, and adds a time-delay trip to the circulating water pumps triggered off of a normal value. This causes loss of cooling water flow resulting in the loss of condenser vacuum tripping the turbine and causing the plant to be tripped offline.

Assumptions:

- The pump house equipment utilizes a local networked, microprocessor-based relay control system to control pump house equipment – including trips.
- The threat actor has knowledge of power plant operations and knowledge of the access parameters.
- The time-delay is triggered off of an intake level transmitter value within normal limits that adds a random factor to the trip frequency.
- The main control room system access to the pump house is limited by design to only allow start and stop commands to equipment and to receive generic trouble alarms (e.g., motor trouble, high or low water levels, high differential pressure).
- The pump house is located outside of the inner security perimeter of the plant and it not actively guarded.
- Surveillance is limited to periodic spot checks once-per-shift to check for leaks and obvious mechanical issues.
- Pumps are single speed pumps in standard configuration.
- Equipment controls use no passwords or default passwords.
- A backup copy of the pump house controls logic has been kept off-site, but it may not include all the tuning and setpoint adjustments.

Variants of the scenario:

- Change the local set-point to cause pumps to trip unnecessarily without the time delay.
    - Changing a set-point would be easier to detect and remediate.
- Disabling the pump trip on high differential pressure and disabling the travelling screens could potentially damage the screens and pumps.
    - The effects of taking this action would be more gradual and detected earlier under plant operations and monitoring than the original. However, if downstream indications were not properly monitored – the plant could be down for a longer period of time.
- Install a small computer to provide remote access to the pump house network.
    - By leaving a device behind, the threat agent could have remote access and perform commands at will. However, the probability of detection would be higher and the threat agent would be leaving behind more evidence.
- Install the pump house within the security parameter.
    - Access would still be available by water, thereby, bypassing the traditional physical security portals.
- Repeatedly start and stop the motor.
    - This would cause more potential damage to the motor than the original scenario.

Physical location for carrying out scenario:

- Physical access to the pump house assets is required to make these adjustments.

Threat agent(s) and objectives

Possible threat agents could include:

- Malicious Criminals
    - Given the domain knowledge that is necessary, a disgruntled employee or a contractor is a strong possibility.

- Terrorists
  - Nation-state actors: given that all thermal plants have cooling water, a coordinated attack on several sites by multiple sophisticated actors could have a grid-level impact.

Relevant vulnerabilities:

- *Physical access may be obtained by unauthorized individuals* as many sites have pump houses well outside of the security perimeter of the plant
- *System relies on credentials that are easy to obtain for access* to make configuration changes to the equipment controls,
- *System permits unauthorized changes* to the configuration,
- *Commands or other messages may be inserted on the network by unauthorized individuals* resulting in unauthenticated changes to sensitive parameters

Relationship to NISTIR 7628 logical reference model functions: The generation domain includes actor 1: Plant Control System – Distributed Control System (DCS). This is included in Logical Interface Category (LIC) 6. This is a local control system at a bulk generation plant. The focus of this failure scenario is having physical access to the control system and launching an attack.

2.5.2 Analyze Impact

Impact:

- [a] Inadequate cooling water to the condenser will lead to a loss of vacuum that will trip the turbine.
- [b] Improper cooling water levels could damage the condenser and turbine.
- [c] Lost generation.
- [d] Time and expense to diagnose problem.
- [e] Plant thermal cycle gives greater opportunity for boiler tube leak.

The table below shows those general categories of impacts that are most relevant to this scenario, as they relate to the discussion above.

Table 4
Impact Categories for GEN.1

	Impact category	Text reference
1	Public safety concern	
2	Workforce safety concern	
3	Ecological Concern	
4	Financial Impact of Compromise on Utility (excluding #5)	
5	Cost to return to normal operations	[a] [d]
6	Negative impact on generation capacity	[a] [c]
7	Negative impact on the energy market	
8	Negative impact on the bulk transmission system	
9	Negative impact on customer service	
10	Negative impact on billing functions	
11	Damage to goodwill toward utility	
12	Immediate macro economic damage	
13	Long term economic damage	[b] [e]
14	Loss of privacy	
15	Loss of sensitive business information	

Detectability of occurrence:

- Detection: Loss of condenser vacuum
    - Diagnosis:
        - The most common reaction would be to restart the pumps until there are repeated instances of the scenario.
        - This requires verification against the last known good backup of the pump house controls logic.
- Variants could have a more significant impact

Recovery timeline:

Following detection and diagnosis, the recovery would be as follows:

- 0-3 hours: Identify the change.
    - The identification of the change would require comparing files against a trusted backup and capturing the corrupted file for forensics.
- 4-24 hours: Restore the original configuration and confirm the integrity of related controls.
    - The key to this estimate is that a trusted backup of the configuration is available. There would need to be a verification of the set points and safe operation of the pump house equipment.

- 25-48 hours: Bring the plant back online.
  - This depends on the plant configuration; but cooling water is a necessary component of any thermal plant operation.

- Post Recovery
  - Perform forensics to determine:
    - Sequence of events
    - Mitigations to prevent attack from happening again

2.5.3 Analyze Factors that Influence Probability of Occurrence

Difficulty of conditions:

Condition numbers used here are shown in figure below.

- For Condition 1, the threat agent needs to gain physical access
  - This equipment, while remote, does not have network connectivity. This requires the threat agent to be present.

- For Conditions 2 and 3, the threat agent needs to have the necessary software and hardware to access the local network.
  - While the networks often run on major commercial operating systems and computers – the control software is proprietary.

- For Condition 4, he threat agent must have familiarity with controls system and power plant operations to identify the most damaging attack.
  - The nature of this attack is targeted at control logic and is not a simple network breach. A threat agent would have to understand power plants and controls systems.

Potential for multiple occurrences: This would initially be misdiagnosed as a spurious trip and the system could be restarted multiple times with the corrupted configuration before it was determined that this was not a hardware failure.

Best practices require that the cause of a trip be diagnosed and rectified. However, common practice is to get the unit back online and productive.

Also, if this attack can be achieved once, it can be executed multiple times. However, depending on the attack vector, lessons learned will make repeat occurrence on the same system less likely.

Likelihood relative to other scenarios:

- **Manipulating sensors and equipment**: A threat agent could disconnect a sensor, jumper an indication, disable equipment through a direct command, open the breakers, or physically fix a level indication. This would be easier to diagnose and fix than the current scenario, but this could have the same effect – if only once.

- **A disgruntled or social-engineered employee** carrying out the attack is perhaps a utility's most vulnerable means of attack since the insider threat is difficult to defend against.

- **For a malicious criminal or terrorist**, the higher level of skill and resources required for this attack is commensurate with established criminal or terrorist groups that have vast resources and highly skilled members.

2.5.4 Mitigations

Potential Mitigations

- *Restrict physical access* to pump house using, for example, card swipes, pin codes, etc., (Condition 1)
- *Require video surveillance* of the human interfaces to the pump house equipment, (Condition 1)
- *Require periodic physical surveillance* of intake structures and equipment (new common mitigation), (Condition 1)
- *Restrict physical access* by implementing personnel security control procedures, (Condition 1)
- *Authenticate users* so that physical access to the system(s) does not automatically grant logical access, (Conditions 2, 3)
- *Restrict configuration access* to limit who has access and can make configuration changes, (Condition 2)
- *Define procedures* to evaluate the credibility of high intake level readings from a pump house. For a spurious reading, other plant indications related to open loop cooling system would not be consistent, (Condition 4)
- *Authenticate users* for all user interface interactions, (Conditions 2, 3)
- *Generate alarms* on remote equipment when there is evidence of tampering of controls and instrumentation (Condition 4).

Organizations involved in scenario and recovery:

- Plant staff to replace the pumps, if they assume this was a hardware failure.
- Plant staff to reinstall the controls logic and/or make the tuning and setpoint adjustments.
- Physical security staff for assessing access to the pump house and potential physical security controls.
- IT staff, in coordination with the plant staff, to assess the failure once it is determined that it was the result of a cyber security event.

2.5.5 References

Source scenario(s): GEN.1 scenario in the Generation Failure Scenarios.

Publications: None.

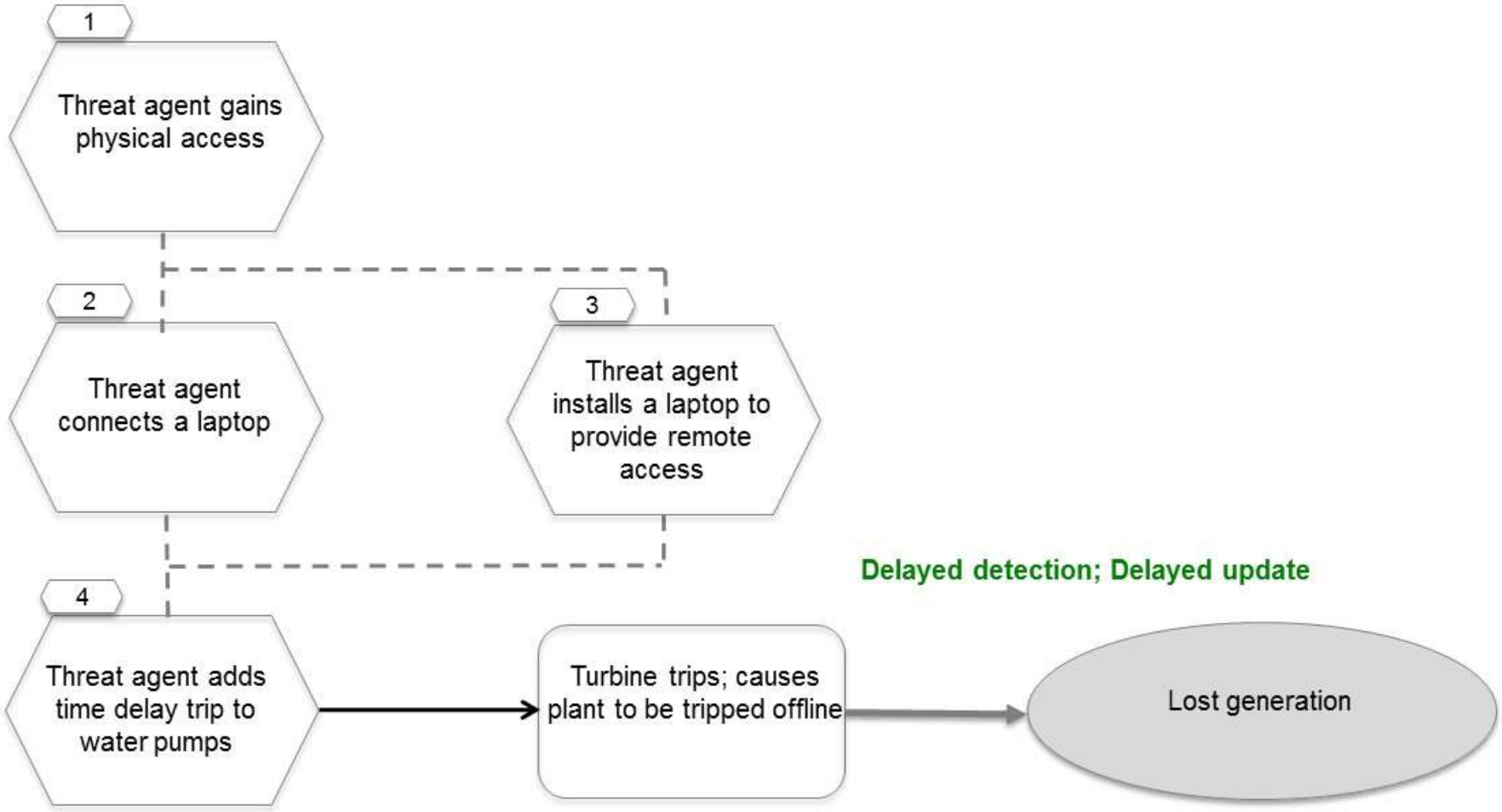

Figure 10
Threat Agent Adds Spurious Trip Parameters

2.6 GEN.15 Plant tripped off-line through access gained through a compromised vendor remote connection

2.6.1 Describe Scenario

Description: The threat agent, a disgruntled or compromised vendor employee, uses the authorization credentials and verification procedure to a secure remote maintenance solution. The remote access solution involves a vendor-maintained asset on the DCS network that prompts the utility to grant the asset access to the DCS network. In addition to the prompt, the procedure requires a separate call from the vendor to the utility describing the need to remotely connect before the utility will complete the connection. The threat agent calls the utility and claims the need to collect routine system performance information. The utility connects the vendor maintained computer to the DCS network, giving the threat agent access. The payload delivered by the threat agent is a modified system file that starts polling networked assets sending commands that cause a flood of traffic in the DCS network. The commands overwhelm the processing ability of the network causing loss of DCS control of the plant. On loss of plant control, the assigned operator initiates an immediate unit trip.

Assumptions:

- The attacker has detailed knowledge of the system to develop and execute the attack.
- The attacker is employed by the vendor at the time of the attack.
- The equipment supported by the vendor, if disrupted, has immediate impact on operations.
- The vendor remote access solution is authorized though the DMZ and firewalls.
- The remote access solution allows administrative access to the control system or DCS. This allows the attacker to carry out the full scope of the attack.
- The vendor remote solution offers access to the balance-of-plant controls.
- The affected computer is centrally connected within the DCS network with connection to the systems required for operation.

- The vendor is not actively monitored when provided remote access through the vendor remote access solution.

- Utility employees follow all appropriate procedures when granting remote access, but those do not include control room notification.

- Vendor remote access to the utility network is not limited to the IP range of the vendor.

- The vendor uses a single support team to support all customers.

- The DCS does not employ an active configuration change detection solution.

- The backup system is in place and the files being backed up are sufficient for recovery. This has been confirmed by testing.

- The hardware is not damaged and does not require replacement parts to be shipped.

Variants of the scenario:

- The launching of the attack is time-delay. This may make it more difficult to identify the specific threat agent.

- There is insufficient backup of the configuration and/or the firmware and software.

- Multiple vendor customers are attacked in the same manner.

- The payload modifies the configuration and obscures any warnings to non-normal operations causing more widespread damage and/or personnel safety before the operator is prompted to trip the unit.

- The payload spreads to the operating systems of the computers connected to the network and renders them inoperable.

Physical location for carrying out scenario:

The remote access allows for the attacker to be anywhere with internet access.

Threat agent(s) and objectives

Possible Threat Agents could include:

- Malicious Criminals
  - A disgruntled vendor employee with privileges and domain knowledge.
- Terrorists
  - Nation-state actors: for a multi-site attack, this may require a nation state with access to multiple compromised vendor employees.

Relevant vulnerabilities:

- *System may become overwhelmed by traffic flooding or malformed traffic* through the DCS network,
- *Insiders with high potential for criminal or malicious behavior have access to critical functions or sensitive data*,
- *Publicly accessible and/or third-party control links used*,
- *Design permits unnecessary privileges*,
- *Presence of features or functions that may be misused by users*,
- *System permits installation of malware*,
- *Users lack visibility of threat activity,* specifically unexpected access to network components or unusual traffic on the network,
- *Users and hardware/software entities are given access unnecessary for their roles* to perform duties that should be separated,
- *Users lack visibility that unauthorized changes were made* to the DCS,
- *System permits unauthorized changes* by allowing remote access for vendors to do monitoring and maintenance.

Relationship to NISTIR 7628 logical reference model functions: The generation domain includes actor 1: Plant Control System – Distributed Control System (DCS). This is included in Logical Interface Category (LIC) 6. This is a local control system at a bulk generation plant. The focus of this failure scenario is having remote access to the control system and launching an attack.

2.6.2 Analyze Impact

Impact:

- [a] Affected assets will have to be restored and verified operational.

- [b] Trips will result in costs to restart the unit and to purchase replacement power. An unexpected and sudden trip challenges grid stability at the moment that the plant is taken offline.
- [c] Any unexpected plant trip stresses the major plant components (e.g., generator, turbine, and boiler) leading to a reduction in the expected life of the components and a greater possibility of damage when the units restart.

The table below shows those general categories of impacts that are most relevant to this scenario, as they relate to the discussion above.

Table 5
Impact Categories for GEN.1

	Impact category	Text reference
1	Public safety concern	
2	Workforce safety concern	
3	Ecological Concern	
4	Financial Impact of Compromise on Utility (excluding #5)	
5	Cost to return to normal operations	[a] [b]
6	Negative impact on generation capacity	[a] [b]
7	Negative impact on the energy market	
8	Negative impact on the bulk transmission system	
9	Negative impact on customer service	
10	Negative impact on billing functions	
11	Damage to goodwill toward utility	
12	Immediate macro economic damage	
13	Long term economic damage	[c]
14	Loss of privacy	
15	Loss of sensitive business information	

Detectability of occurrence:

- Detection: Loss of plant control in an immediate time frame.

- Diagnosis:
  - The most common reaction would be to restart the computers on the network.

  - Diagnosis time will be affected by which computer had the offending system file installed (e.g., if the file was installed on an HMI, diagnosis would be faster than if the file was installed on an engineering station).

- Diagnosis time will be affected by the amount of technology monitoring available – particularly logging of events.

- Diagnosis time will be affected by the capabilities of the employees.

Variants may have a greater effect.

Recovery timeline:

Following detection and diagnosis, the recovery would be as follows:

- 0-3 hours from disturbance:

  - Notify dispatch and plant management
  - Implement incident response plan that includes any necessary regulatory reporting.
  - Determine the required information that is needed to reconstruct the sequence of events, including attribution and apparent cause.

- 4-72 hours from disturbance:

  - Expand the troubleshooting team – to include the vendor - and identify the compromised machine via traffic and packet analysis.
  - Remove the compromised machine from the network and replace with a *clean* machine.
  - Variants that result in damage to the operating or control assets may require extensive time to repair/replace those assets.

- Post-recovery:

  - Forensic review to determine sequence of events, cause, and attribution (if possible).
  - Coordination with the vendor for appropriate legal action against the threat actor.
  - Identify the extent of enabling conditions and determine if mitigation strategies can be implemented.
  - Apply lessons learned and revise the remote access policies, procedures, and technical controls. (These remote access revisions may be applicable to both vendors and employees.)

2.6.3 Analyze Factors that Influence Probability of Occurrence

Difficulty of conditions:

Condition numbers used here are shown in Figure 11 below.

- For Conditions 2, 3, and 4, this attack is limited to insiders with appropriate access and domain knowledge.
- For Condition 4, the threat actor must have knowledge of the network configuration.
- For Condition 5, he threat actor must have knowledge of the operator's reaction to a loss of control. This may include both procedural and technical responses.
- For Conditions 4, 5, the threat actor must have knowledge of how to execute the attack and the specific attack vector (e.g., installing the appropriate payload). A more technically mature utility organization should have applicable mitigations in place.

Potential for multiple occurrences:

- This is largely dependent on the scenario variants.
- If the vendor is responsible for implementing the mitigation strategy, this could potentially leave the vulnerabilities unresolved and the threat actor undetected.

Likelihood relative to other scenarios:

- A command to an HMI could freeze the device. This would not require a file to be modified and, consequently, would leave minimal evidence.

2.6.4 Mitigation

Potential mitigations:

- *Train personnel* in proper configuration requirements for assets connected to the DCS system (Conditions 1, 2),
- *Enforce least privilege* for access to the DCS by limiting remote administrative access through vendor monitoring employee sessions for cases of configuration and file system changes (Condition 3),

- *Restrict remote access* to not allow direct file transfer as a default privilege (Conditions 2, 3, 4),
- *Require second-level authentication* that includes (Condition 5):
  - management authorization for configuration changes and file transfers and
  - "Escorted remote access" requiring live monitoring of vendor access for potentially damaging actions.
- *Restrict configuration access* to limit who has access and can make configuration changes (Conditions 3, 4, 5),
- *Create audit logs* that record the remote access sessions (Condition 3),
- *Detect unauthorized configuration changes* to the asset (Condition 4),
- Automated *configuration change detection* (Condition 4),
- *Detect unauthorized access* in network traffic between the vendor and the DCS device (Conditions 1, 2),
- *Require intrusion detection* (Condition 1),
- *Detect abnormal behavior* in machines and flag this behavior (Condition 5),
- *Require application whitelisting* on the DCS network (Condition 5).

Organizations involved in scenario and recovery:

- Plant staff to make the system operational.
- Plant staff, in coordination with the IT staff, to remove the malicious software and reconfigure the DCS system.
- IT staff, in coordination with the plant staff, to assess the failure and determine mitigation strategies.

2.6.5 References

Source scenario(s): GEN.1 scenario in the Generation Failure Scenarios.

Publications: None.

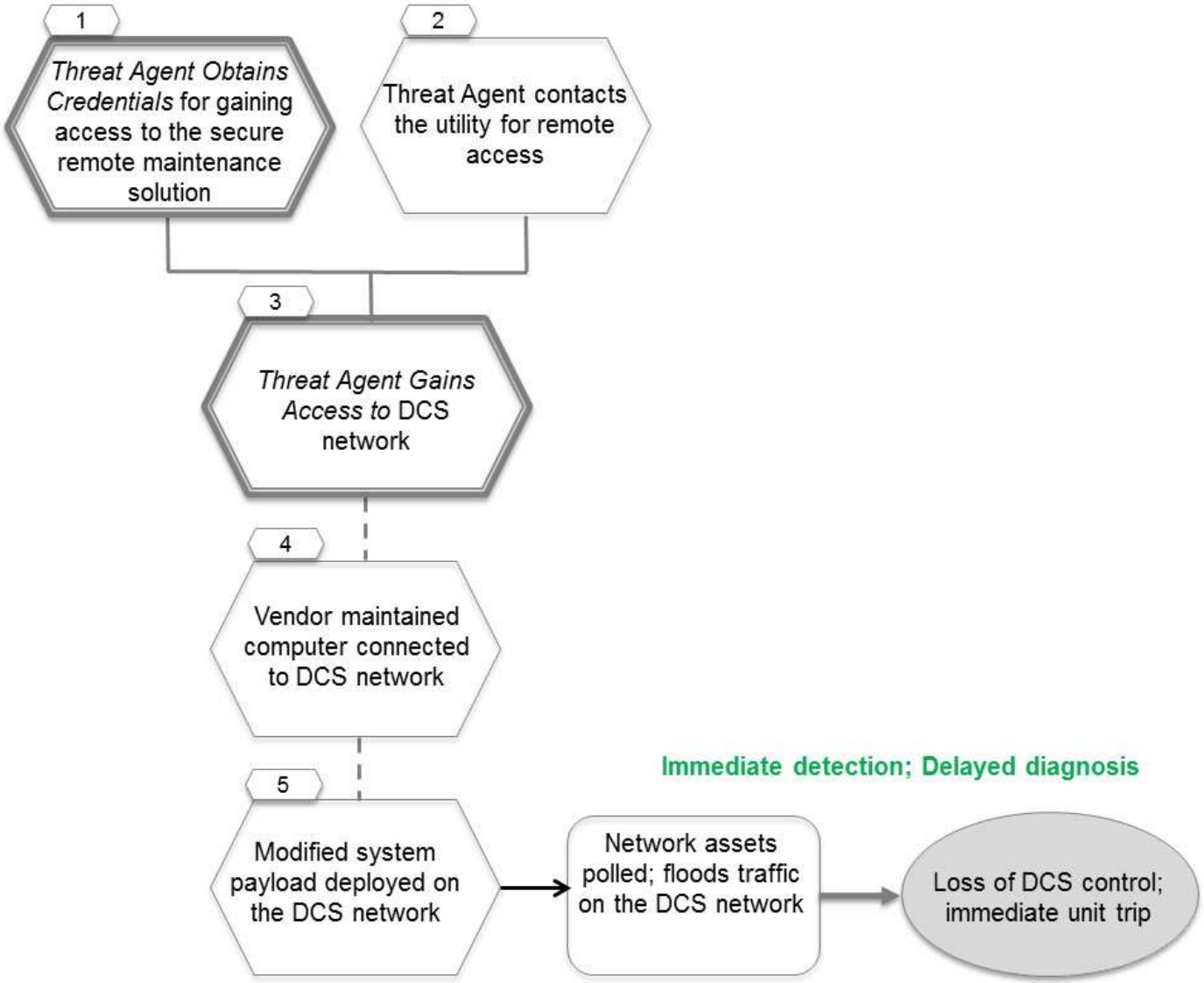

Figure 11
Plant Tripped Off-Line Through Access Gained Through a Compromised Vendor Remote Connection

3 ADDITIONAL ATTACK TREES

3.1 General

Included in this section are attack trees for the following failure scenarios from the domains indicated. Detailed text analyses are not available in this draft for these failure scenarios. Summary text information based on [1] is provided for context before each attack tree. Appendix B provides the rationale for selection of these failure scenarios for detailed analysis. Section 2.1.2 provides a brief summary of the attack tree notation.

