NESCOR Cybersecurity Failure Scenarios

Advanced Metering Infrastructure (AMI)

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.

Relevant Vulnerabilities:

- *System relies on credentials that are easy to obtain for access* (via social engineering) in the AMI system,
- *Workforce may be unaware of recommended precautions* to prevent social engineering attacks,
- *System relies on credentials that are easy to obtain for access* to a meter disconnect command (single-factor authentication),
- *Network interconnections provide users and hardware/software entities with access unnecessary for their roles* from remote networks to network containing the AMI system.

Impact:

- Customers experience power outages,
- Utility may need to roll a truck to identify the problem,
- Utility loses revenue (scales based on number of meters affected),
- Threat agent may use power outage to mask criminal activity at customer sites.

AMI.32 Power Stolen by Reconfiguring Meter via Optical Port

Description: Many smart meters provide the capability of re-calibrating the settings via an optical port, which is then 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.

Relevant Vulnerabilities:

- *Insiders with high potential for criminal or malicious behavior have access to critical functions or sensitive data*, in particular, procedures and equipment for modifying meter configurations,
- *System relies on credentials that are easy to obtain for access* to the meter optical port, which in many cases allows reconfiguration of the meter settings (the optical port password may be found unencrypted on the meter or in field equipment that accesses the meter),
- *System permits unauthorized changes* to the configuration that determines how power consumption is recorded,

- *System relies on credentials that are easy to obtain for access* (via password) to field tool or third party installations of software that can reconfigure meters.

Impact:

- The utility experiences a loss of revenue due to under billing.

Distributed Energy Resources (DER)

DER.7 Incorrect Clock Causes Substation DER System Shut Down During Critical Peak

Description: A utility-owned DER system is located in a substation with the primary purpose of providing additional power during a critical peak. A threat agent changes the time clock in the DER system through a false time-synchronization message, so that either the DER system believes that the critical peak event is over or that all time-stamped messages to it are invalid, so it goes into default shut-down mode.

Relevant Vulnerabilities:

- *System permits messages to be modified by unauthorized individuals* in the time synchronization communication protocol,
- *Message modified by an adversary is either difficult or infeasible to distinguish from a valid message* in the time synchronization communication protocol,
- *System takes action before confirming changes with user* in the DER management system.

Impacts:

- The DER system performs an immediate shut down and causes damage to a transformer,
- Customer outages occur during the critical peak,
- Utilities need to curtail customer generation and/or loads until a new transformer is installed.

DER.16 DER SCADA System Issues Invalid Commands

Description: A threat agent breaches a DER SCADA system and causes the DER SCADA system to issue an invalid command to all DER systems. Since DER systems may react differently to invalid commands, the power system experiences immediate and rapid fluctuations as some DER systems shut down, while others go into default mode with no volt-var support, still others revert to full output, and a few become islanded microgrids. The distribution equipment tries to compensate automatically, but causes more problems as the voltage experiences severe surges and sags.

Relevant Vulnerabilities:

- *System permits potentially harmful command sequences,* in particular issuance of commands with unknown impact on the DER systems,
- *System permits unauthorized changes* to SCADA application data or software that allows the DER SCADA system to send invalid commands to DER systems,
- *System relies on credentials that are easy to obtain for access* to the SCADA DER system.

Impacts:

- Power system rapid fluctuations that cause power quality problems for customers, including outages,
- Equipment damage (that can lead to loss of life) due to power system surges and sags,
- Transmission power quality problem.

DER.20 Compromised DERMS Weather Data Modifies DER Output Forecasts

Description: A threat agent accesses the DERMS system and modifies the weather data being used to forecast loads and DER generation/storage. Consequently, less than optimal requests are sent to DER systems, causing financial impacts to the utility.

Relevant Vulnerabilities:

- *System relies on credentials that are easy to obtain for access* to the DERMS system,
- *System permits messages to be modified by unauthorized individuals* for the DERMS data access from remote locations,
- *Message modified by an adversary is either difficult or infeasible to distinguish from a valid message* for the DERMS data access from remote locations,
- *Users lack visibility that unauthorized changes were made* to DERMS data.

Impact:

- Inefficient or cost-ineffective power system operated by the utility,
- Financial impact to the utility,
- Utility legal costs related to DER owner litigation for unfair practices.

Wide Area Monitoring, Protection, and Control (WAMPAC)

WAMPAC.6 Compromised Communications between PMUs and Control Center

Description: WAMPAC communications are slowed down or stopped by manipulating the communications link between the PMUs and the control center. This might be done by attacking network components such as routers, or gaining access to the network and employing a flooding attack.