- Advanced Metering Infrastructure failure scenarios:
    - AMI.9 Invalid Disconnect Messages to Meters Impact Customers and Utility
    - AMI.12 Improper Firewall Configuration Exposes Customer Data
    - AMI.14 Breach of Cellular Provider's Network Exposes AMI Access
    - AMI.16 Compromised Head end Allows Impersonation of CA
    - AMI.27 Reverse Engineering of AMI Equipment Allows Unauthorized Mass Control
    - AMI.29 Unauthorized Device Acquires HAN Access and Steals Private Information
- Demand response failure scenarios:
    - DR.1 Blocked DR Messages Result in Increased Prices or Outages
    - DR.4 Improper DRAS Configuration Causes Inappropriate DR Messages

3.2 AMI.9 Invalid Disconnect Messages to Meters Impact Customers and Utility

Description: A threat agent obtains legitimate credentials to the AMI system via social engineering. The threat agent may already have access to the network on which this system resides or may succeed in reaching the network from another network. The threat agent issues a disconnect command for one or more target meters. Alternatively, a disconnect may be placed in a schedule and then occur automatically at a later time.

Assumptions

- No Internet access from AMI headend
- A limited number of individuals have privilege to do disconnects

Potential Mitigations

Conditions apply to the following figure(s).

- See common sub tree *Threat Agent Obtains Legitimate Credentials* for <system or function> (Condition 1)
- See common sub tree *Threat Agent Gains Access to* <*Network*> (Condition 2)
- *Design for security* by not permitting disconnects originating from headend (For example, require meter to verify signature by business system) (Condition 4)
- *Cross check* payment status and critical service against business rules (Condition 5)
- *Enforce least privilege* to a minimum number of individuals requiring MDMS access (Condition 5) – *Generate alerts* for users to another instance of their account in use (if they are logged in), and time of last login (Condition 5)
- *Detect unusual patterns* of disconnects on smart meters (Condition 5)

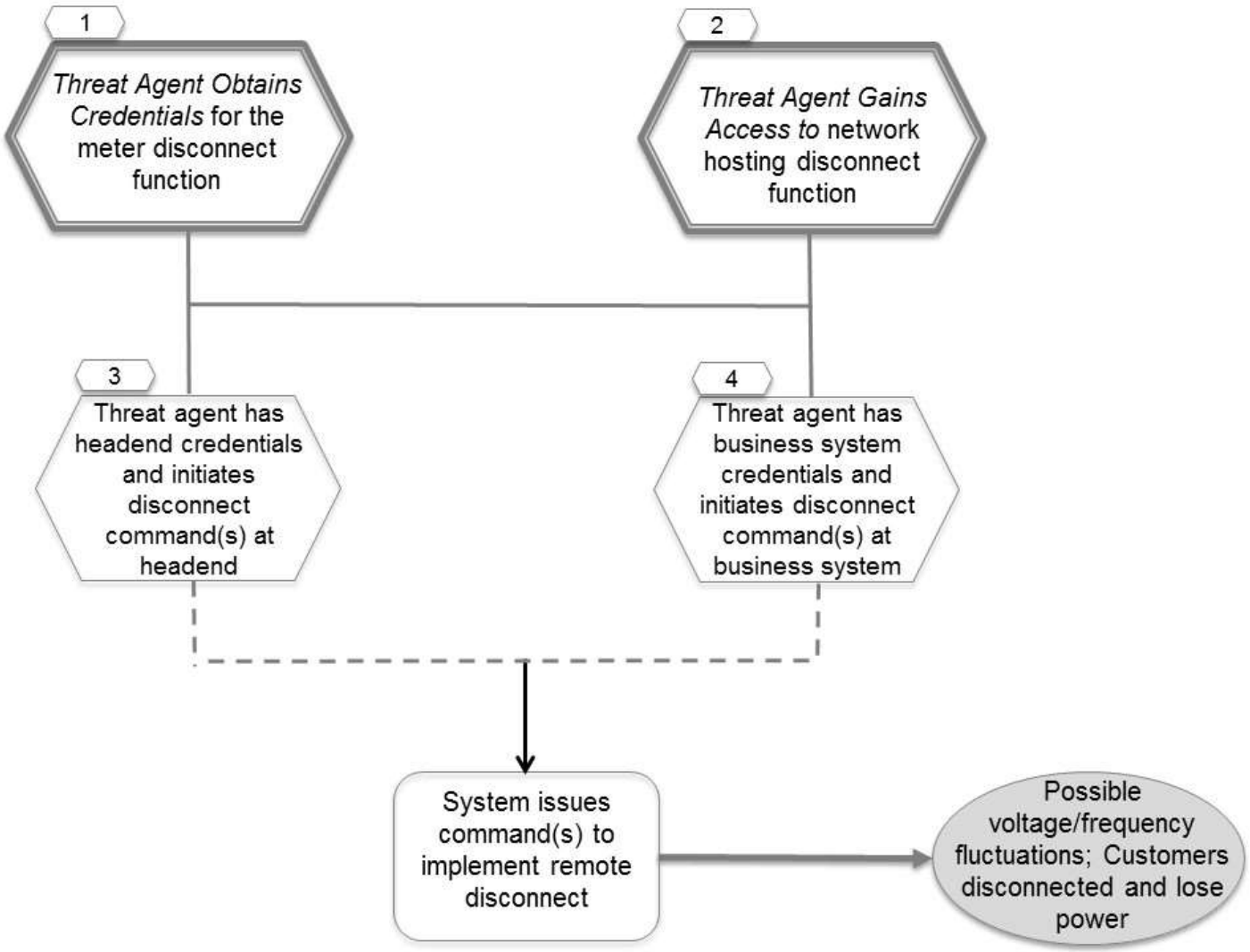

Figure 12
Invalid Disconnect Messages to Meters Impact Customers and Utility

3.3 AMI.12 Improper Firewall Configuration Exposes Customer Data

Description: A firewall rule is intentionally or unintentionally created allowing direct access from another network. Taking advantage of this rule, a threat agent subsequently gains access to the central database that receives data from the customer accounts database and from the energy usage application. This enables the threat agent to steal customer identifiable information, including electricity usage data.

Assumptions

- Authentication and roles in place for access to customer data
- Operations network hosts customer private data

Potential Mitigations

Conditions apply to the following figure(s).

- See common sub tree *Threat Agent Finds Firewall Gap* (Condition 1)
- See common sub tree *Threat Agent Obtains Legitimate Credentials*
- *Require authentication* to the network
- *Enforce least privilege* for individuals with access to hosts on the network
- *Detect unusual patterns* of usage on hosts and network
- *Enforce least* privilege to limit central database/application access to authorized applications and/or locally authenticated users

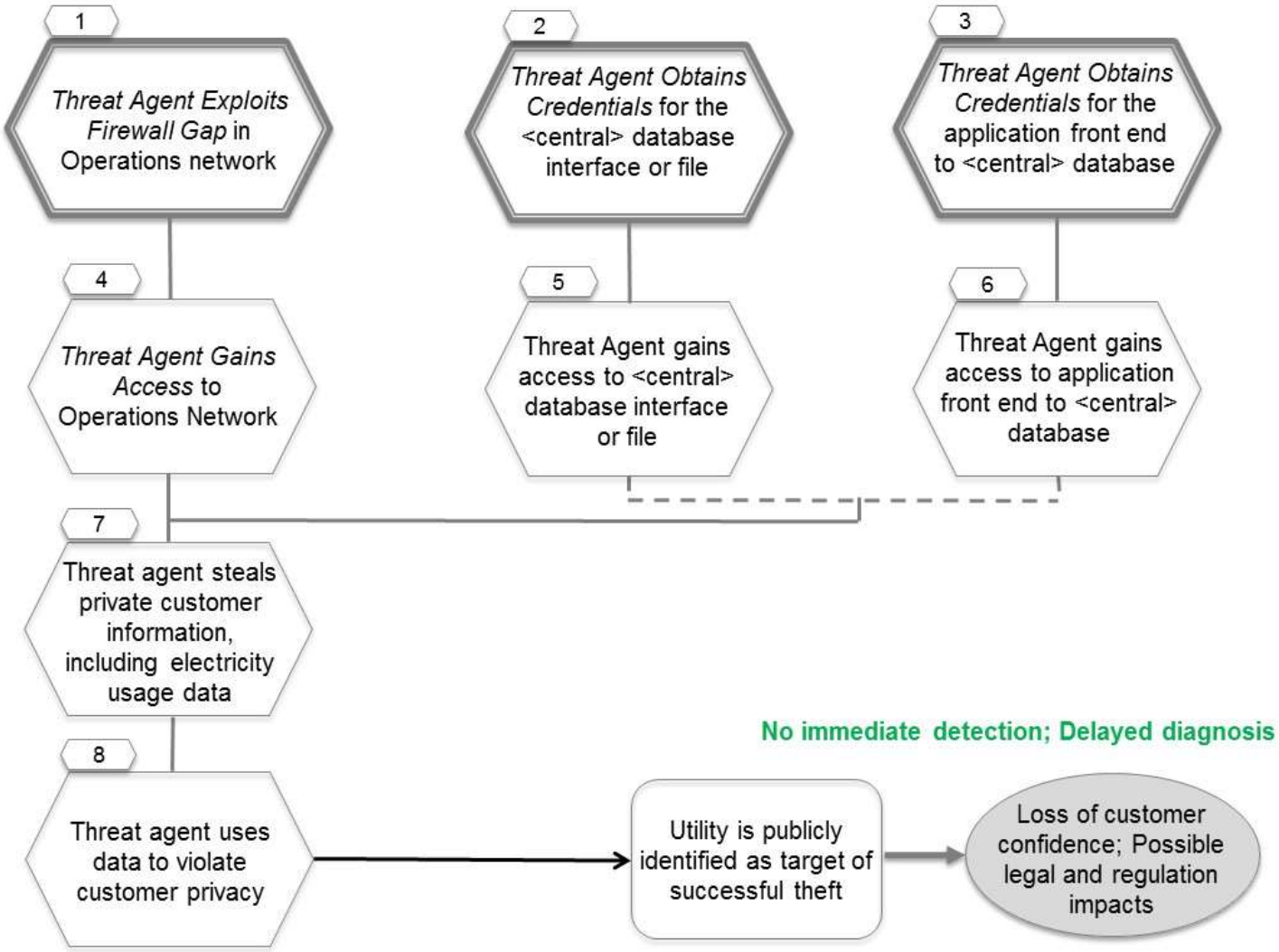

Figure 13
Improper Firewall Configuration Exposes Customer Data

3.4 AMI.14 Breach of Cellular Provider's Network Exposes AMI Access

Description: A cellular phone provider's network is breached, allowing access to a private network leased to a utility for AMI command and control. The AMI implementation is vulnerable to replay attacks and DR messages are replayed to a group of customers.

Assumptions

- Inadequate separation of private leased networks between cellular phone provider and leased utility network for AMI
- Weak or no cryptography for network access
- Replay ability for commands

Potential Mitigations

Conditions apply to the following figure(s).

- *Isolate networks* using different encryption keys to prevent a breach in one network from affecting another network (Conditions 1, 2)
- *Require approved cryptographic algorithms* at the link layer to prevent a threat agent from being able to affect the confidentiality and integrity on the AMI network if a breach should occur (Condition 2)
- *Protect against replay* using time-stamping or other methods (Condition 3)

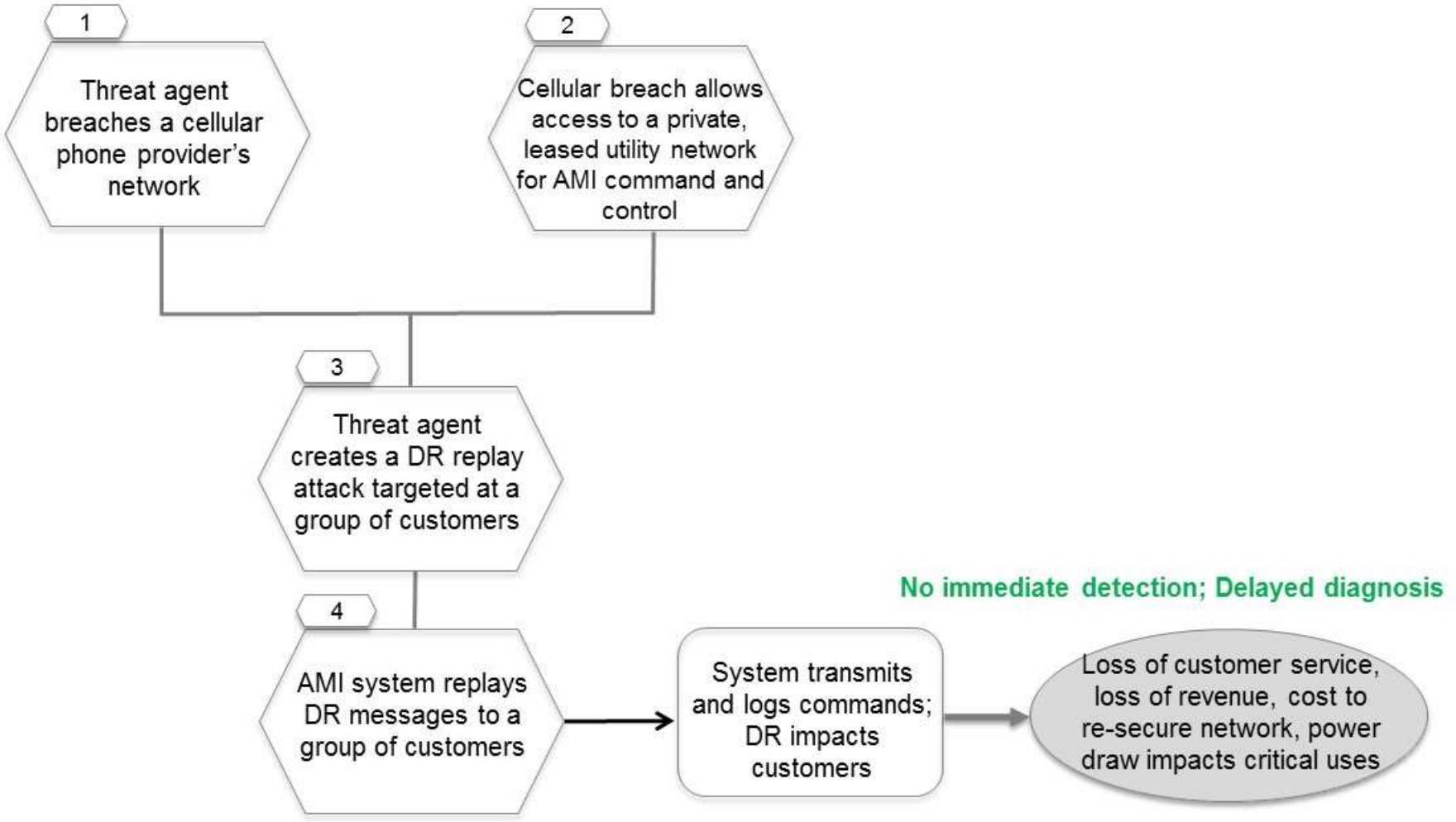

Figure 14
Breach of Cellular Provider's Network Exposes AMI Access

3.5 AMI.16 Compromised Head end Allows Impersonation of CA

Description: The private key for the certificate authority (CA) used to set up a Public Key Infrastructure (PKI) at the head end is compromised, which allows a threat agent to impersonate the CA.

Assumptions

- No cryptography for AMI network access
- PKI is used on the AMI network

Potential Mitigations

Conditions apply to the following figure(s).

- *Require approved key management* including secure generation, distribution, storage, and update of cryptographic keys (Condition 1)
- See common sub tree *Threat Agent Gains Access to* <network> (Condition 2)

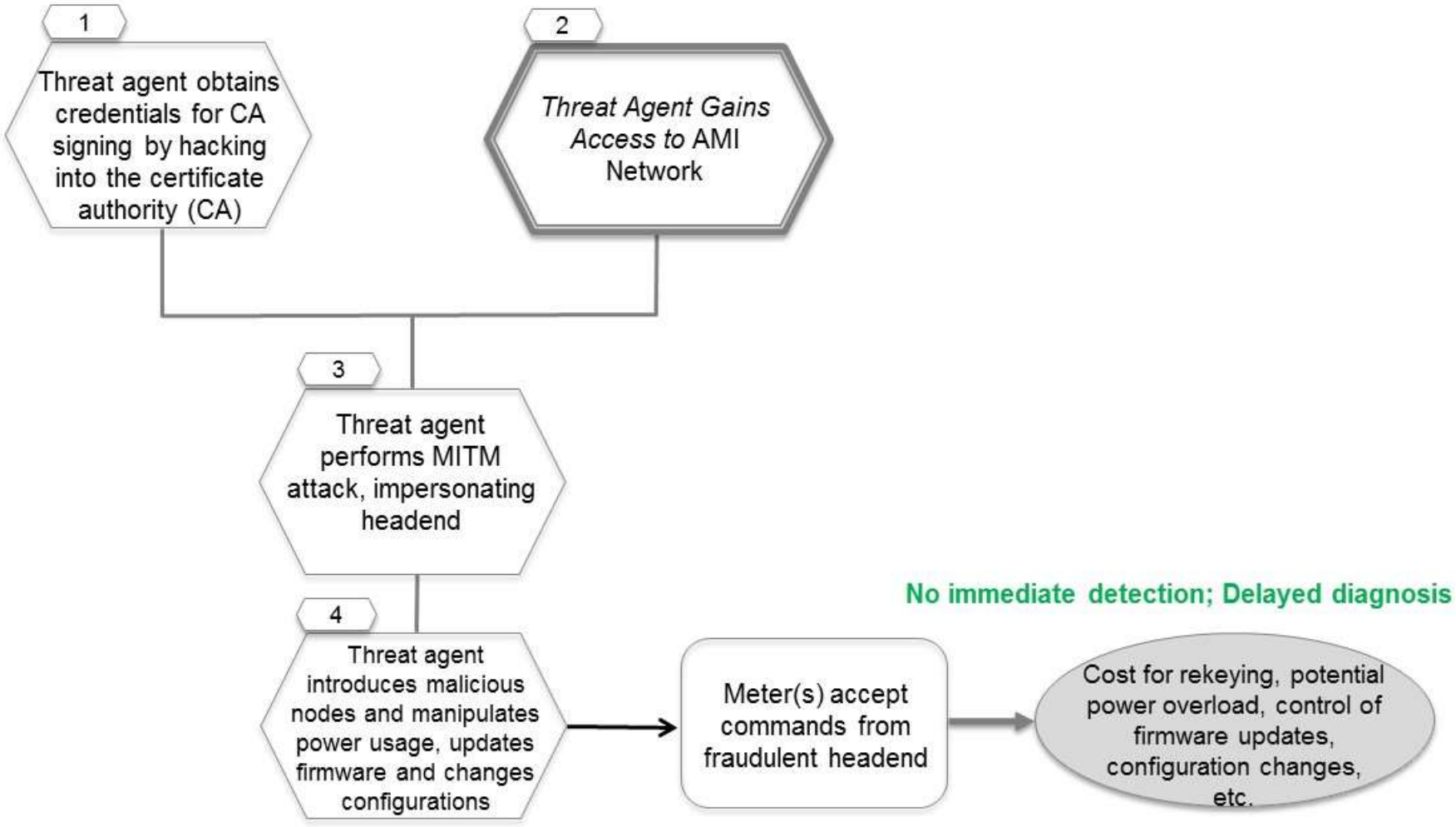

Figure 15
Compromised Headend Allows Impersonation of CA

3.6 AMI.27 Reverse Engineering of AMI Equipment Allows Unauthorized Mass Control

Description: A threat agent is able to reverse engineer AMI equipment (meters and concentrators) to determine how to remotely control them. This allows the threat agent to control many devices simultaneously, and, for example, to perform a simultaneous mass disconnect, send DR messages that cause consumption of electricity to go up dramatically, or cause devices to send out last gasp or self-test failed messages.

Assumptions

- Devices are not built with adequate security
- Backdoors and unprotected interfaces remain on production equipment

Potential Mitigations

Conditions apply to the following figure(s).

- *Design for security* to identify and remove unsecure development features and nonstandard" interfaces from production devices (Condition 1)
- See common tree *Threat Agent Obtains Legitimate Credentials* (Condition 2)
- *Design for security* in equipment such that knowledge alone should not allow a threat agent to access a device without knowledge of keys and other credentials in equipment design (Condition 3)
- *Configure for least functionality* by removing unnecessary interfaces and labeling from production devices (Condition 3)

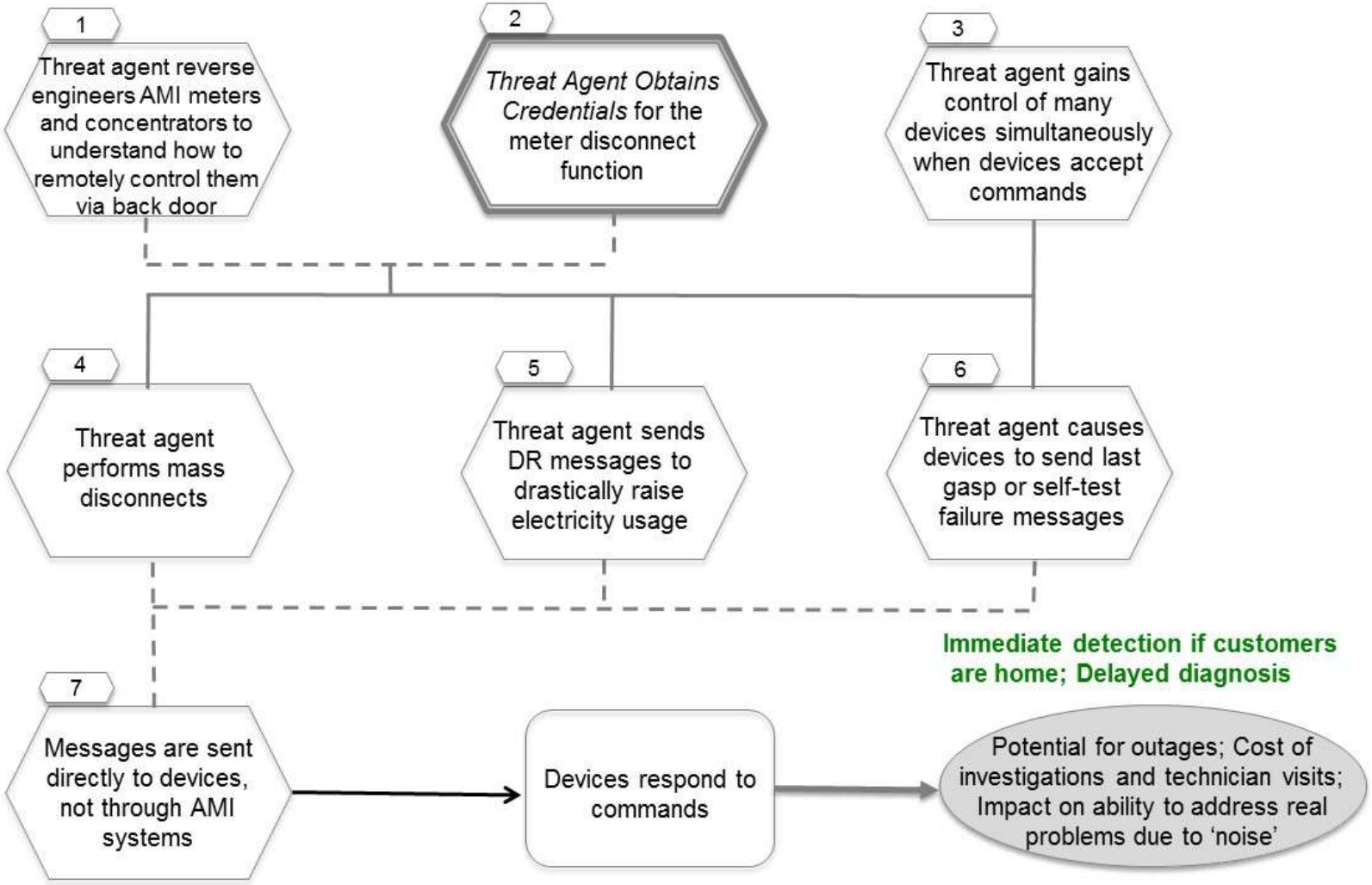

Figure 16
Reverse Engineering of AMI Equipment Allows Unauthorized Mass Control

3.7 AMI.29 Unauthorized Device Acquires HAN Access and Steals Private Information

Description: An unauthorized device gains access to the HAN and uses the web interface to obtain private information. Examples of such information are patterns of energy usage and the presence of medical devices.

Assumptions

- Weak or no authentication required for HAN access

Potential Mitigations

Conditions apply to the following figure(s).

- Restrict network access to the HAN (Condition 1)
- Minimize private information in HAN systems and devices (Condition 2)

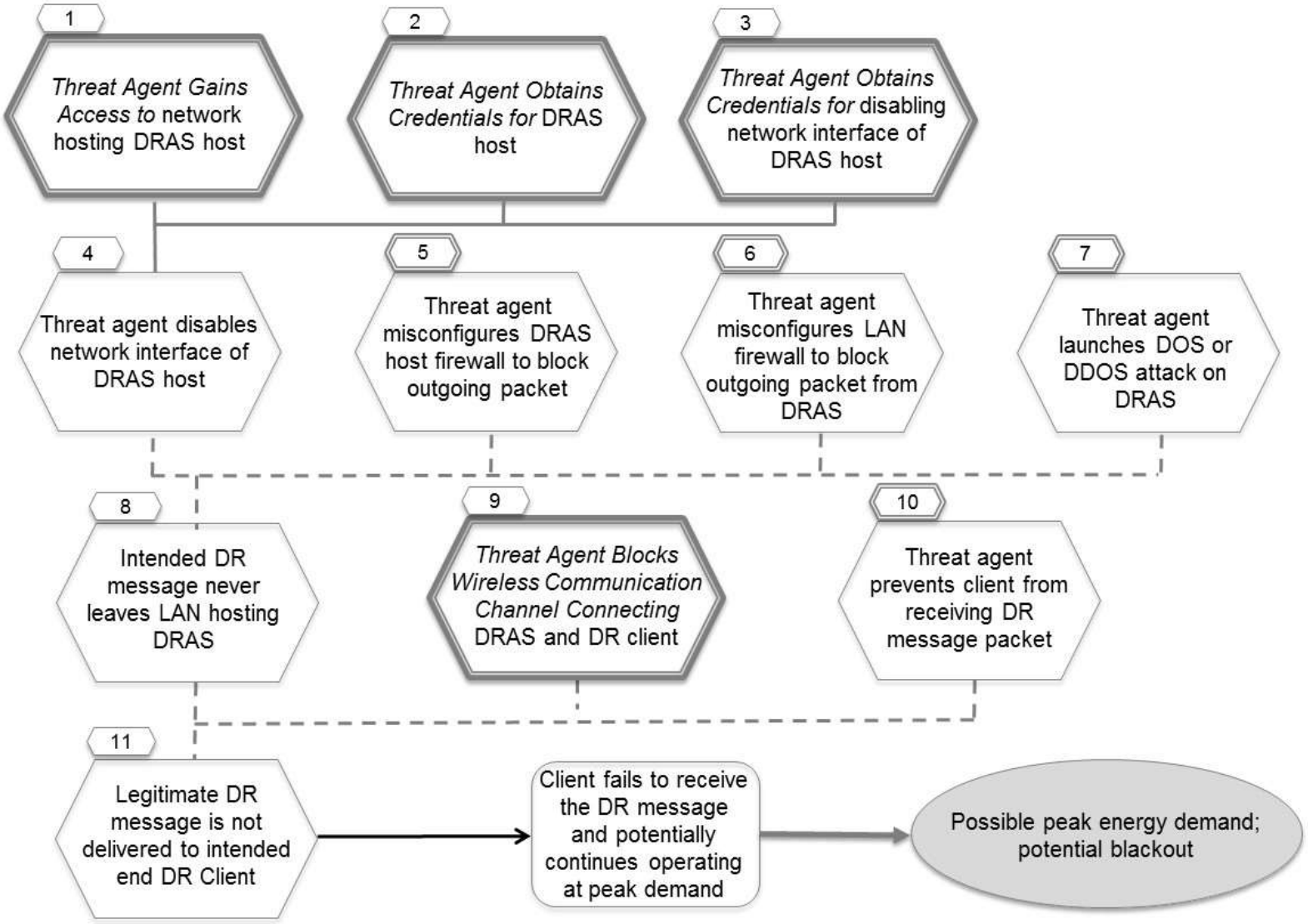

Figure 17
Unauthorized Device Acquires HAN Access and Steals Private Information

3.8 DR.1 Blocked DR Messages Result in Increased Prices or Outages

Description: A threat agent blocks communications between a demand response automation server (DRAS) and a customer system (smart meters or customer devices). This could be accomplished by flooding the communications channel with other messages, or by tampering with the communications channel. These actions could prevent legitimate DR messages from being received and transmitted. This can occur at the wired or the wireless portion of the communications channel.

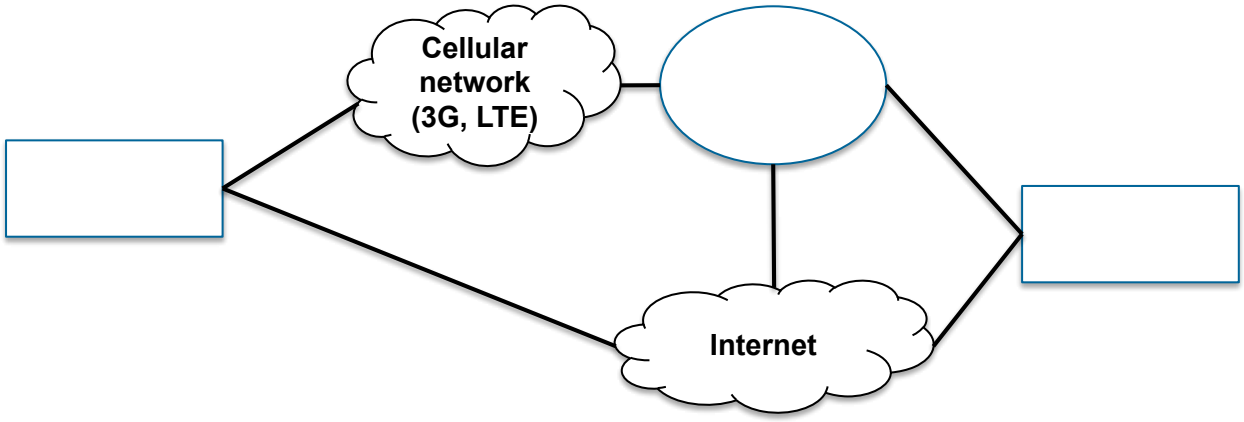

Figure 18
Architecture for DR.1 Scenario

Assumptions

- None currently identified.

Potential Mitigations

Conditions apply to the following figure(s).

- See common sub tree Threat Agent Gains Access to <network> (Conditions 1, 16)
- See common sub tree Threat Agent Obtains Legitimate Credentials for <system or function> (Conditions 2, 3, 12, 17, 18, 19)
- Generate alerts on changes to device configurations on DRAS host; Require acknowledgement of link status to ensure network connectivity; Detect unauthorized configuration changes (Condition 4)

- Generate alerts on changes to firewall rules on DRAS host; Require acknowledgement of link status to ensure network connectivity; Detect unauthorized configuration changes (Condition 4)
- Generate alerts on changes to rules on LAN firewall; Detect unauthorized configuration changes; Create audit log of packet filtering rule changes (Condition 6)
- Require intrusion detection and prevention; Detect unusual patterns of network traffic; Enforce restrictive firewall rules for DRAS LAN access (Condition 7)
- See common sub tree *Threat Agent Blocks Wireless Communication Channel Connecting <x and y>* (Condition 9)
- See common sub tree *Threat Agent Gains Capability to Reconfigure Firewall <firewall description>* (Conditions 13, 24)
- *Maintain patches* in all computers; *Maintain anti-virus*; *Test for malware*; *Restrict remote access* to internal computers (Condition 14)
- See common sub tree *Authorized Employee Brings Malware into <system or network>* (Conditions 15, 26)
- *Generate alerts* on changes to device configurations on DR client; *Require acknowledgement* of link status to ensure network connectivity; *Detect unauthorized configuration changes* (Condition 20)
- *Generate alerts* on changes to configurations on DR client; *Require acknowledgement* of link status to ensure network connectivity; *Detect unauthorized configuration changes* (Condition 21)
- *Generate alerts* on changes to rules on LAN firewall; *Detect unauthorized configuration changes*; *Create audit log* of packet filtering rule changes (Condition 22)
- *Require intrusion detection and prevention*; *Detect unusual patterns* of network traffic; *Enforce restrictive firewall rules* for Client LAN access (Condition 23)
- *Maintain patches* in all computers; *Maintain anti-virus*; *Test for malware*; *Restrict remote access* to internal computers (Condition 25)

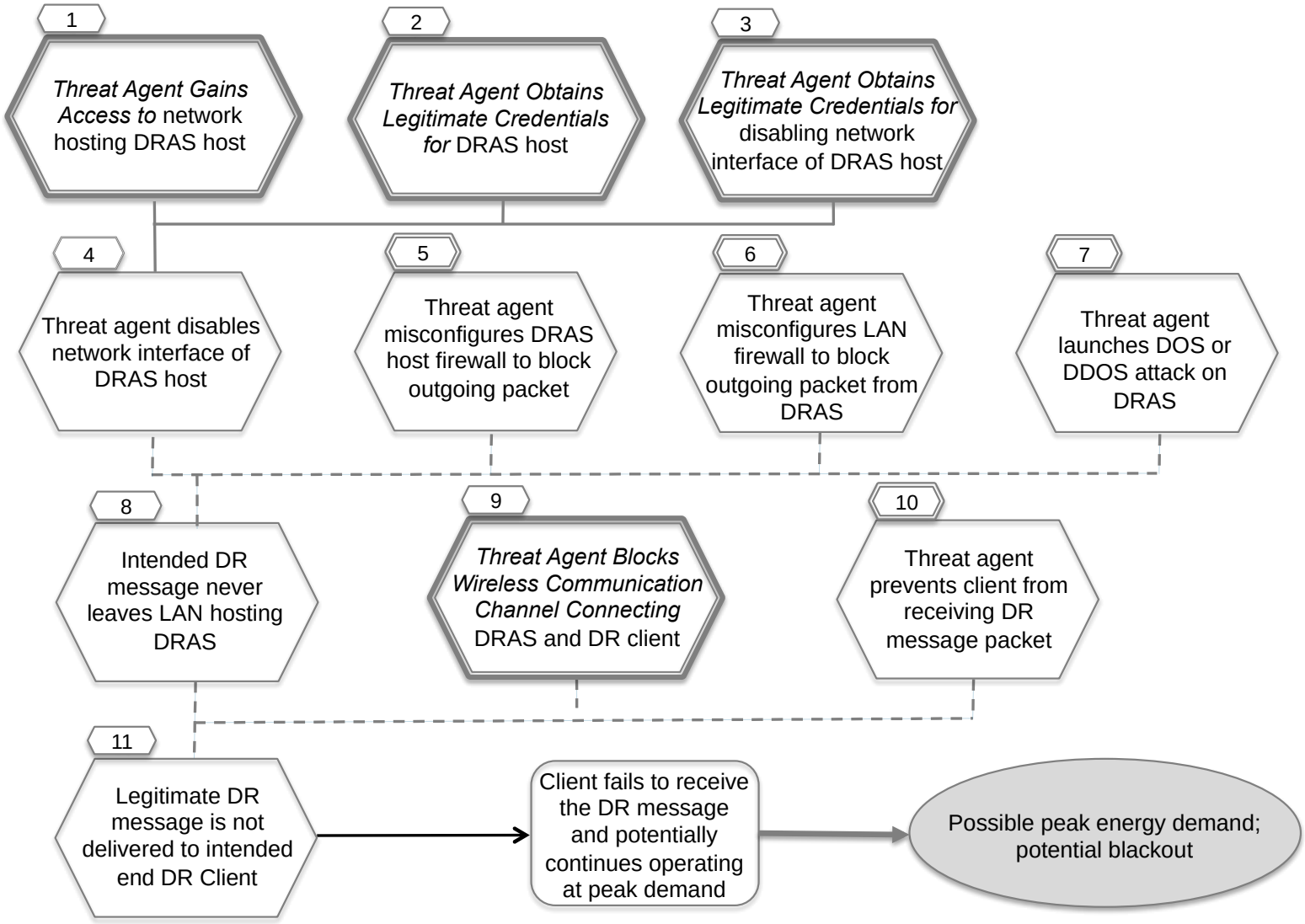

Figure 19
Blocked DR Messages Result in Increased Prices or Outages (1/8)

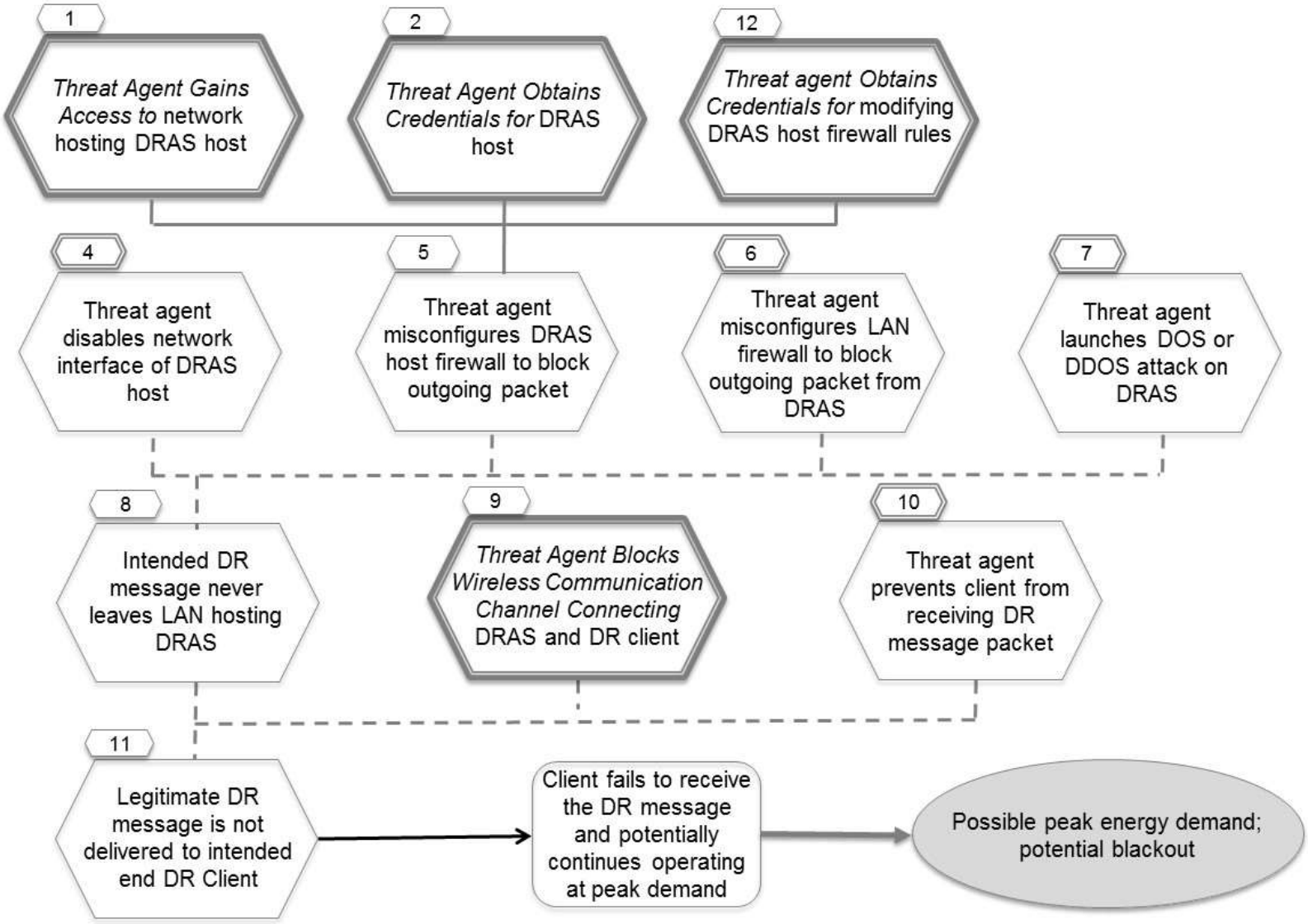

Figure 20
Blocked DR Messages Result in Increased Prices or Outages (2/8)

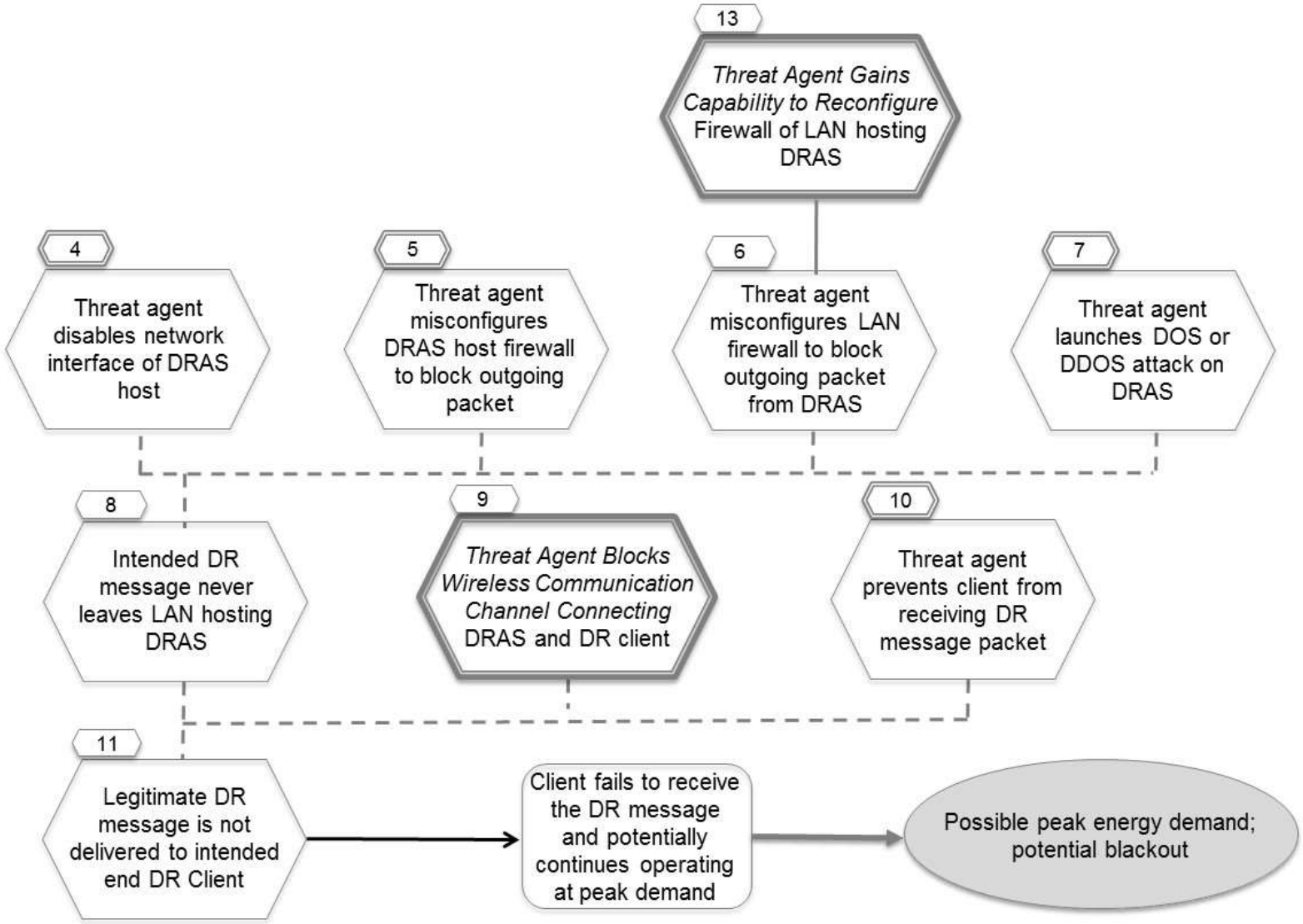

Figure 21
Blocked DR Messages Result in Increased Prices or Outages (3/8)

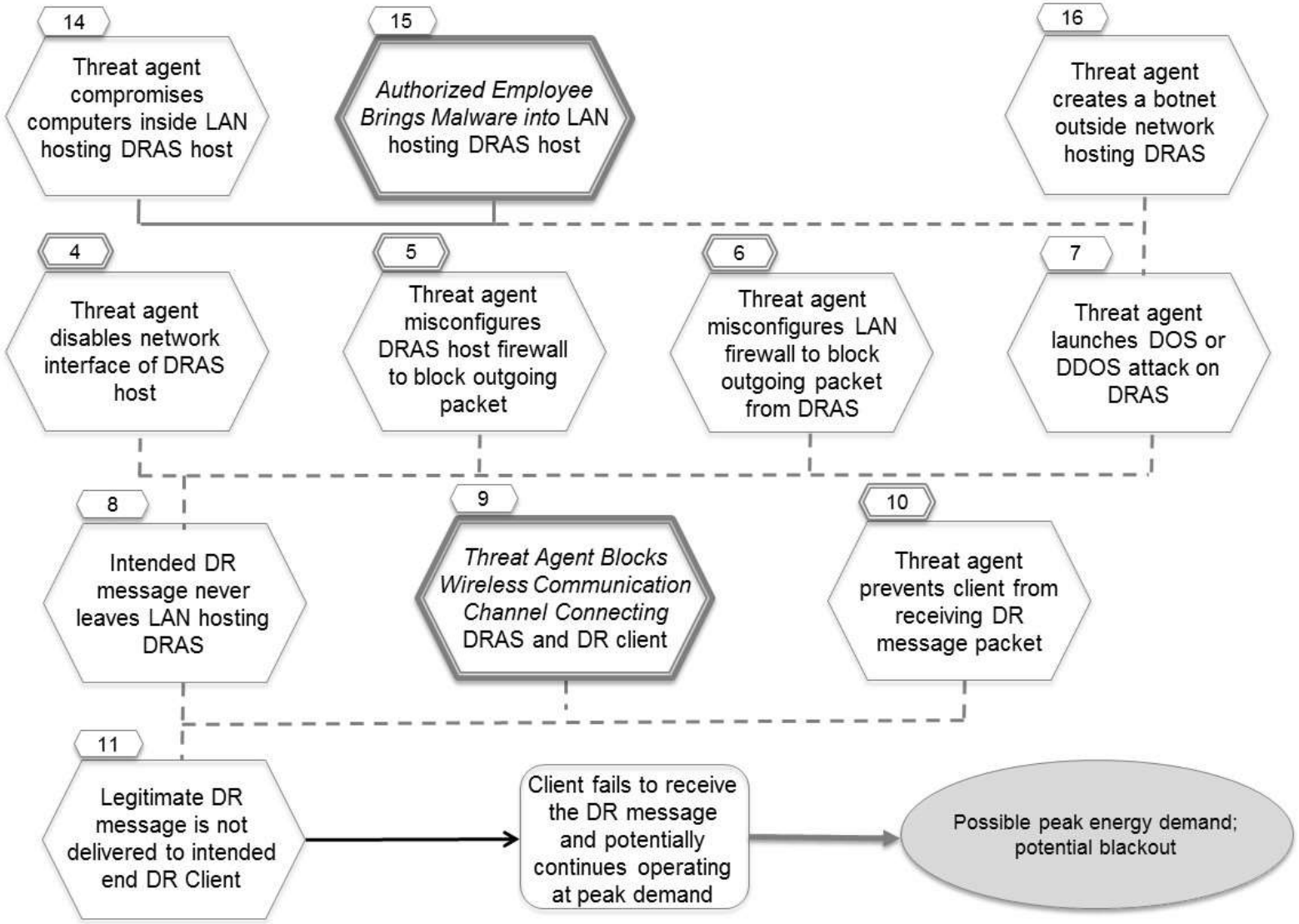

Figure 22
Blocked DR Messages Result in Increased Prices or Outages (4/8)

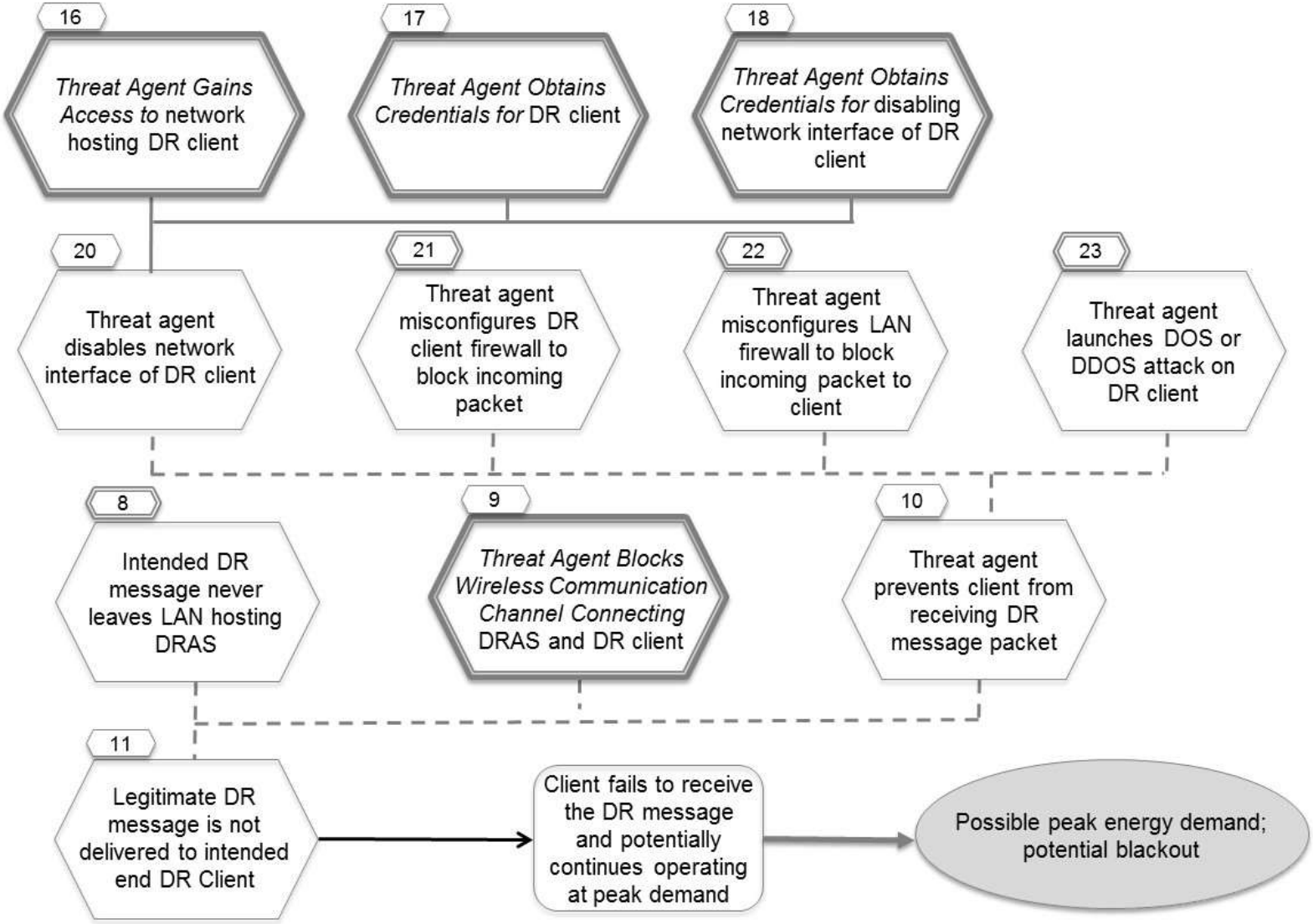

Figure 23
Blocked DR Messages Result in Increased Prices or Outages (5/8)

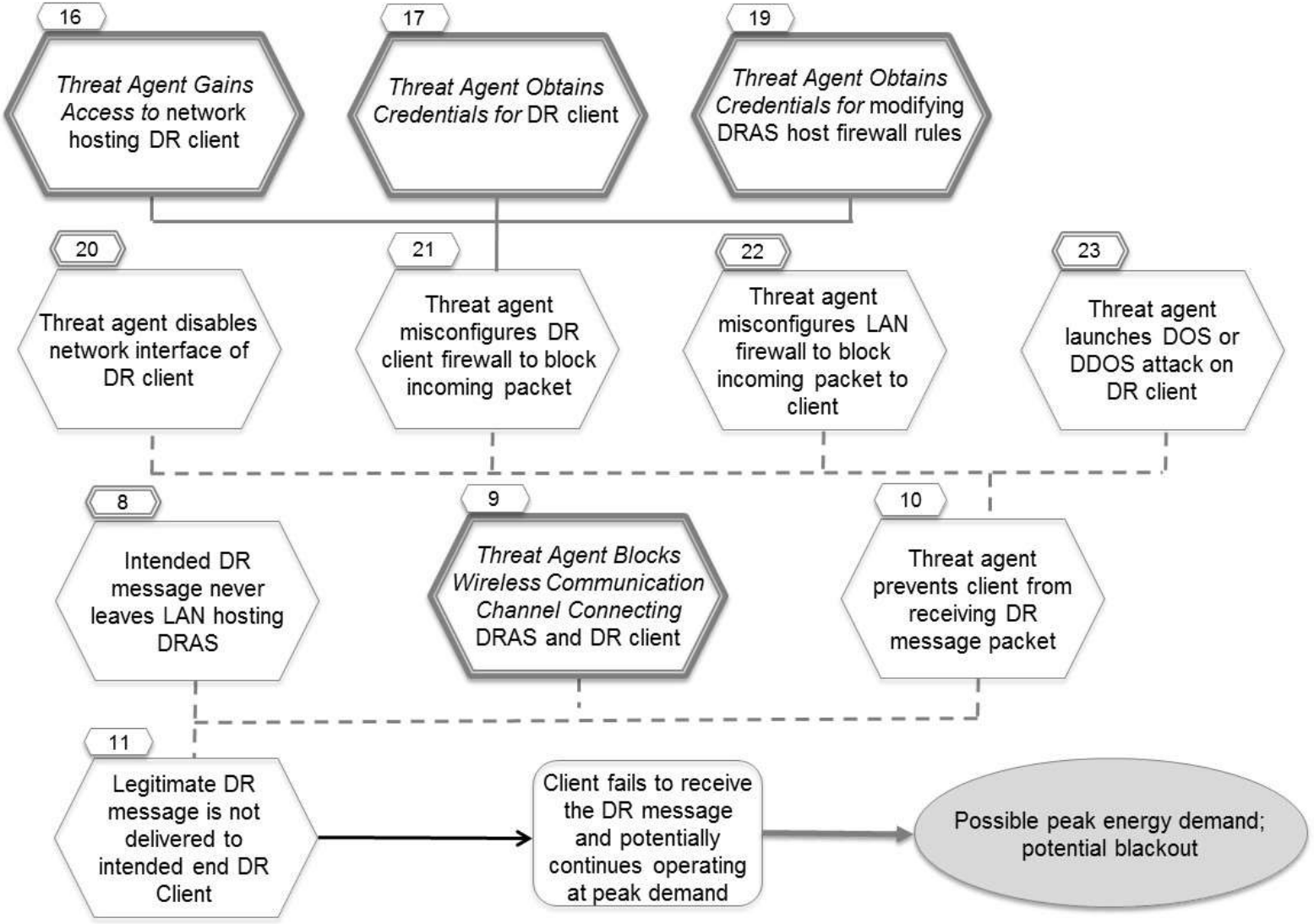

Figure 24
Blocked DR Messages Result in Increased Prices or Outages (6/8)

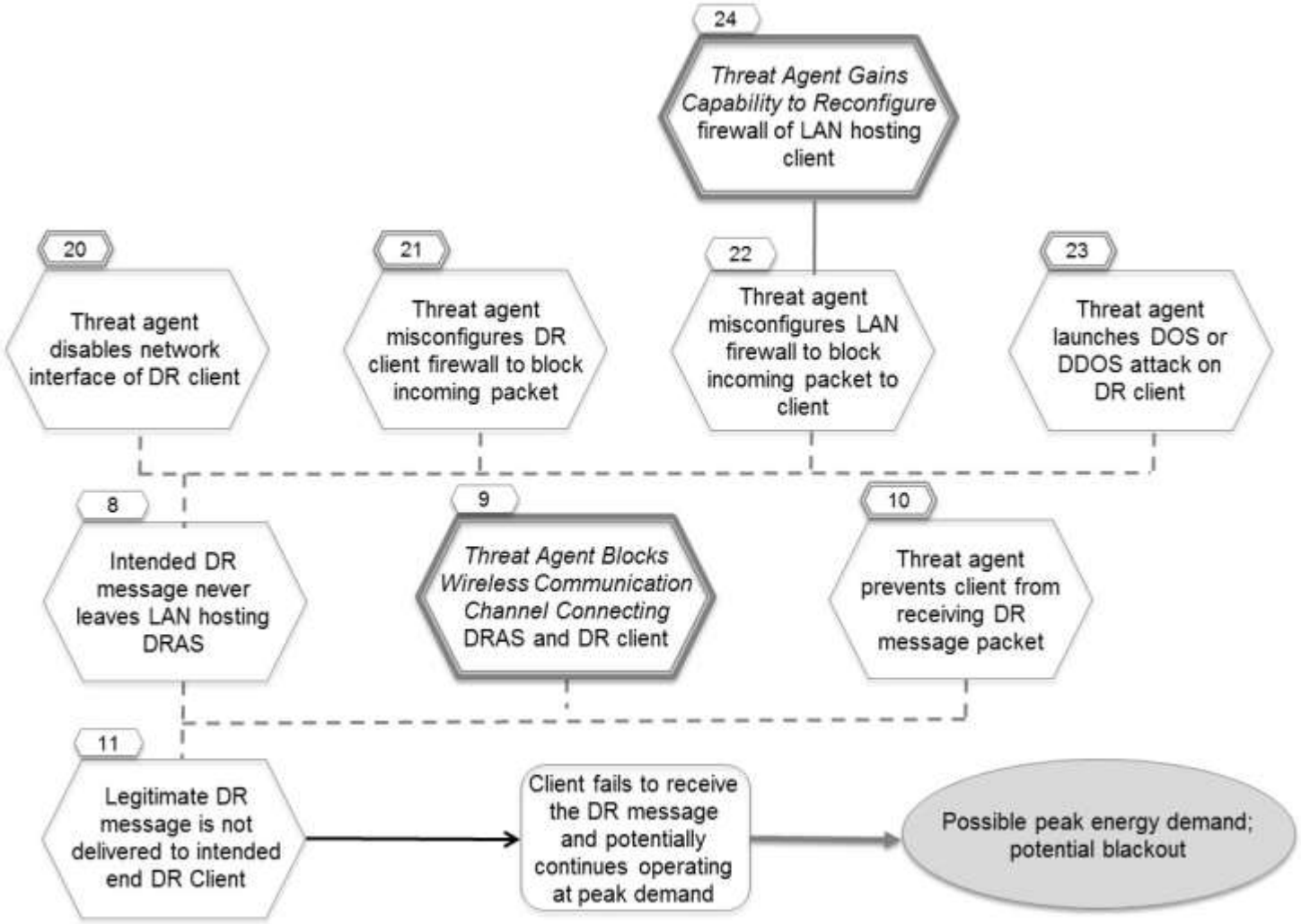

Figure 25
Blocked DR Messages Result in Increased Prices or Outages (7/8)

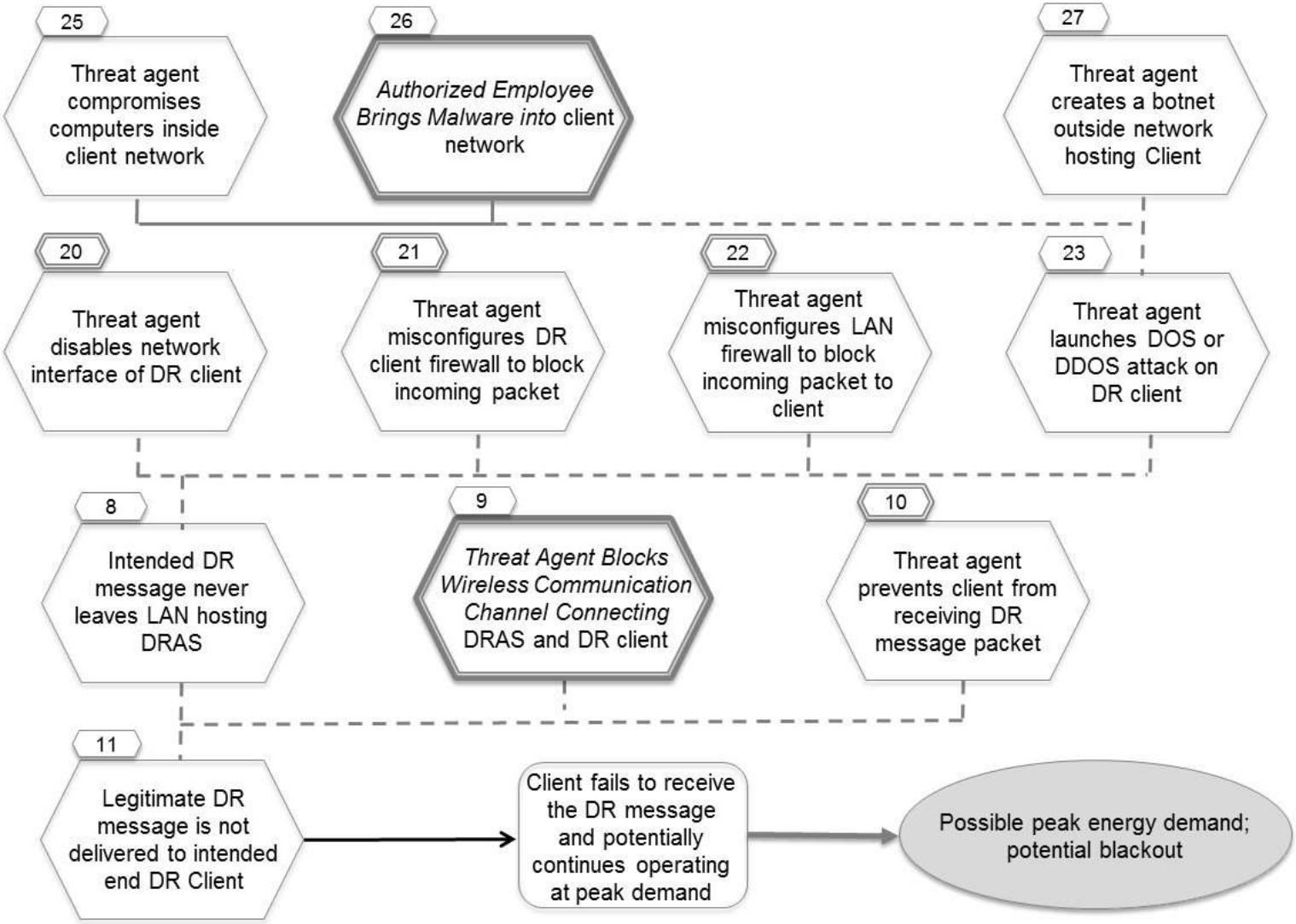

Figure 26
Blocked DR Messages Result in Increased Prices or Outages (8/8)

3.9 DR.4 Improper DRAS Configuration Causes Inappropriate DR Messages

Description: A threat agent unintentionally or maliciously modifies the DRAS configuration to send (or not send) DR messages at incorrect times and to incorrect devices. This could deliver a wrong, but seemingly legitimate set of messages to the customer system.

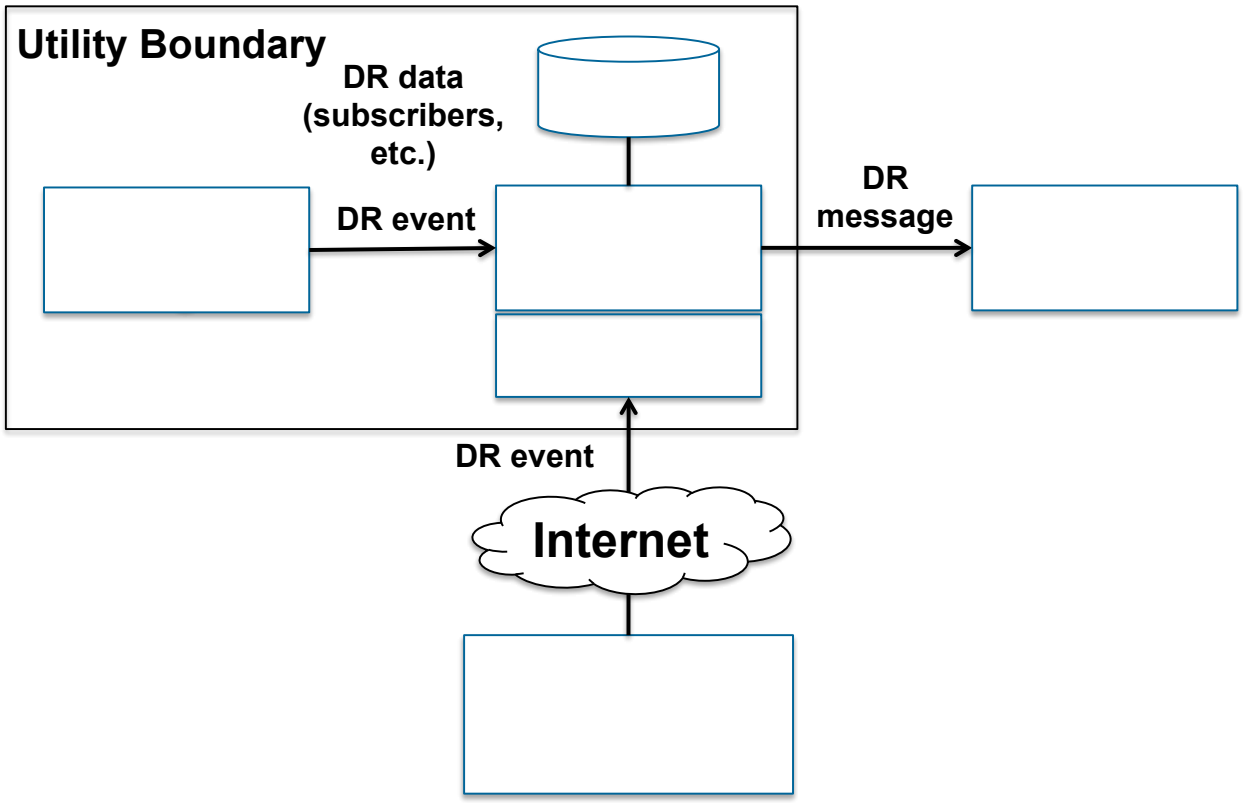

Figure 27
Architecture for DR.4 Scenario

Assumptions

- DRAS issues a DR message when receiving DR event information in the following ways. (1) Business Logic feeds DR event to DRAS automatically based on its analysis; (2) Authorized manager manually generates and feeds DR event to DRAS through management GUI.

Potential Mitigations

Conditions apply to the following figure(s).

- See common sub tree *Threat Agent Gains Access to Network <specific network>* (Condition 1)
- See common sub tree *Threat Agent Obtains Legitimate Credentials for <system or function>* (Conditions 2, 13)
- *Generate alerts* on changes to configurations on DRAS; *Detect unauthorized configuration changes*; *Create audit log* of DR messages generated; *Require second-level authentication* to change configuration (Condition 3)
- *Validate inputs*, specifically the reasonableness of DR event (Condition 5)
- *Validate inputs,* specifically the reasonableness of DR event (Condition 6)
- See common sub tree *Threat Agent Finds Firewall Gap* (Condition 7)
- See common sub tree *Authorized Employee Brings Malware into <system or network>* (Condition 8)
- *Require application whitelisting* (Conditions 9, 11)
- *Conduct penetration testing*; *Perform security testing*; *Maintain patches* in DRAS host; *Maintain anti-virus* (Condition 11)
- *Use RBAC* to limit generation of DR event; *Generate alerts* on changes to configurations on Business Logic; *Detect unauthorized configuration changes*; *Create audit log* of DR events generated (Condition 14, 15)
- *Generate alarm* on unexpected DR event generation (Condition 15)
- *Maintain patches* in DRAS GUI host; *Maintain anti-virus*; *Detect unauthorized connections* to DRAS GUI; *Restrict Internet access* to DRAS GUI (Condition 18)

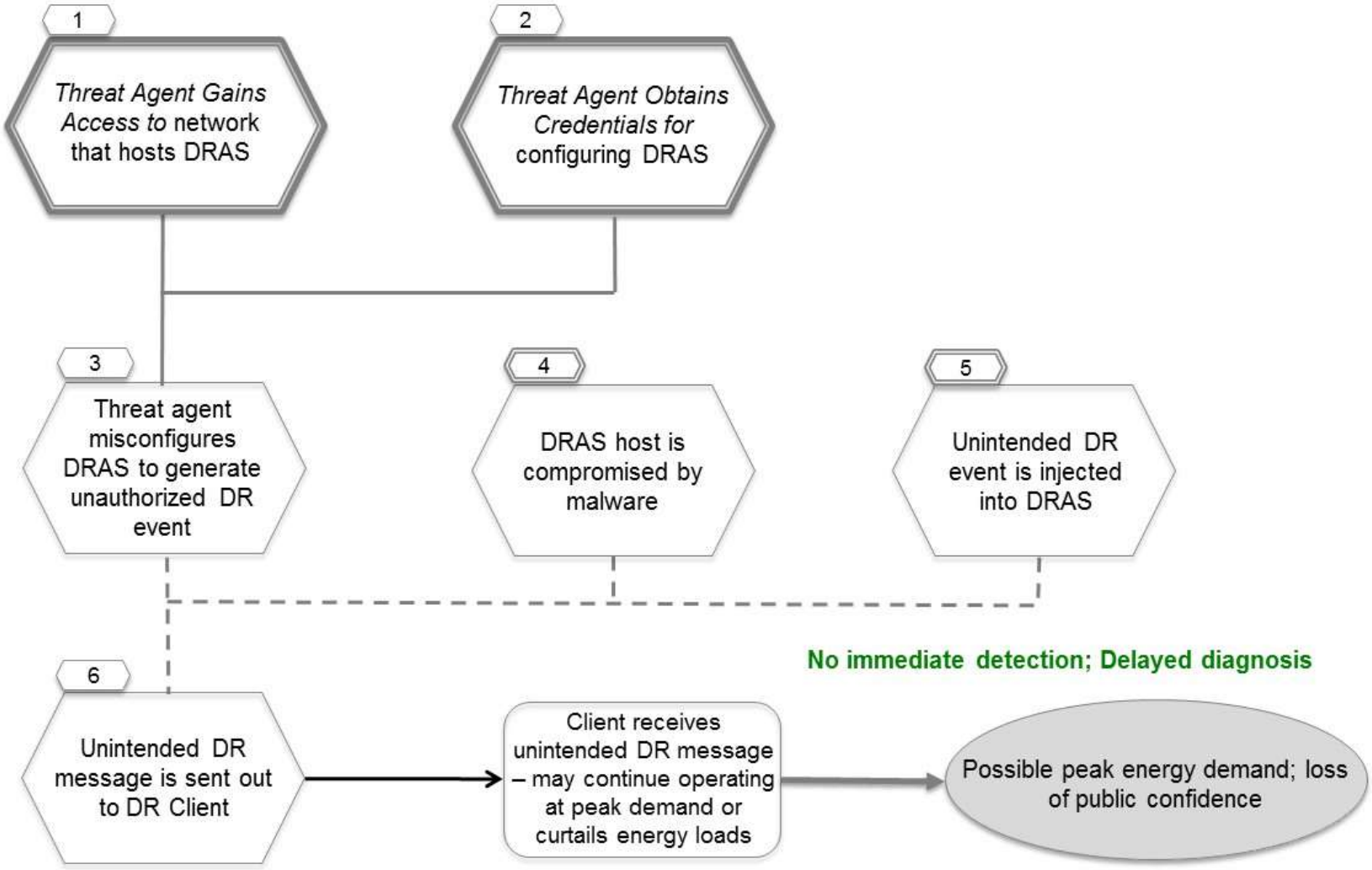

Figure 28
Improper DRAS Configuration Causes Inappropriate DR Messages (1/4)

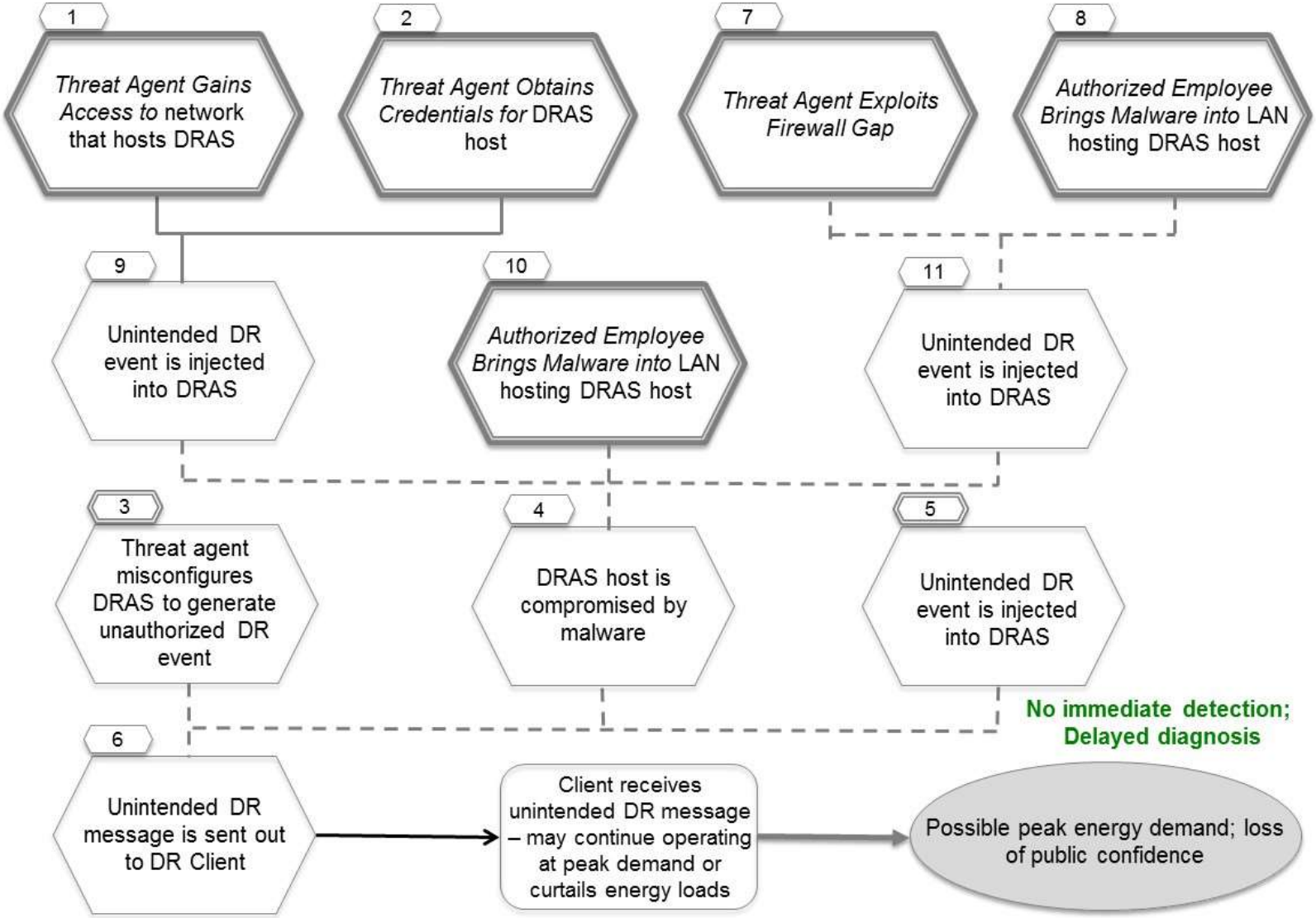

Figure 29
Improper DRAS Configuration Causes Inappropriate DR Messages (2/4)

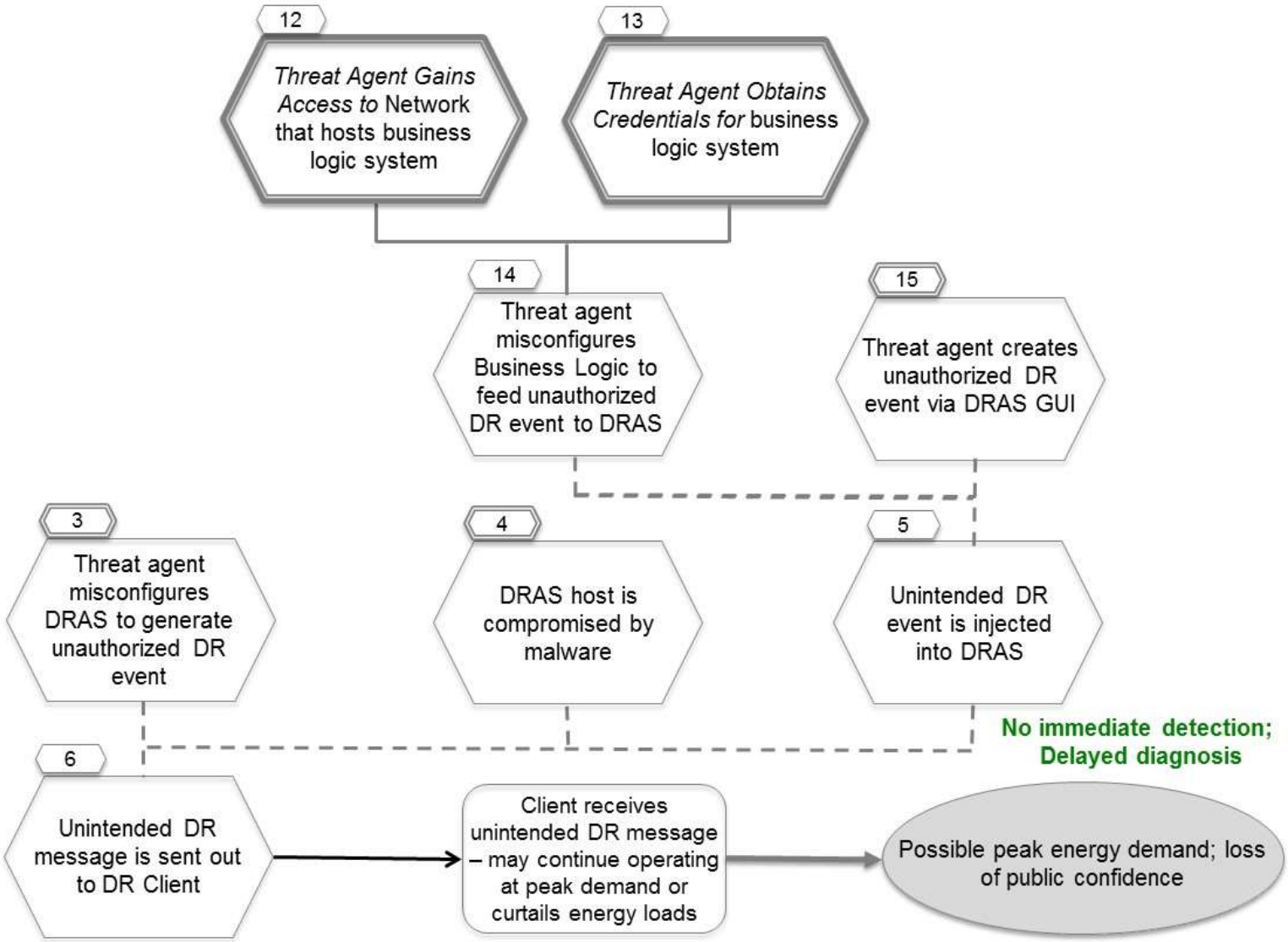

Figure 30
Improper DRAS Configuration Causes Inappropriate DR Messages (3/4)

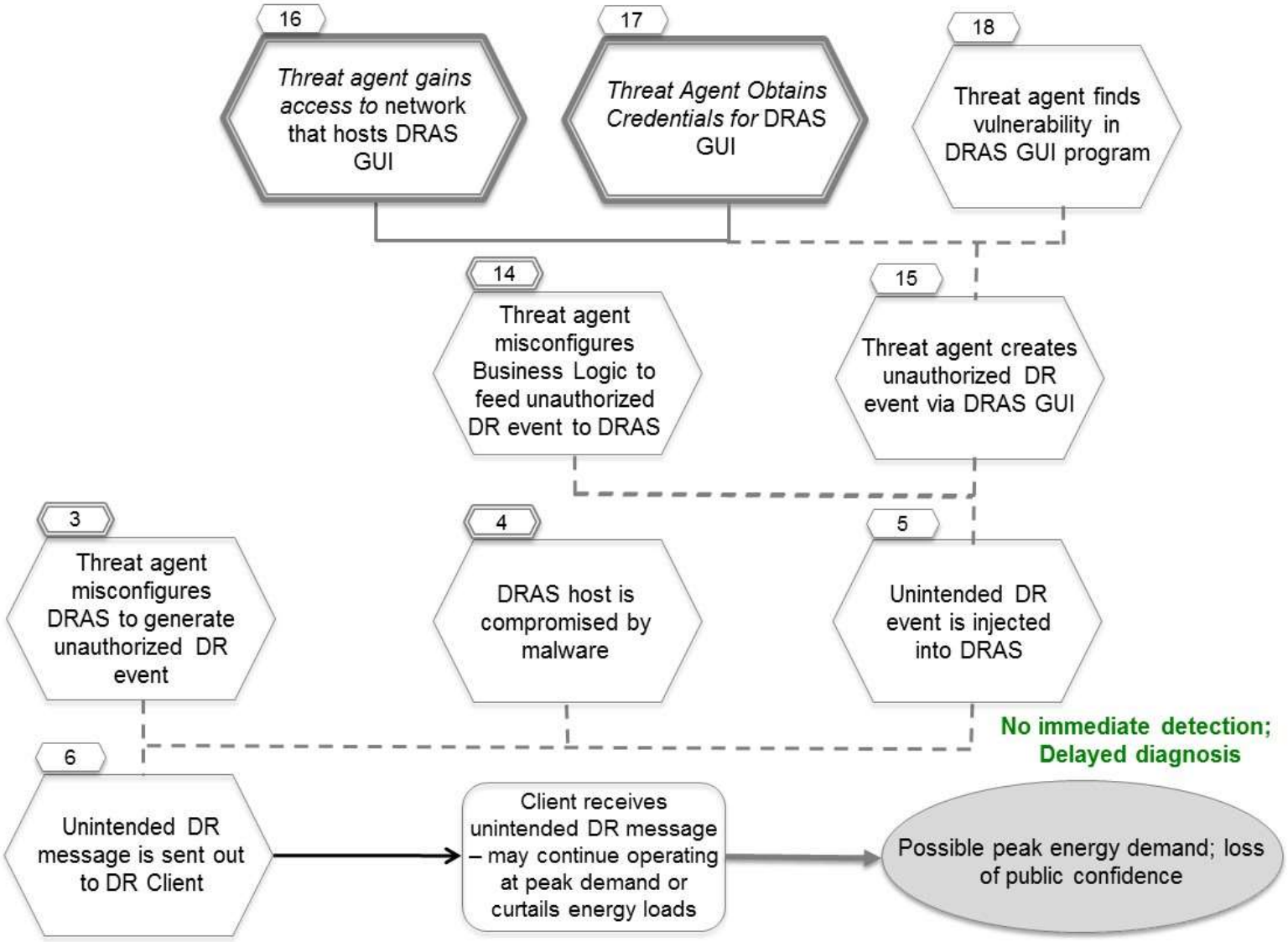

Figure 31
Improper DRAS Configuration Causes Inappropriate DR Messages (4/4)

4 COMMON SUB TREES

The following trees have been identified while creating the failure scenario attack trees, by understanding where there are common branches that occur in several situations. They have been abstracted into trees that can be instantiated via the bracket '<>' notation, where the bracket is then filled in with appropriate detail when the common tree is used in a failure scenario tree.

4.1 Threat Agent Gains Capability to Reconfigure Firewall

Description: A threat agent gains the capability to change firewall rules on a specific firewall to permit types of traffic to flow through the firewall that will enable future attacks.

Assumptions

- Threat agent has access to a network with a firewall interface

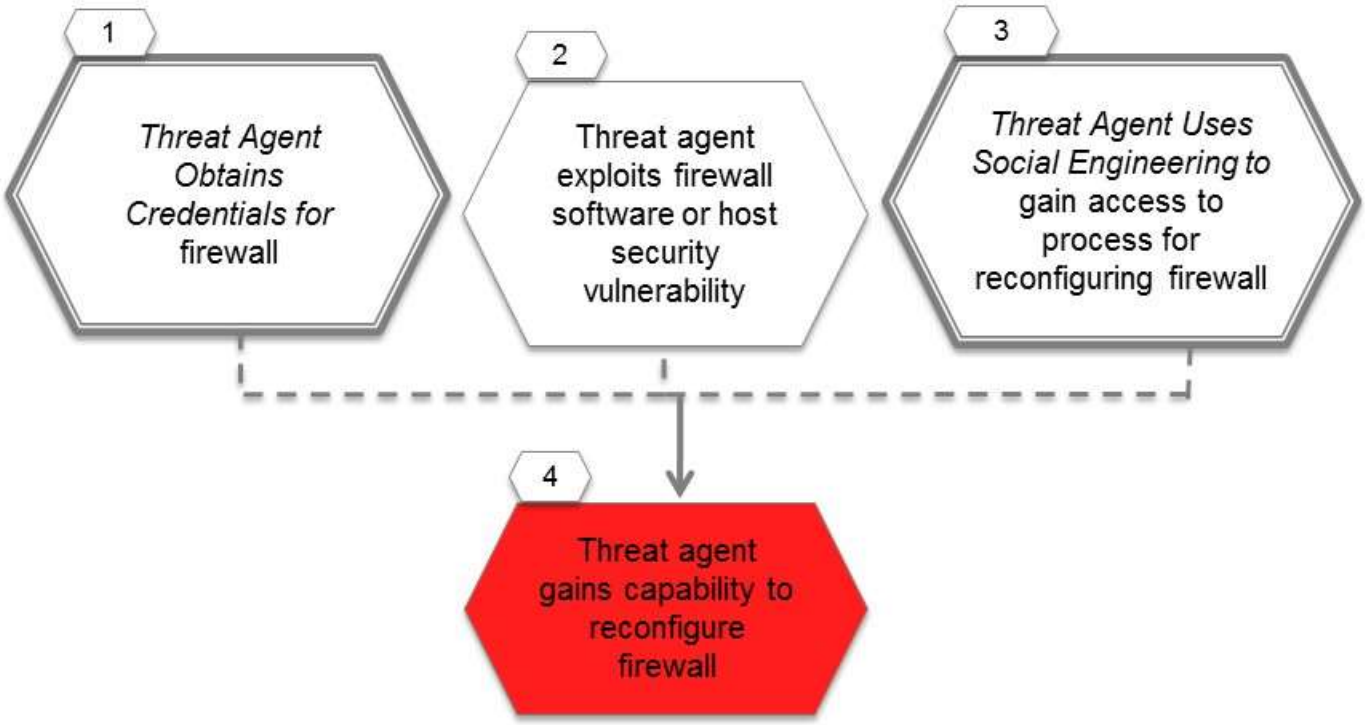

Figure 32
Threat Agent Gains Capability to Reconfigure Firewall

Mitigations

Mitigations apply to the conditions included in the figure above.

- See mitigations for common sub tree *Threat Agent Obtains Credentials for <system or function>* (Condition 1)
- *Conduct penetration testing* to uncover firewall vulnerabilities (Condition 2)
- *Implement configuration management* for the firewall system (Condition 2)
- *Maintain patches* on firewall system (Condition 2)
- *Detect unauthorized access* through traffic monitoring, specifically to detect reconnaissance; *Generate alarm* on detection (Condition 2)
- *Require intrusion detection and prevention* (Condition 2)
- *Create audit log* of attempts to access firewall host (Condition 2)
- *Require authentication* for system and database access to firewall (Condition 2)
- *Restrict database access* on firewall to authorized applications and/or locally authenticated users (Condition 2)
- See mitigations for common sub tree *Threat Agent Uses Social Engineering to <desired outcome>* (Condition 3)

4.2 Threat Agent Blocks Wireless Communication Channel

Description: The threat agent stops the flow of messages on a wireless communication channel connecting two entities, or slows it down to a point that it is essentially stopped.

Assumptions

- The backbone network for this wireless channel is wired, e.g., the Internet. Therefore, the wireless communication connecting <x and y> consists of two wireless channels in the access networks: node/station x to the wireless Access Point (AP) and the wireless AP to node/station y. Assuming these two channels are functionally the same, this common sub tree considers the wireless channel between the wireless AP and a node/station, x or y. The terms ‘sender’ and ‘receiver’ refer to the entity that sends or receives the wireless signal, respectively, which may be an AP or a node/station.

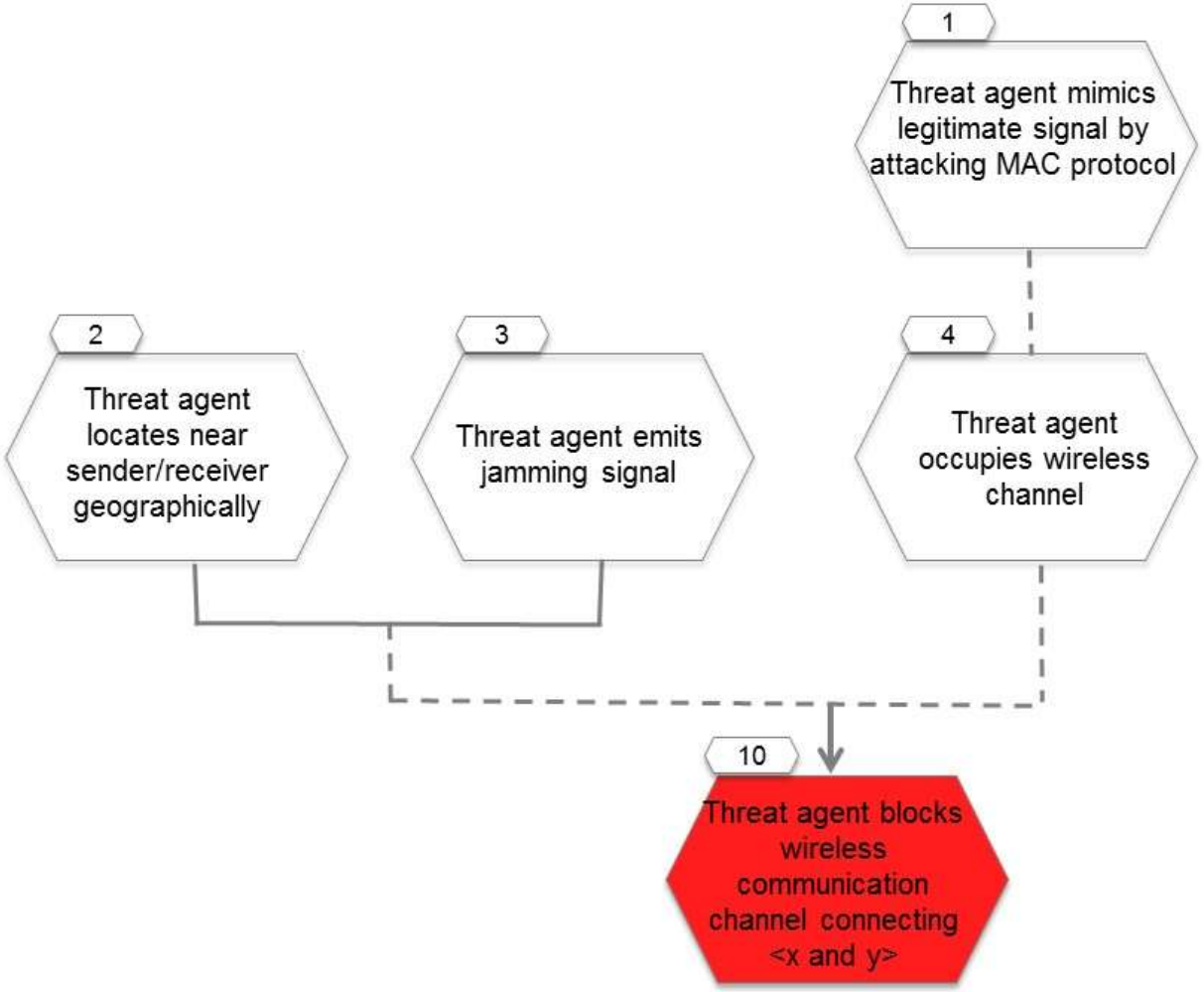

Figure 33
Threat Agent Blocks Wireless Communication Channel (1/2)

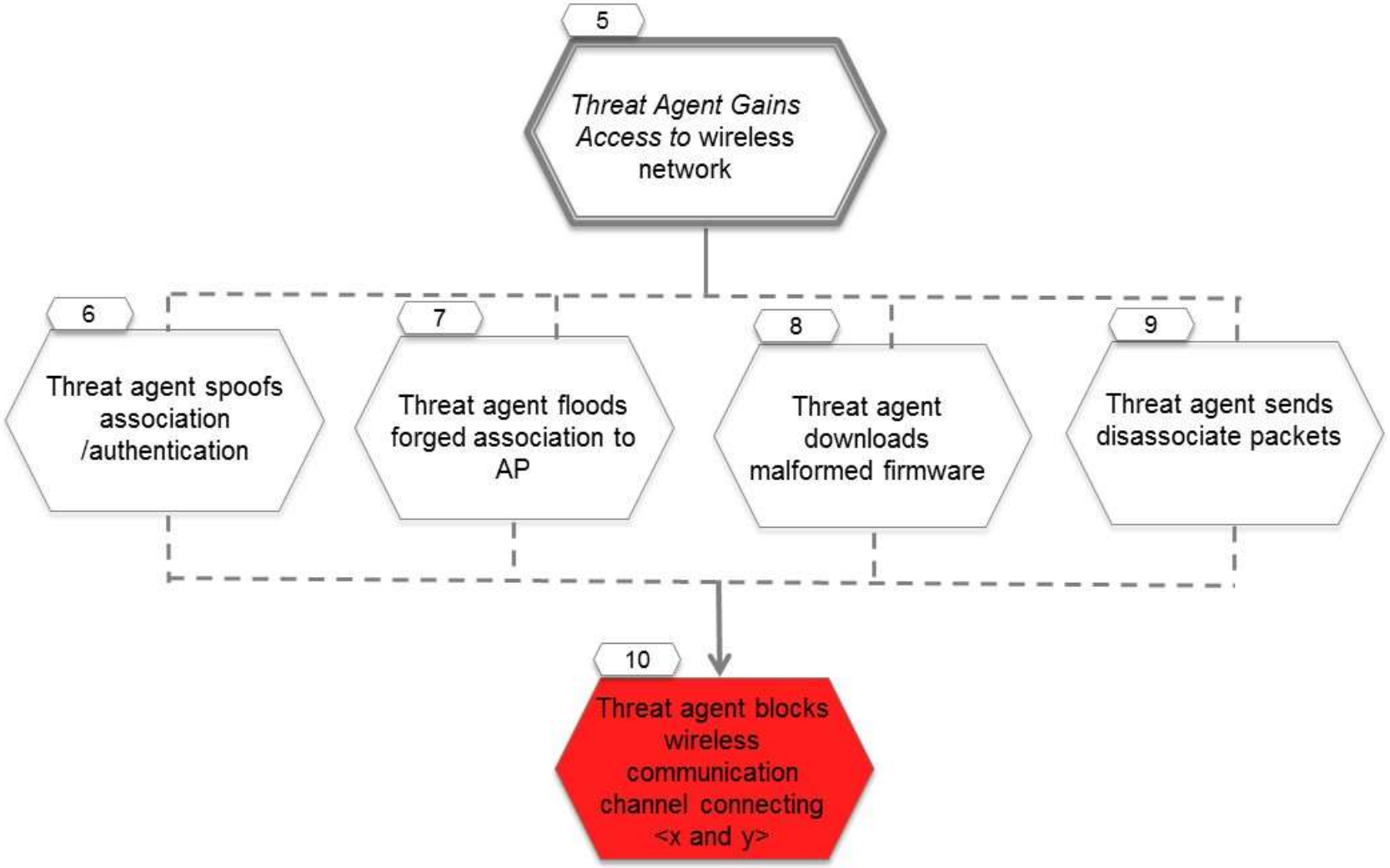

Figure 34
Threat Agent Blocks Wireless Communication Channel (2/2)

Mitigations

Mitigations apply to the conditions included in the figures above.

- *Create audit logs* for network connectivity; *Restrict remote access*; *Require multi-factor authentication* (Condition 1)
- *Restrict physical access* to APs and nodes/stations (Condition 2)
- *Detect unusual patterns* on wireless channel; *Generate alarm* on detection (Condition 3)
- *Create audit logs* for network connectivity (Condition 4)
- See mitigations for common sub tree *Threat Agent Gains Access to <network>* (Condition 5)
- *Detect unusual patterns* on authentication and association for wireless communication (Condition 6)
- *Generate alarm* on detection of abnormal association delay (Condition 7)
- *Generate alerts* on changes to configurations; *Detect unauthorized configuration changes; Maintain patches* on all systems; *Maintain anti-virus* on all systems (Condition 8)
- *Generate alarm* on network disconnection (Condition 9)

4.3 Authorized Employee Brings Malware into System or Network

Description: An authorized employee uses the IT infrastructure to perform any action that results in the introduction of malware onto a specific network or a system.

Assumptions

- The network under discussion is protected by perimeter security tools (e.g., enterprise firewall), and communications within the local network is less restricted (e.g., no port number filtering and internet protocol (IP) address filtering). Once a compromised device is connected to the local network, the malware may infect other systems in the network. A compromised device may be remotely controlled by a threat agent.

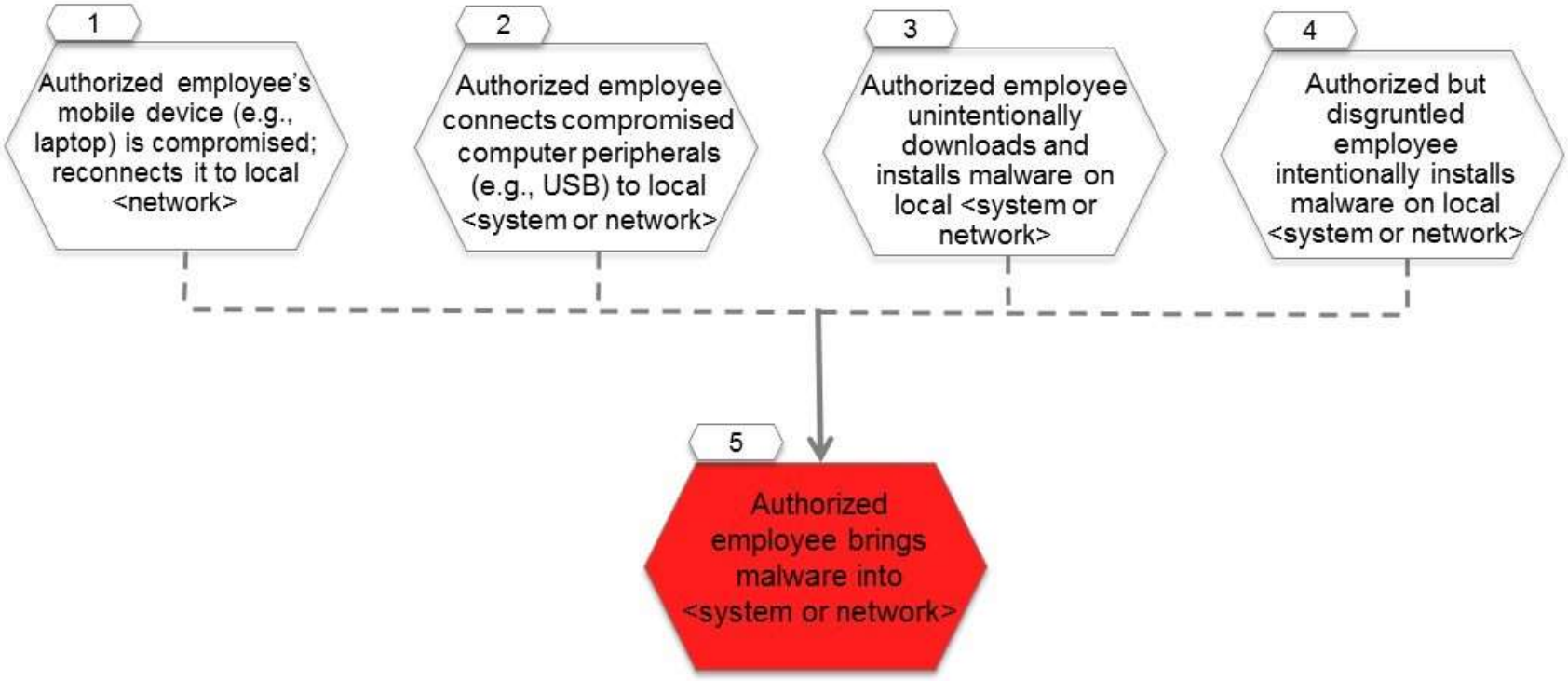

Figure 35
Authorized Employee Brings Malware into System or Network

Mitigations

Mitigations apply to the conditions included in the figure above.

- *Train personnel* regarding possible paths for infection to internal network (Conditions 1, 2, 3)

- *Maintain patches* on all systems; *Maintain anti-virus* on all systems; *Require intrusion detection and prevention* (Conditions 1, 2, 3, 4)

- *Create policy* regarding connection of mobile devices and peripherals to the network; *Test for malware* before connecting mobile device or peripheral to local network (Conditions 1, 2)

- *Verify personnel* to find any previous actions against employers (Condition 4)

4.4 Threat Agent Obtains Credentials for System or Function

Description: A threat agent may gain credentials for a system, or credentials that provide privileges to perform specific functions, in a number of ways. This includes finding them, stealing them, guessing them, or changing them. The threat agent may use social engineering techniques to carry out these methods. Each technology and implementation used for credentials is resistant to some methods and susceptible to others

Assumptions

- Credentials used are either any static piece of data (referred to as a password), biometrics, or a physical object (such as a key card/token). If multi-factor authentication is used, such as a token with a PIN, the adversary must take additional steps to obtain all “factors” of the credentials.

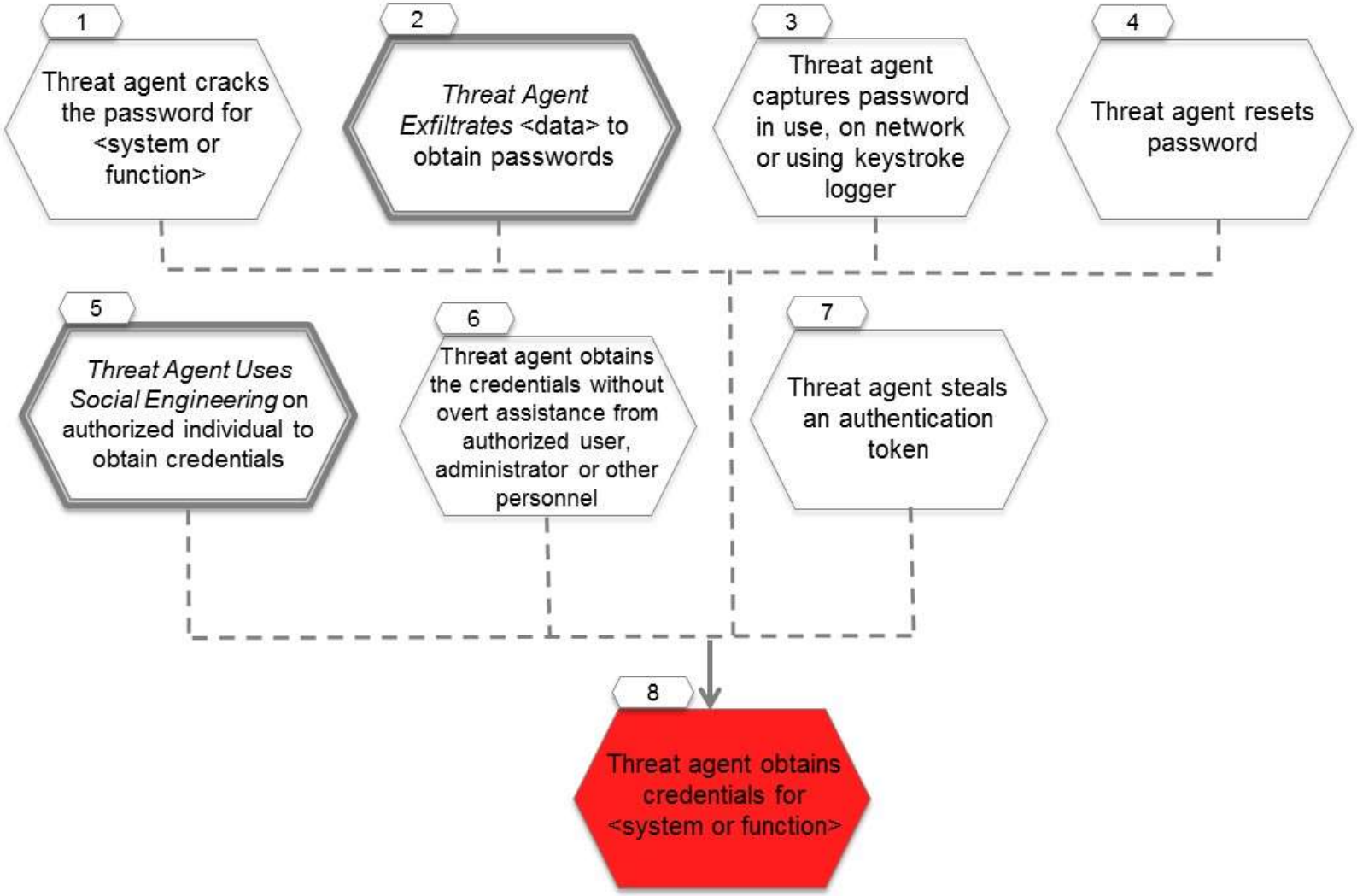

Figure 36
Threat Agent Obtains Credentials for System or Function

Mitigations

Mitigations apply to the conditions included in the figure above.

- *Design for security* by using strong passwords (Condition 1)
- See mitigations for common sub tree *Threat Agent Steals File* (Condition 2)
- *Design for security* by not recording clear text passwords in log files (Condition 2)
- *Test for malware* on user devices (Condition 3)
- *Design for security* by not sending passwords in the clear over the network (Condition 3)
- *Encrypt communication paths* on the network (Condition 3)
- *Protect against replay* on the network (Condition 3)
- *Design for security* by using strong security questions and protect answers (Condition 4)
- See mitigations for common sub tree *Threat Agent Uses Social Engineering to obtain <desired information or capability>* (Condition 5)
- *Design for security* by using strong security questions and protect answers; *Require multi-factor authentication* (Condition 6)
- *Require multi-factor authentication* such as using a token with a PIN (Condition 7)
- *Define policy* regarding reporting and revocation of missing tokens (Condition 7)

4.5 Threat Agent Uses Social Engineering

Description: A threat agent uses techniques of social engineering to persuade a victim to perform a desired action that results in an outcome that benefits the threat agent. Common examples of actions are to disclose particular information or to install/execute software that collects information or harms the victim's IT environment.

Notes:

- The attack tree provides an overview of the use of social engineering, there are many varieties
- More details and common examples may be found at: http://www.social-engineer.org/framework/Social_Engineering_Framework

Assumptions

- None currently identified

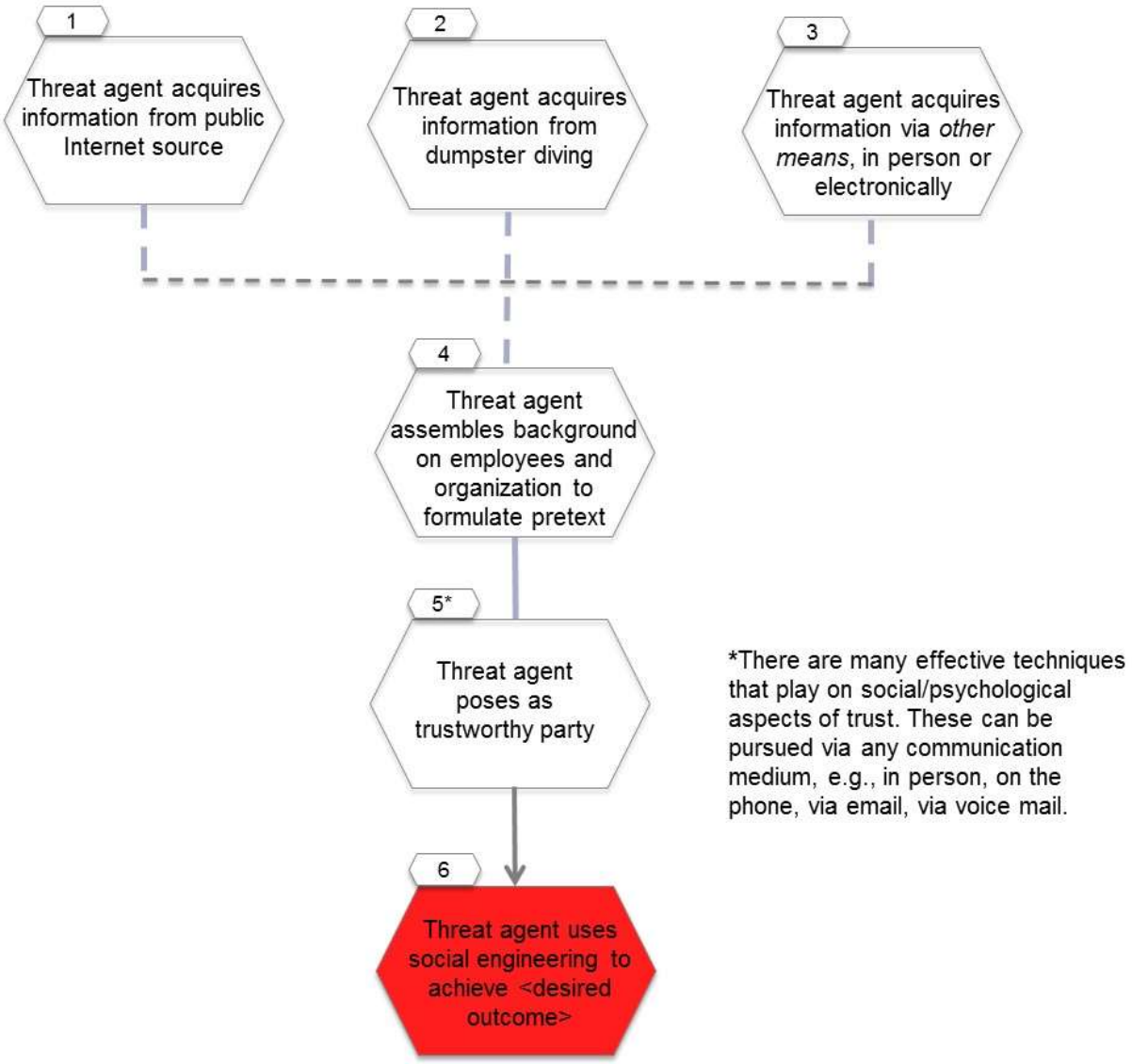

Figure 37
Threat Agent Uses Social Engineering

Mitigations

Mitigations apply to the conditions included in the figure above.

- *Define policy* to minimize Internet disclosure, e.g., “do not make calendars public” (Condition 1)

- *Conduct penetration testing* periodically, posing as a threat agent (Conditions 1, 2, 3, 5)

- *Define policy* to minimize leakage of physical artifacts (e.g., shredding, locked receptacle) (Condition 2)

- *Train personnel* that they are potentially targeted for these types of attacks and the consequences for the organization (Condition 5)

- *Train personnel* to report social engineering attacks (Condition 5)

- *Track social engineering attacks and warn personnel* (Condition 5)

- *Train personnel* including users and administrators in procedures to foil threat agents, e.g., always call back to the number in the directory (Condition 5)

4.6 Threat Agent Exploits Firewall Gap

Description: An authorized employee either accidently or intentionally sets a firewall rule that allows an exploitable form of access to a network from another network.

Assumptions

- None currently identified

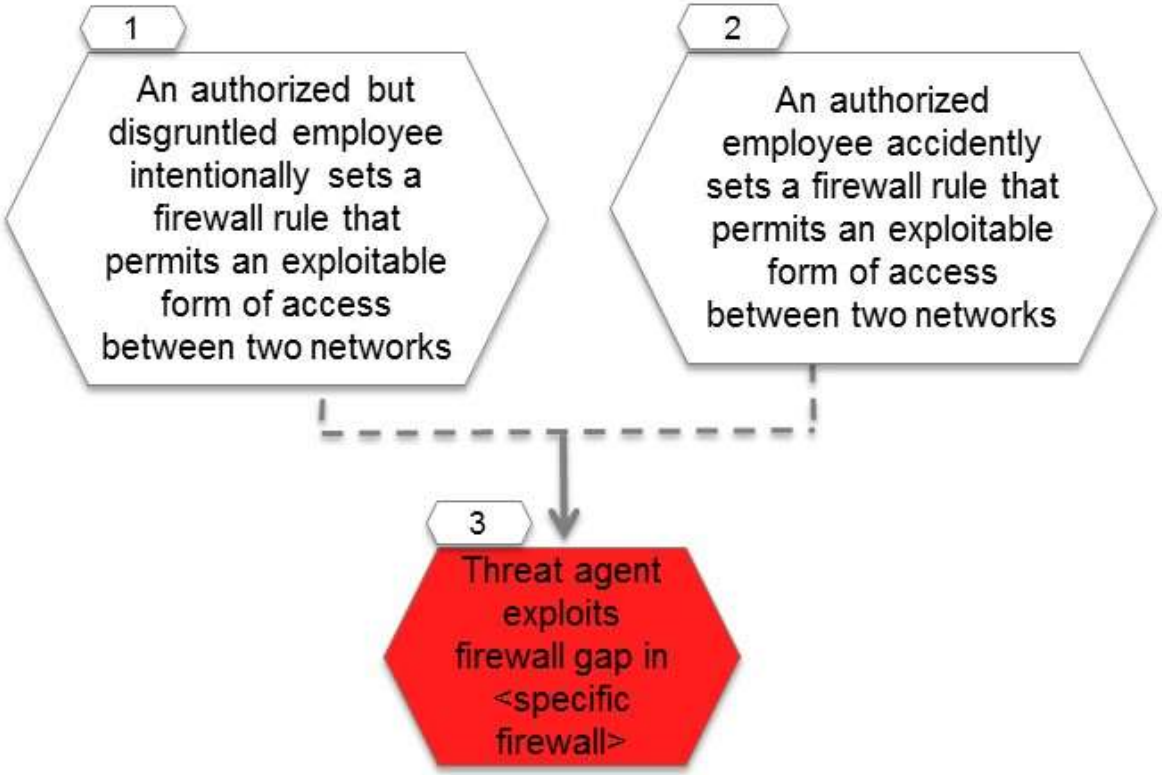

Figure 38
Threat Agent Exploits Firewall Gap

Mitigations

Mitigations apply to the conditions included in the figure above.

- *Conduct penetration testing* to uncover firewall gaps, *implement configuration management* to protect entire system (Conditions 1, 2)
- *Verify all firewall changes* (Conditions 1, 2)
- *Require intrusion detection and prevention* (Conditions 1, 2)
- *Require authentication* to network (Conditions 1, 2)
- *Restrict database access* to the firewall to authorized applications and/or locally authenticated users (Conditions 1, 2)

4.7 Threat Agent Exfiltrates Data

Description: A threat agent may use direct or indirect methods to obtain data, including a direct break-in to the host, finding the data on back-up media, scanning peripherals such as printers, and use of social engineering to influence a victim to give them the data.

Assumptions

- None currently identified

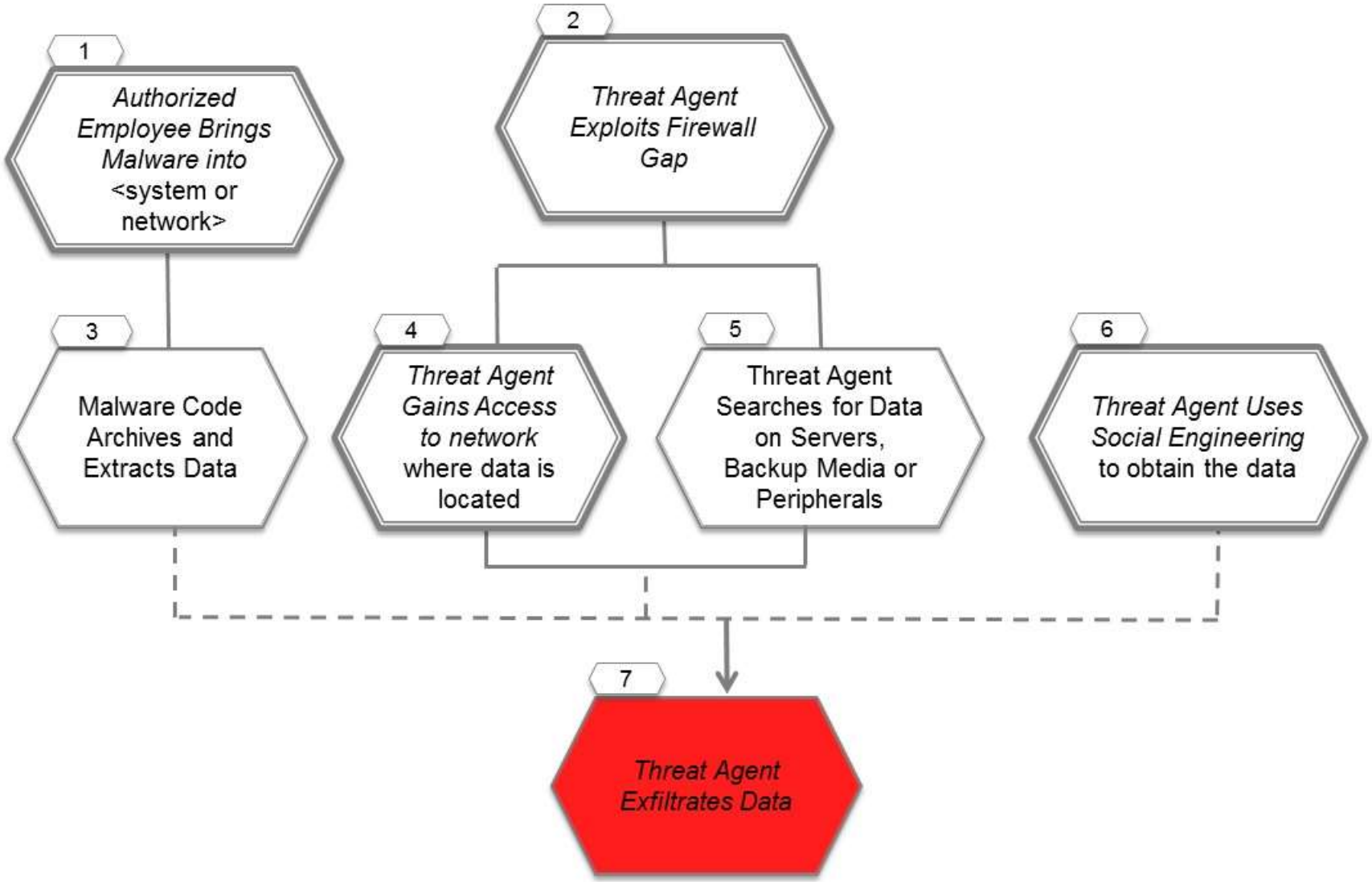

Figure 39
Threat Agent Exfiltrates Data

Mitigations

Mitigations apply to the conditions included in the figure above.

- *Train personnel to protect against malware (Condition 1)*
- *Test for malware on system or network (Conditions 1, 3)*
- *Require on-going validation of software/firmware* (*Condition 1*)
- See mitigations for common sub tree *Threat Agent Exploits Firewall Gap in <specific firewall> (Condition 2)*
- *Detect abnormal output* (unexpected data or destinations) (Condition 3)
- See mitigations for common sub tree *Threat Agent Gains Access to <network> (Condition 4)*
- *Authenticate users to servers, backup media, and peripherals (Condition 4)*
- *Enforce least privilege for individuals with access to hosts on the network (Condition 4)*
- *Detect unusual patterns of usage on hosts and network (Condition 5)*
- See mitigations for common sub tree *Threat Agent Uses Social Engineering to <desired outcome> (Condition 6)*

4.8 Threat Agent Gains Access to Network

Description: A threat agent becomes capable of sending traffic within a network and attempting to communicate with its resident hosts.

Assumptions

- None currently identified

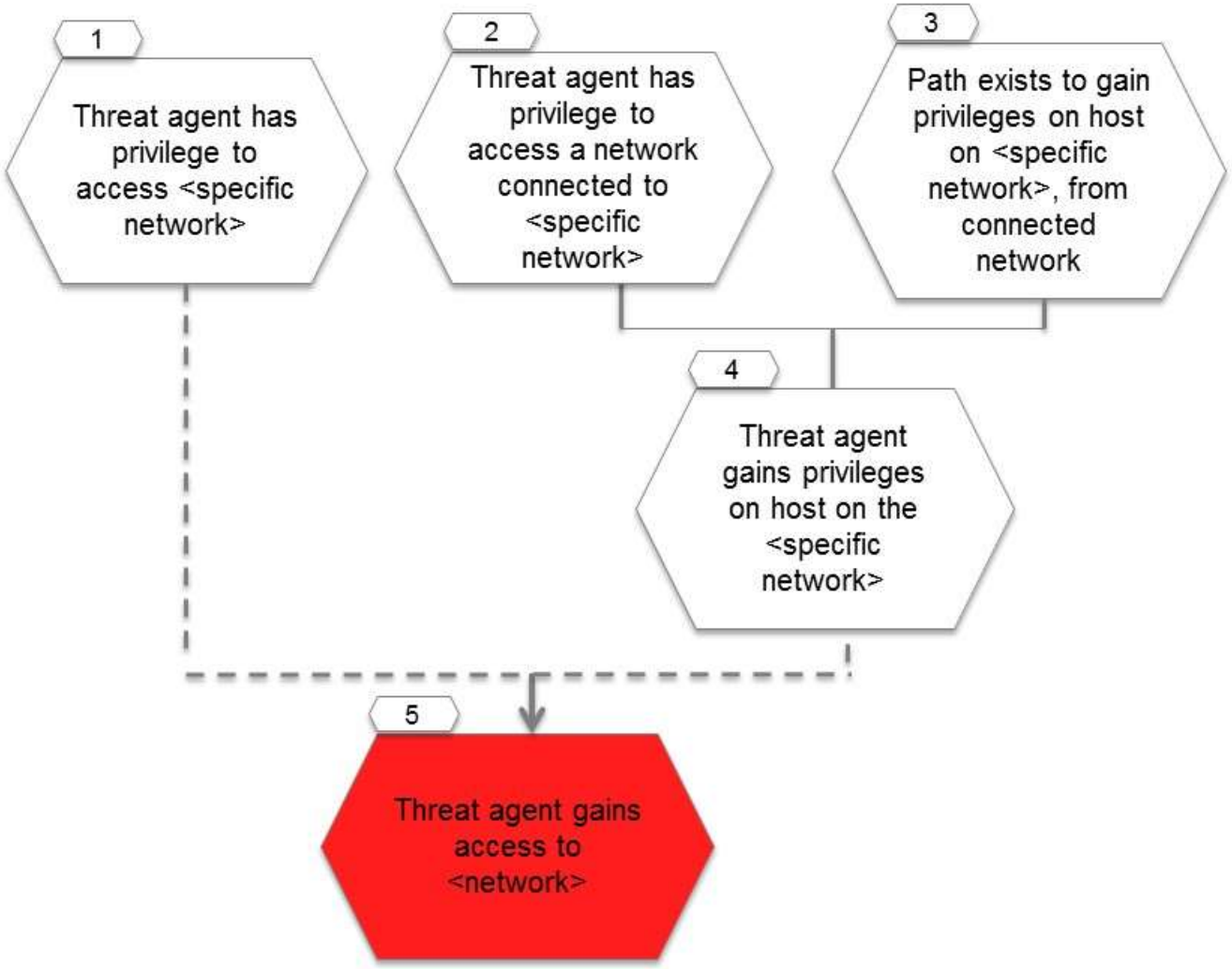

Figure 40
Threat Agent Gains Access to Network

Mitigations

Mitigations apply to the conditions included in the figure above.

- *Enforce least privilege* to limit individuals with privilege to the network and connected networks (Conditions 1, 2)
- *Isolate network* (Condition 2)
- *Enforce restrictive firewall rules* for access to network (Condition 3)
- *Design for security* by limiting connection points to networks that are widely accessible and by limiting number of hosts on same network (Condition 3)
- *Require authentication* to the network (Condition 3)
- *Enforce least privilege* for individuals with access to hosts on the network (Condition 4)
- *Detect unusual patterns* of usage on hosts and network (Condition 4)

5 ACRONYMS

ACL	Access Control List
ADR	Automated Demand Response
AMI	Advanced Metering Infrastructure
API	Application Programming Interface
APN	Access Point Name
AVR	Automatic Voltage Regulator
CA	Certificate Authority
CAPEC	Common Attack Pattern Enumeration and Classification Schema
CCTV	Closed-Circuit Television
CDEMS	Customer DER Energy Management System
CD-ROM	Compact Disk - Read Only Memory
CF	Compact Flash
CIS	Customer Information System
CPP	Critical Peak Pricing
DER	Distributed Energy Resources
DERMS	Distributed Energy Resources Management System
DGM	Distribution Grid Management
DHS	Department of Homeland Security
DMS	Distribution Management System
DMZ	Demilitarized Zone
DOE	Department of Energy
DoS	Denial-of-Service
DR	Demand Response
DRAS	Demand Response Automation Server
ET	Electronic Transportation
EV	Electric Vehicle
EVSE	Electric Vehicle Service Equipment
GPS	Global Positioning System
GSM	Group Special Mobile

HAN	Home Area Network
HMI	Human-Machine Interface
IDS	Intrusion Detection System
ICMP	Internet Control Message Protocol
IED	Intelligent Electronic Device
IPS	Intrusion Prevention System
JTAG	Joint Test Action Group
LAN	Local Area Network
LSS	Line Sharing Switch
LTC	Load Tap Charger
MDMS	Meter Data Management System
MITM	Man-in-the-Middle
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NESCOR	National Electric Sector Cybersecurity Organization Resource
NTP	Network Time Protocol
OC	Optical Carrier
OpenADR	Open Automated Demand Response
OPSEC	Operational Security
PCC	Point of Common Coupling
PDC	Phasor Data Concentrator
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLC	Power Line Carrier
PMU	Phasor Measurement Unit
PWM	Pulse-Width Modulation
QoS	Quality of Service
RBAC	Role-Based Access Control
REP	Retail Energy Provider

RF	Radio Frequency
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SD	Secure Digital
SEP	Smart Energy Profile
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SVC	Static VAR Compensators
TOU	Time-of-Use
TPM	Trusted Platform Module
TWG	Technical Working Group
USB	Universal Serial Bus
V2I	Vehicle-to-Infrastructure
V2G	Vehicle-to-Grid
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAMPAC	Wide Area Monitoring, Protection, and Control
WAN	Wide Area Network

Appendix A Glossary of Mitigations

The following glossary terms support the detailed failure scenarios presented in this document. Unless noted otherwise, all definitions below are derived from NISTIR 7298, Revision 2, *Glossary of Key Information Security Terms*. The purpose of this glossary is to avoid duplicating identical information across a number of scenarios, but provide convenient access to this information when using the failure scenarios.

Access Control Policy Also known as *Access Control List*, describes the access permissions associated with a resource. The policy describes who or what is allowed to access the resource and what operations are allowed to be performed on the resource. For example, an access control policy for a database might allow a user to read the contents of specific tables.

Acknowledgment A reply sent by the receiver of a message, to indicate they have received it. [New definition]

Alarm An Alert that is accompanied by a visible or audible indicator that typically requires a user action to dismiss. An alarm escalates the severity of an Alert and demands immediate attention. An example is a notification that sensitive data has been changed. See Alert. [New definition]

Alert Notification that a specific attack has been directed at an organization's information systems. Unlike an Alarm, an alert may not require immediate attention from a user. For example, an alert might be generated when unsuccessful attempts to change sensitive data were detected. See Alarm.

Application Whitelisting For systems with a relatively stable set of software running, a method of limiting the particular software that is permitted to run on the system. Permitted software is usually identified by a hash value. Whitelisting is contrasted with blacklisting, which is an attempt to identify software that should not be permitted to run. Possible issues in using whitelisting are: weak implementations in which the whitelisting function is easily turned off or bypassed, management of whitelisting functionality for software updates, and software that is not whitelisting friendly (e.g., DLLs being dynamically loaded/unloaded, small applications being called from other applications, custom configurations, and very old code).

Artifact An information object to which access must be controlled, using either physical or logical (i.e., computer-based) means. An artifact must be protected from unauthorized disclosure or modification. Examples include paper-based files, computer-based records, and similar objects. [New definition]

Association delay (related to wireless) A condition of concern where the time required to authenticate a wireless device with an available wireless access point takes

longer than expected. Such a condition may indicate a man-in-the-middle attack where the attacker pretends to be the wireless access point in order to intercept and observe all wireless communications from the device. [New definition]

Clear Text Information that is not encrypted. Sensitive information such as a password should not be stored on information systems or transmitted between information systems without protections such as cryptography. This will prevent it from being observed or modified.

Configuration Management Also known as *Configuration Control*, is the process of controlling modifications to hardware, firmware, software and documentation to protect the information system against improper modification prior to, during, or after system installation. For example, the source code used to build information systems should be placed under configuration management.

Digital Signature A method of cryptography. An asymmetric key operation where a private key is used to compute a unique hash for ("digitally sign") data and a public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation. For example, the binary file containing a software program might be digitally signed to ensure that tampering and modification are detected, but the digital signature would not prevent the software program from being executed.

Execution integrity - A property of software that is executing, in particular, that the intended, authorized version of the software is actually executing. Execution integrity may be compromised at any phase of the software install/load process. [New definition]

Intrusion Detection A technique of gathering and analyzing information from various areas within a computer or network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). For example, an organization may deploy intrusion detection on its network to watch for unauthorized network traffic that bypassed the organization's network firewall.

Intrusion Prevention A method of detecting intrusive activity but also attempting to stop the activity, ideally before it reaches its target. See Intrusion Detection. For example, an organization may deploy intrusion prevention software on a computer host to detect and block malicious software that gains a foothold on that host.

Least Privilege The security objective of granting users only those accesses they need to perform their official duties. Also, the principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. For example, the typical user

on an information system should not be granted access to perform administrative functions on that system.

Malware A program that is inserted into a system (often covertly) with the intent of compromising the confidentiality, integrity or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. An example is malicious software that transmits sensitive data, such as credit card numbers, from the victim's computer to the Internet.

Message Authentication Cryptographic protections applied to individual messages communicated over a network that ensure that the sender of the message is matches what is claimed by the message header. These protections are especially important for messages containing commands to change sensitive data such as configuration settings. [New definition]

Multi-factor Authentication Using two or more factors to authenticate a user (i.e., verify the identity of that user) to an information system. Factors include: (i) something the user knows (e.g., password/PIN), (ii) something the user has (e.g., cryptographic authentication device, token), or (iii) something the user is (e.g., biometric). An example would be requiring a token along with a PIN.

Network Isolation The act of logically or physically separating two or more computer networks so that activity conducted on one network cannot adversely affect activities being conducted on a different network. Logical separation may include the use of a computer firewall with very restrictive rules or the use of different cryptographic keys to protect the traffic on each network. An example of network isolation is the recommended separation of the business enterprise network from the control network in industrial control systems. [New definition]

Patch An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

Penetration Testing A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system. Penetrating testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability. For example, an assessor might leverage both known flaws and social engineering attacks (e.g., pretending to be a system administrator to gain sensitive information from an unsuspecting user) to gain access to the information system.

Reconnaissance Also called the *discovery phase*, the phase of a cyber attack where information gathering about the target system occurs. The discovery phase occurs in two parts: the first part is the start of actual testing and includes information gathering and scanning, and the second part is the vulnerability analysis, which compares the information gathered against known vulnerability databases in order to identify fruitful attacks. An attacker may conduct reconnaissance for weeks or months and so usually seeks to avoid detection during this phase. [Source: NIST SP 800-115]

Replay Attack An attack that involves the capture of transmitted information (e.g., system messages, authentication or access control information) and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access. Replay attacks can be especially damaging to cyber physical systems that lack integrity checks on commands that alter device configuration settings, because repeated transmissions can put the device in a dangerous or unstable state.

Security Question A challenge issued to a user where the user's response provides evidence of something the user knows (see Multifactor Authentication), to authenticate the user's identity. The user typically inputs the correct response when the user's account is first established, so subsequent challenges verify that the provided response is the correct one. The user should select security questions whose responses cannot be gleaned easily from other sources. [New definition]

Token An object possessed or controlled by a user that is used to authenticate the user's identity. A token is typically considered to be something the user has, such as a cryptographic key or smartcard, as opposed to something the user knows (e.g., a password) or something the user is (e.g., biometrics). The token may be presented alone or in combination with other authentication factors (see Multifactor Authentication).

Appendix B Rationale for Selection of Failure Scenarios

B.1 General

This section presents the rationale for selection of particular failure scenarios in this document for detailed analysis. This selection process considered the results of a ranking process applied to all of the failure scenarios in [1]. A brief background on that ranking process is provided. The discussion also highlights failure scenarios of interest for future analysis work.

B.2 Ranking Failure Scenarios

After development of the short failure scenarios document, which contained over 100 scenarios, it became clear that a method of ranking the failure scenarios was required to prioritize further work. NESCOR TWG1 agreed that the correct method for prioritization was by level of risk represented by the failure scenario. To estimate risk for the scenarios, a set of detailed criteria that relate to risk was developed and tested for several scenarios. Ultimately, however, a rougher ranking method was executed over all of the scenarios. A complete description of this work is found in [1]. Here, a summary is provided as background to aid in understanding of the method for selection of failure scenarios for the present document.

The rough ranking method provides a number representing the benefit to cost ratio of carrying out the attack represented in the failure scenario, from the point of view of the threat agent. Thus a failure scenario with a higher ranking has a higher benefit to cost ratio for the threat agent, and therefore represents a higher risk to the utility. It was understood that the rough ranking method would not qualify as a scientific study; however it was felt it be sufficient for prioritizing the work of TWG1, which was its purpose.

To rank the scenarios, five different sub teams within TWG1 independently assigned numerical scores to two criteria for each scenario. These criteria are:

- Impact, considering all types of impacts (as 0,1,3, or 9 from low to high impact)

- Cost to the adversary, considering the overall difficulty and financial cost to the threat agent to carry out the failure scenario (as 0.1, 1, 3 or 9 from low to high cost to the adversary)

Examples to guide the scoring were given to the teams. The overall ranking assigned by each sub team was then calculated as Impact divided by the Cost to the adversary.

The level of consensus, among the teams as well as the scores, was considered to place the failure scenarios into four ranking categories as follows. The approach intended to weed out failure scenarios with low impact, and to find the areas of strongest agreement among both high and low rankings.

Table 6
Failure Scenario Ranking Categories

Ranking Category	Description	Number of failure scenarios
1 (highest rank)	Three teams assigned rank ≥3 AND one team assigned impact ≥9 AND one team assigned impact ≥3.	7
2	Two teams assigned ranks ≥3, AND one team assigned impact ≥9 AND one team assigned impact ≥3.	17
3	Any scenario not in categories 1, 2 or 4	29
4	Three teams assigned rankings of ≤ 1, unless any team put a scenario in their top 20 OR any team gave it an impact of 9.	52

These ranking categories were used to assist in selection of failure scenarios for detailed analysis, as described in the following sections.

B.3 Rationale: Failure Scenarios Selected for Text and Attack Tree Analysis

- **AMI.1 Threat Agent Performs Mass Meter Disconnect**

Interest in the topic of AMI failure scenarios for mass meter disconnect was uniform across all of the utility members of TWG1. This is illustrated by the fact that it was the first failure scenario on the failure scenario list presented in [1]. This scenario was among those in the highest risk rank category in the rough risk ranking and the only scenario in category 1 among all AMI failure scenarios. Note that the AMI.1 scenario has an authorized individual as a threat agent. The utilities requested that the scenario be expanded to cover additional cases, and then split into several scenarios as needed to include all potential methods for an unintended mass meter disconnect. Such an outcome would not only harm those that relied for power on the individual meters involved in such an event, but also, in extreme cases, would harm the overall stability of the power grid due to a sudden loss of load. Remote on/off digital control for meters is a fundamental new element introduced with AMI, and the utilities are aware of its potential for harm as well as its benefits. There is interest in detailed analysis of all cases related to AMI.1, although only the original AMI.1 is addressed for this draft.

- **DGM.11 Blackout due to remote Distribution Grid Access**

The DGM scenario DGM.11 "Blackout due to remote distribution grid access" was a later selection by the group, and is not present in earlier versions of the short failure scenario document. This selection came about during a review of the set of failure scenarios in the highest-ranking categories, when the group noted that the DGM domain was likely underrepresented. This was thought to be because some of the DGM scenarios focused on narrow individual cases which themselves might be seen as unlikely. However, the overall set of variants of the scenario was of concern. In particular, the early version of DGM.11 had a more narrow scope; it was named "Data and Personnel equipment stolen to trip feeder lines." The group decided that the overall capability to gain remote access to the distribution grid, trip feeder lines and potentially cause a blackout, was the full scenario that should be considered, and that this broader scenario should have high priority. Broadly, the group believed it important for the detailed analysis effort to cover some aspects of distribution, since the impact can be similar to attacks on the transmission system, and distribution is not covered by the North American Electric Reliability Corporation (NERC) cyber security efforts. Thus the short scenario DGM.11 was revised and renamed, and a long scenario analysis for the broadened DGM.11 was developed for this document.

- **AMI.32 Power Stolen by Reconfiguring Meter via Optical Port**

This scenario was also not in the first set of scenarios in earlier versions of [1], and was added at a later time to that document. This failure scenario was specifically proposed by a utility member as a candidate for detailed analysis for two reasons: (1) at the 2012 NESCOR workshop, a demonstration was given of how to access the optical port on a meter and (2) news articles describing actual cases of this failure scenario were presented during a TWG1 conference call, that reported staggering losses to utilities. This information proved this scenario was real, which raised its priority. Further, potential mitigations were not obvious. There was a general consensus that failure scenarios such as this one that impacted revenue alone, should be given lower priority than those that impacted the provision of power or public safety. Nevertheless, in this case, since a real utility had found that 10% of their meters were tampered with and they lost $400M annually, the group decided to analyze this failure scenario.

B.4 Rationale: Failure Scenarios Selected for Attack Tree Analysis

B.4.1 AMI Failure Scenarios

Six AMI scenarios were selected for development of attack trees for this document. The AMI domain had a large number of failure scenarios, and a large number of failure scenarios of near term interest to the utilities. In this case, all of the ranking category 3 AMI failure scenarios were selected for development of attack trees. The plan was for later concurrent development of both text and attack trees for the failure scenarios in the second risk category. Treatment of the single category 1 failure scenario AMI.1, is discussed above.

B.4.2 DR Failure Scenarios

Attack trees were developed for two DR failure scenarios. TWG1 agreed that DR for individual residence customers does not have sufficient usage at this time to cause significant impact on a utility via the failure scenarios that had been identified. However, it was agreed that failure scenarios involving very large industrial DR customers could have a significant impact. The two DR failure scenarios in category 2 were selected for attack tree analysis. These deal with blocking of DR messages (DR.1) and an attack on the administration system that causes invalid DR messages to be sent (DR.4). There were no DR failure scenarios in ranking category 1.

B.5 Rationale: Failure Scenarios Not Analyzed

There are many more scenarios than could be analyzed for this first draft document, and which remain of near term interest to the utilities. There are also some failure scenarios that are felt not to be of short term interest for further analysis, although they may be of interest in the longer term. This section discusses rationale related to those scenarios not selected, specifically from the WAMPAC, DER, ET, and Generic domains.

Six of the eight WAMPAC domain failure scenarios fell into the top two ranking categories. This broad high ranking for the WAMPAC scenarios was due to the fact that members believed WAMPAC would be used in the future for applications such as stability monitoring that would directly impact the grid. Although WAMPAC is not often used in this way today, this was a clear path forward. All agreed that a WAMPAC scenario should be selected for detailed analysis as soon as possible, and that it would ultimately be useful to analyze most of the WAMPAC failure scenarios in detail.

DER failure scenarios overall had relatively low risk rankings. 15 of 25 were in category 4. This was because impacts on the utility were believed to be relatively modest. This is due to the current small scope of implementation for DER. The one scenario among the DER scenarios in category 1 (DER.1) discussed electrocution of a worker due to a live power resource that was not reported as live. The group judged that a failure in the cyber security domain in this case should be covered by the safety domain, and therefore analysis of this case would not yield new insights regarding cyber security.

The utilities believed that the cyber security impact of ET *from their perspective* was minimal at this time, and large impacts were far in the future. However, there are certainly critical privacy and safety impacts to be considered in the near term by other stakeholders, in particular manufacturers and owners of electric vehicles. Although the scenario ET.15 *Malware Causes Discharge of EV to the Grid* would touch the grid and the utility, it was believed that standard utility procedures would handle excess power in the amounts likely to be introduced via these events, even in quantity. The scenario ET.16 *EV is Exploited to Threaten Transformer or Substation* could become of interest to utilities in the future. It describes the potential for a virus infection passing from a vehicle through a charging station up to the utility infrastructure. Since current protocols do not have data flowing along this path, it appeared that a detailed analysis of this failure scenario at this time would not yield results useful to utilities. The scenario

should be considered, however, by groups in the process of defining such communication protocols.

Three of the four failure scenarios in the "Generic" category were placed in category 1. These covered the general topics of insider threat, network segregation and portable media. Although these were agreed to be critical topics, it was unclear whether the planned text and attack tree analysis formats would be a useful approach via which to address them. Other approaches would be the development of reference network architectures and example policies related to these topics.

Appendix C Failure Scenario Template

An initial step in developing the cyber security failure scenarios for the electric sector was to define how these failure scenarios would be documented. This "template" definition specifies both (1) the content that will be included when documenting a failure scenario and (2) the format in which this content will be presented. This section presents a working template, followed by the rationale for this template. The failure scenarios presented in this document use this template.

The template and rationale were first developed and presented in [1]. This material has been moved to the present document for maintenance going forward. Modifications made for the present document are:

- Additional detail added for the impact and mitigation topics in the text portion of the template
- Additional features added to the graphic attack tree notation, specifically to support the concept of common attack tree fragments.

C.1 Failure Scenario Template Overview

The fields in Table 6 define the information included for the failure scenarios described in this document. This information includes descriptive data about the failure scenario and information related to the likelihood and impact of the failure scenario. A failure scenario developed using the template will consist of a graphic (described in Section C.3 below) and accompanying text. The third column of Table 7 indicates the information in the template that is covered in the graphic. The following section defines the form of the graphic. The graphic provides an overview, while the accompanying text provides additional details that can't be included in the graphic.

TWG1 decided not to define a field in the template called "likelihood." The consensus was that this would be speculative and would also differ among the utilities. Rather, there is information in the template to assist a utility in considering the likelihood of a failure scenario.

Table 7
Failure Scenario Template - Content

Information	Comments	Covered in Graphic Format
Describe scenario		

Information	Comments	Covered in Graphic Format
Failure scenario ID		✓
Failure scenario name	Short descriptive name for the failure scenario	✓
General description of the failure scenario		
Assumptions	Key facts about the operational environment and architecture, mitigations in place	✓
Variants of scenario	Lists variants of this scenario that have impact on the potential mitigations	✓
Physical location for carrying out scenario	Clarifies aspects of the scenario could be carried out remotely and those that require physical access to equipment	
Threat agent(s)	Threat agents from in Appendix D	✓
Threat agent objective	Applies to malicious failure scenarios	
Steps in failure scenario – quality attribute scenario data	See description below of quality attribute failure scenario data	✓
Relevant vulnerabilities		✓

Information	Comments	Covered in Graphic Format
Relationship to the NISTIR 7628[2] logical reference model architecture (a.k.a. "spaghetti diagram")		
Analyze impact		
Impact	Description of impact has two parts, a text description and a table, with content and format as described below in 2.1.1. It may include the effects on systems but should include ultimate business impacts such as health and safety, infrastructure damage, evaluations/displaced persons, economic and financial impacts, service disruption.	✓
Detectability of occurrence	For example - immediate, delayed, or not detectible - together with rationale and description of how detection takes place	✓
Recovery description and timeline	What actions are required for recovery and how long these actions take	

[2] National Institute of Standards and Technology, Department of Commerce, United States of America. Interagency Report 7628: *Guidelines for Smart Grid Cyber Security,* August 2010. Gaithersburg, Maryland.

Information	Comments	Covered in Graphic Format
Analyze factors that influence probability of occurrence		
Difficulty of achieving conditions	Discuss for each node of the attack tree, how difficult it is to obtain physical and/or logical access and tools/software required, as well as the skill level required to achieve the intermediate conditions represented by that node	
Potential for multiple occurrences		
Likelihood relative to other scenarios	For example, specify if same impact can be achieved using simpler methods	
Mitigation		

Information	Comments	Covered in Graphic Format
Potential mitigations	Lists prevention and deterrence methods, and advanced or early detection and response methods that could stop the full scenario or possible impacts from occurring. Include paragraph text describing how each mitigation applies to this failure scenario. Mitigations may include cybersecurity controls as well as examples of power system operational practices. A discussion of all relevant power system operational practices is not expected. Refer to glossary of mitigations, as appropriate.	✓
Organizations involved in failure scenario and recovery	Refer to standardized list of organizations to select from to fill in this template item.	
References		
Source scenario(s)	Initial scenarios that this failure scenario covers, from list in NESCOR TWG1 "Electric Sector Failure Scenarios and Impact Analysis," Nov 9, 2012 [1].	

Information	Comments	Covered in Graphic Format
Publications	For example, reports of incidents of this scenario in the electric sector, similar cases in other sectors, or discussions of technical feasibility.	

The quality attribute scenario concept comes from the reference *Software Architecture in Practice*, by Bass, Clements and Kazman[3]. The specific quality attribute scenario data used in the failure scenario steps are *source*, *stimulus,* and *response*. The source is the actor (human or system) that takes the action (stimulus) for the step. The response is what the system does following the action. The concept of source also incorporates relevant characteristics of the actor, such as whether or not the individual is authorized to take the action. For example, a step in a failure scenario could be an authorized employee (source) executes a command to disconnect a meter (stimulus) and the system in response disconnects the designated meter and logs the transaction (response).

C.1.1 Impact Categories

Impact is the effect of the failure scenario on the delivery of power, the business of the utility, and the interests of its customers. As noted in the prior section, in the write up for a failure scenario, description of impact includes a discussion of important impacts of the scenario followed by a table that lists common categories of impacts and marks which of these are relevant to this scenario. The text description should be as specific as possible, in terms of both factor and magnitude (which may be a range). This would include possible cascading effects. The purpose of this table is to assist the author and reader in identifying as broad a range of potential impacts as possible. Below is an example of an impact discussion and the table of impact categories to be used in the impact section for a failure scenario.

Example:

[3] Len Bass, Paul Clements, and Rick Kazman, Software Architecture in Practice, Second Edition, Addison-Wesley Professional, 2003.

Impact:

e) Loss of customer power might spread to entire service area
   - Depending on the sequence of the feeders tripped, timing of attack, severity of cascading effects (if any), and utility response, power loss can range from select feeders supplying a town, to portions of a suburb, a large city, or a large geographic area

b) Possible customer and utility equipment damage
   - Voltage sags and swells could damage customer electronic equipment
   - Shifting electrical load might overload transformers and switchgear or blow fuses,
   - Oscillatory behavior might damage distribution level generation

c) Disclosure of proprietary utility documents or information
   - SCADA employee names and contact information
   - Precise location of critical feeders
   - Brand and model numbers of equipment
   - Network architecture of DMS communications
   - Installed operating systems and software, version numbers, patch levels
   - Password requirements and cyber security countermeasures
   - Policy and procedure documentation

The table below shows those general categories of impacts that are most relevant to this scenario, as they relate to the discussion above.

Table 8
Categories of Impact for a Specific Scenario

	Impact category	Text reference
1	Public safety concern	[a]
2	Workforce safety concern	
3	Ecological Concern	
4	Financial Impact of Compromise on Utility (excluding #5)	
5	Cost to return to normal operations	[a] [b]
	Impact category	**Text reference**

6	Negative impact on generation capacity	[a]
7	Negative impact on the energy market	
8	Negative impact on the bulk transmission system	[a]
9	Negative impact on customer service	[a] [b]
10	Negative impact on billing functions	
11	Damage to goodwill toward utility	[a]
12	Immediate macro economic damage	[a]
13	Long term economic damage	
14	Loss of privacy	
15	Loss of sensitive business information	[c]

C.2 Failure Scenario Template Rationale

The above description of the failure scenario template takes into account (1) the particular uses intended for the failure scenario documentation developed by NESCOR and (2) existing practice in the computer security community for documenting similar information.

The primary audience for the failure scenarios is utilities. A secondary audience will be other industry bodies working in related areas as well as other NESCOR working groups. The team discussion of uses for the failure scenario write-ups yielded the following list:

- Utility activities (primary)
  - Planning, (including selection of countermeasures)
  - Risk assessment,
  - Staff training,
  - Tabletop exercises,
  - Security testing,
  - Procurement.

- Activities by other industry organizations (as a by-product)
  - Security design analysis,
  - Security test input,
  - Find gaps in standards and best practices.

The information selected for the template was designed to support utility needs. For example, information included in “relevant vulnerabilities” and “difficulty of steps in attacks” may be used in a risk assessment. Information included in “potential mitigations” supports planning and procurement. Information included in “organizations involved in failure scenario and recovery” supports tabletop exercises.

The failure scenarios are not intended to define specific technologies or standards. This information is useful to other industry organizations but is outside the scope of this document. Information for “relationship to spaghetti diagram functions” will assist in driving specificity as well as permit placement of the issue being discussed in a context familiar to the overall community.

The team reviewed the CAPEC template “Common Attack Pattern Enumeration and Classification Schema” [4] as a comprehensive source for information that could be included in the NESCOR template. CAPEC is a Department of Homeland Security (DHS) funded effort to create a database of common attack patterns. CAPEC has developed a template for documenting each pattern, called the CAPEC schema. For example, the discussion of indications and warnings in the CAPEC schema pointed to the need to address the detection of an attack in the NESCOR template – this element was therefore added. Many CAPEC schema items parallel those in the NESCOR schema. The NESCOR template is not the same as the CAPEC schema, since the CAPEC effort is intended to address detailed failures of software (vs. sector functions), and to be both more generic in application (vs. industry specific) and more academically comprehensive.

Since the primary audience for the failure scenarios is utilities, the format for the template is designed for their needs. First, as much information as possible in the template is provided in a graphical format to facilitate comprehension and discussion among utility personnel of the important points about a failure scenario. The goal is to provide useful information to utility personnel, regardless of their background in cyber security. The graphically oriented format is a more effective format than a lengthy text document. The text portion of the template will include the information in Table 7 that is not included in the graphic format. The text information may also augment the information included in the graphic format. Utilities were particularly interested in text descriptions of potential mitigations, beyond the bulleted list shown in the graphic format. To avoid repeating general definitions for mitigations that might not be familiar to the audience, a glossary for these definitions is referenced where appropriate. The glossary can be found in Appendix A. The graphic format will be provided as a few PowerPoint slides that may be edited by a utility. Although other more powerful tools are available in the security community for creating and maintaining attack trees, these are not generally used by utilities – and delivering

[4] http://capec.mitre.org/about/documents.html

results as PDFs with such a tool as the source would limit customization by the users of the deliverable.

The detailed categories requested in the description of impact were developed by TWG1 for risk ranking of scenarios, and were reused in this context to improve the uniformity of discussions of impact across the failure scenarios.

The attack tree format is well known in the cyber security community[5]. The format is usually presented with leaves at the bottom rather than the top. The team decided to show leaves at the top since a flow of events from top to bottom is more logical. The addition of the concepts of source, stimulus and system response came from concepts for documenting Quality Attribute Scenarios found in *Software Architecture in Practice*, by Bass, Clements and Kazman[3]. NESCOR TWG2 is using these ideas for documenting use cases. These concepts will also drive a level of uniformity in the descriptions of the failure scenario conditions.

C.3 Failure Scenario Template Graphic

A graphic format suitable for development as a PowerPoint slide has been developed by TWG1 to provide a visual representation that describes a failure scenario in a concise manner. The template information that is included in the diagram is noted in the last column above. The graphical notation used is illustrated below and shows a modified annotated attack tree. Key aspects of this notation are:

- Each hexagon represents a condition in the sequence of conditions that make up a failure scenario. The leaves directly connected to and above a leaf represent the *full conditions* necessary for that lower leaf to occur. The *conditions* can be descriptions of several steps that must occur within a failure scenario.

- The tree is read from top to bottom, in terms of the sequence of conditions that occur. (This is a revision to the standard attack tree format – where the tree is followed from bottom to top. The objective was to provide a diagram that is easier to read.)

- A condition is labeled with the SOURCE that initiated that condition and the action (STIMULUS) that was initiated. A source is typically a human

[5] Schneier, Bruce (December 1999), "Attack Trees", *Dr Dobb's Journal, v.24, n.12*. http://www.schneier.com/paper-attacktrees-ddj-ft.html

actor or a cyber component.

- The numbers that label each hexagon (Condition) are ID's to enable a user to refer to specifics of the figure. They do not represent an ordering of condition.

- Connection of two conditions by a line means that the lower condition depends upon the higher condition.

- Connection by a dotted line means "OR", that is, a lower condition can occur if either one OR the other of the connected upper conditions occurs. If all upper conditions are required for a lower condition to occur, a solid line is used, representing "AND."

- At the bottom of the attack tree are two additional nodes – the first indicates what happens to the system after the failure scenario occurs (system response), represented with a rounded square, and the second describes the impact when this occurs, represented with an oval.

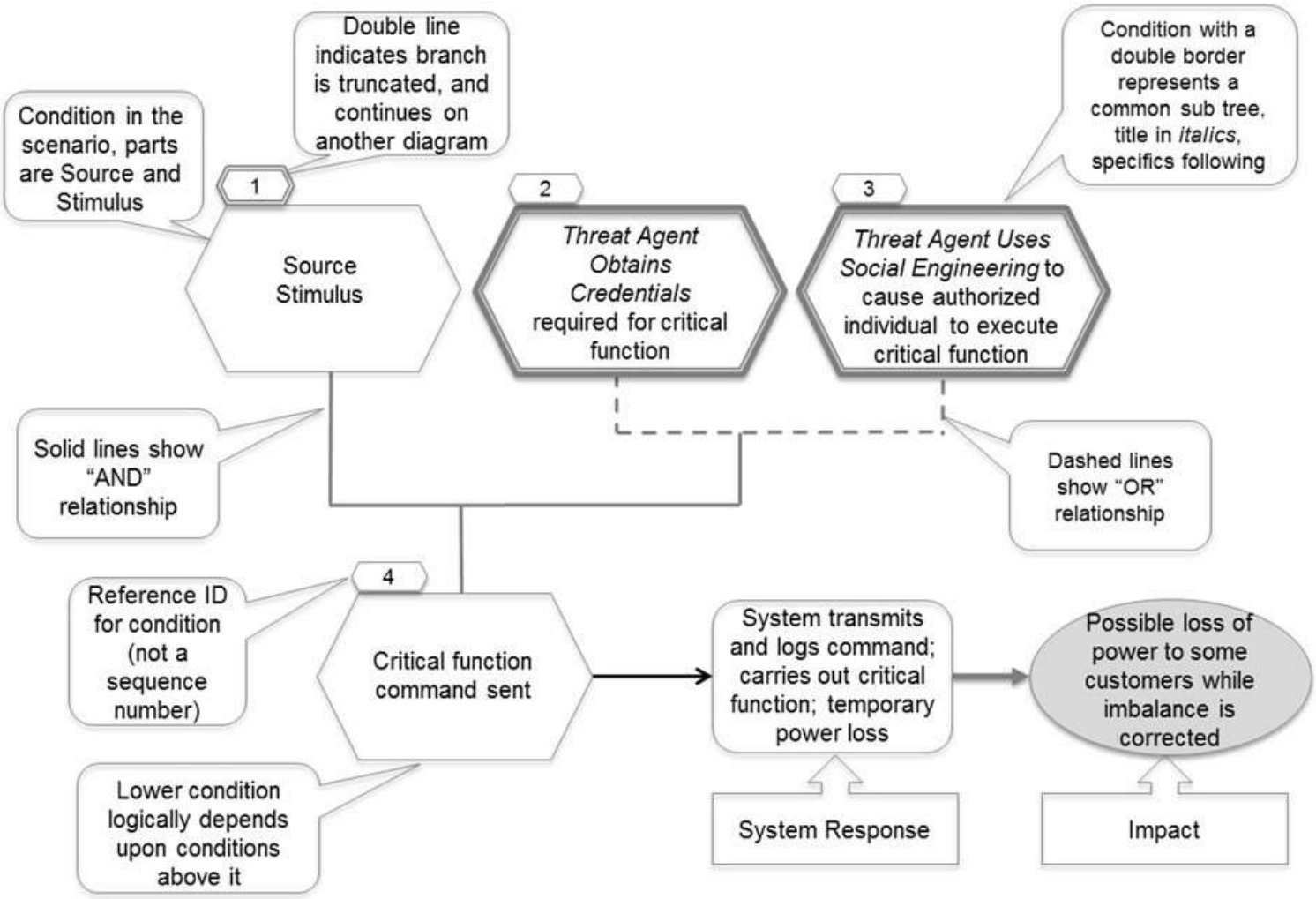

Figure 41
Graphical Notation for Annotated Attack Tree Format

Common Sub Trees are a simplification technique that represent those subsets used in many attack trees, and is represented as a hexagon with double outlines as shown. Creating modular subsets simplifies the specific attack trees by allowing those common details to be documented in their own trees. The specific trees then instantiate a Common Sub Tree with the pertinent context of how it is being referenced.

- The Common Sub Tree has a common name, such as *Threat Agent Obtains Legitimate Credentials*, but also include the context, "for system or function". The specific attack tree will then specify which system or function is referenced.

- The mitigation documented on the specific attack tree will state "See Common Sub Tree *Threat Agent Obtains Legitimate Credentials for <system or function>".*

Elements that are checked in the last column of Table 7, and included in the graphic format, but not represented in the above graphical notation are:

- Failure scenario ID,
- Short descriptive name for the failure scenario,
- Assumptions,
- Variants of scenario,
- Threat agent(s),
- Detectability of occurrence,
- Possible mitigations.

Variants of the failure scenario will be represented in the structure of the tree. The other elements will be added to the PowerPoint slide in the space surrounding the graphics. The scenario ID and the short descriptive name will be the title of the slide. This section also provides the accompanying text-formatted information for this failure scenario. See Section 2 and Section 3 for complete examples of the use of this template.

Appendix D Failure Scenario Threat Model

A *threat model* includes a list of the threat agents that were considered when developing failure scenarios. A *threat agent* is a class of actors that could cause a failure scenario to occur in some specified domain, either as the sole cause or as a contributor to it. Typical examples of threat agents are state-sponsored groups or individuals, insiders (whether malicious or non-malicious), and recreational criminals.

D.1 Threat Model Background

The threat model for this effort has several purposes. The first purpose is to support development of appropriate mitigation strategies for a failure scenario. This requires understanding the causes of the failure scenario. To be effective, mitigation strategies must take into account the motivation, tactics, and capabilities of those threat agents that may cause the failure scenario to occur. A second purpose is to aid in identifying failure scenarios that could otherwise be missed altogether, due to a lack of understanding of the full set of threat agents and their characteristics. The third purpose is to aid in prioritizing failure scenarios for analysis and mitigation. Failure scenarios that are given high priority should be considered to be of serious interest to a capable threat agent. Utilities do not have unlimited resources to address all potential threats and failure scenarios and they need to focus on the failure scenarios that are the most critical to the organization. The list of high priority failure scenarios will vary from utility to utility.

Therefore, a threat model is useful to the extent that it supports these purposes. A threat agent category should define a group of actors with similar characteristics that may contribute in a similar way to similar kinds of failures. The same types of potential mitigations should be applicable to all the threat agents in a threat agent category.

To scope the threat model more precisely, the team specified the term *failure scenario.* Specifically, these are *cyber security failure scenarios.* A cyber security failure scenario is a realistic event in which the failure to maintain confidentiality, integrity, and/or availability of sector cyber assets creates a negative impact on the generation, transmission, and/or delivery of power. The domain for the threat model here includes cyber security events that impact (1) delivery of electricity, (2) the business of running a utility and/or (3) the interests of the customers of a utility. In the following discussion, the term the “electric sector cyber security domain” is used.

D.1.1 Methodology for Development of the Threat Model

To develop a threat model for the electric sector cyber security domain, TWG1 identified a number of existing “reference” threat models, described in [1]. These models identify threat agent categories used in other domains that share some characteristics with the electric sector cyber security domain. Those domains are: (1) missions for specific individual public and private sector organizations that provide critical infrastructure in Minnesota, (2) the energy infrastructure in Europe and (3) safety in general, specifically where the cause of failure is due to human error. The topic of human error was not included in the first two reference threat models. TWG1 members believed that human error should be incorporated in the threat model for the electric sector cyber security domain.

D.2 Electric Sector Cyber Security Threat Model

Table 6 below shows the TWG1 electric sector cyber security domain threat model that was developed using the reference threat models and tailored to the electric sector based on feedback from TWG1 participants. In particular, the electric sector cyber security domain threat model incorporates the following elements:

- Adversaries with intent, driven by money, politics, religion, activist causes, recreation, recognition or simply malevolence
- Adversary activity may include spying or have direct impact on operations
- Insiders or outsiders, groups or individuals
- Failure in people, processes, and technology, including human error
- Loss of resources, in particular key employees or communications infrastructure
- Accidents
- Nature as it impacts cyber security.

Intentional adversaries are grouped to separate them by motive and modus operandi.

Table 9
Electric Sector Cyber Security Domain Threat Model

Threat Agent	Subcategory	Example Members
Economic Criminals		
	Transnational or national criminal Organization	Former Soviet Union Mafia, extortion groups[6]
	Insiders (financial, espionage)	Employees, contractors
	Customers	Residential, commercial, schools
	External individual	
Malicious Criminals		Disgruntled employees or contractors, deranged persons, cyber gangs
Recreational Criminals		Hackers
Activist Groups		
	Eco and cause driven	Earth First, Green Peace
	US national separatists	US militias and hate groups (known to steal power)
Terrorists		
	Religious radical extremists	Al Qaeda, Taliban, ISIS
	Lone extremists	Anti-society individual
	Strategic political	Nation State: China, North Korea, Cuba
	Tactical political	Lashkar-e-Taiba[7], Hammas
Hazards		
	Natural hazards	Tornados, pandemics, floods, earthquakes

[6] http://www.safetyissues.com/site/cyber_crime/cia_reveals_hacker_attacks_on_utilities.html?print

[7] http://en.wikipedia.org/wiki/Lashkar-e-Taiba

Threat Agent	Subcategory	Example Members
	Human errors and other accidents	- Poor human-system design - Configuration or data entry errors - Inadequate or non-existent policies, processes, procedures, and/or training - Non-compliance (not following policies and procedures) - Inadequate auditing, maintenance and testing - Poor plant system design - Aging systems
	Other hazards to required resources	- Employees that monitor cyber security are absent due to terror threat - Loss of processing/communication facilities due to nearby physical attack

Economic criminals are driven by money and malicious criminals are driven by emotion and the desire to harm. Recreational criminals are driven by the desire for fun or self-promotion.

“Other hazards to required resources” refers to loss or degradation of resources required to maintain cyber security, for reasons not otherwise covered in the threat model.

Appendix E Bibliography

[1] "Electric Sector Failure Scenarios and Impact Analyses," NESCOR, http://smartgrid.epri.com/doc/Electric+Sector+Representative+Failure+Scenarios+by+Domain_011312a.pdf

[2] “Cyber Security for DER Systems,” Version 1.0 July 2013 http://www.smartgrid.epri.com/doc/der%20rpt%2007-30-13.pdf

[3] “NESCOR Guide to Penetration Testing for Electric Utilities,” Version 3.0 http://www.smartgrid.epri.com/doc/NESCORGuidetoPenetrationTestingforElectricUtilities-v3-Final.pdf

[4] “Wide Area Monitoring, Protection, and Control Systems (WAMPAC), Standards for Cyber Security Requirements,” Oct 26, 2012 http://www.smartgrid.epri.com/doc/ESRFSD.pdf