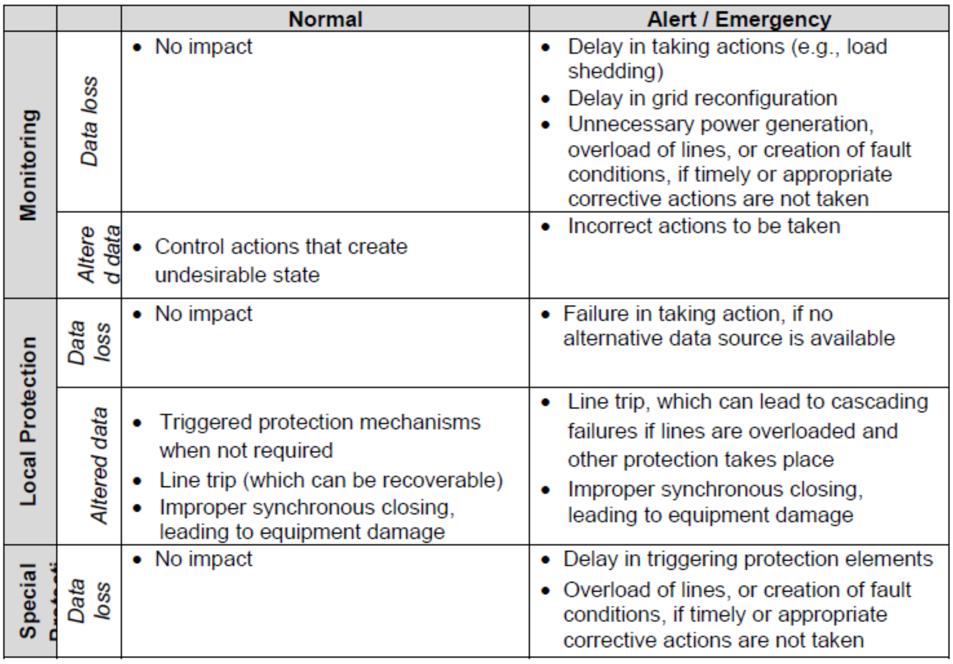
Relevant Vulnerabilities:

- *Unnecessary network access is permitted* to network components,
- *Users lack visibility of threat activity*, specifically unexpected access to network components or unusual traffic on the network,
- *System relies on credentials that are easy to obtain for access* to the WAMPAC network.

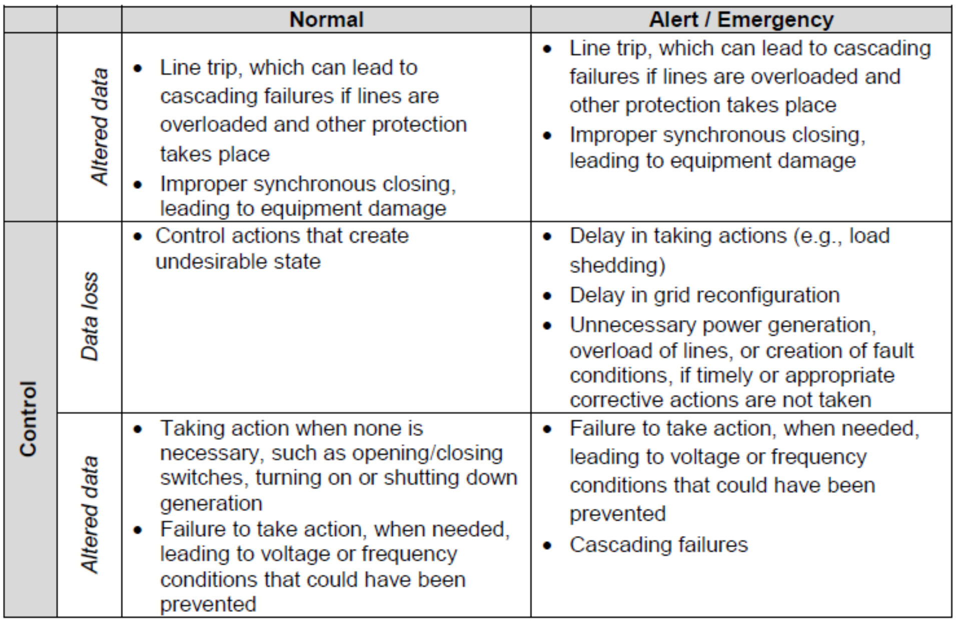
Impact:

- All impacts presented in Table 7, as potentially caused by loss of measurements.

Table 7 - Impact Examples by System State and Type of WAMPAC Application



		Normal	Alert / Emergency
Monitoring	*Data loss*	• No impact	• Delay in taking actions (e.g., load shedding) • Delay in grid reconfiguration • Unnecessary power generation, overload of lines, or creation of fault conditions, if timely or appropriate corrective actions are not taken
	Altered data	• Control actions that create undesirable state	• Incorrect actions to be taken
Local Protection	*Data loss*	• No impact	• Failure in taking action, if no alternative data source is available
	Altered data	• Triggered protection mechanisms when not required • Line trip (which can be recoverable) • Improper synchronous closing, leading to equipment damage	• Line trip, which can lead to cascading failures if lines are overloaded and other protection takes place • Improper synchronous closing, leading to equipment damage
Special Protecti	*Data loss*	• No impact	• Delay in triggering protection elements • Overload of lines, or creation of fault conditions, if timely or appropriate corrective actions are not taken



		Normal	Alert / Emergency
	Altered data	• Line trip, which can lead to cascading failures if lines are overloaded and other protection takes place • Improper synchronous closing, leading to equipment damage	• Line trip, which can lead to cascading failures if lines are overloaded and other protection takes place • Improper synchronous closing, leading to equipment damage
Control	*Data loss*	• Control actions that create undesirable state	• Delay in taking actions (e.g., load shedding) • Delay in grid reconfiguration • Unnecessary power generation, overload of lines, or creation of fault conditions, if timely or appropriate corrective actions are not taken
	Altered data	• Taking action when none is necessary, such as opening/closing switches, turning on or shutting down generation • Failure to take action, when needed, leading to voltage or frequency conditions that could have been prevented	• Failure to take action, when needed, leading to voltage or frequency conditions that could have been prevented • Cascading failures

Electric Transportation (ET)

ET.16 An EV is Exploited to Threaten Transformer or Substation

Description: A threat agent exploits an in-vehicle system at an EV to inject malware to an EVSE in a charging station. In the near future, such systems will be connected both to the battery via a vehicle data bus (e.g., CAN bus) and to the EVSE via wireless channels (e.g., ZigBee). Once compromised, an EVSE may infect other EVSEs, creating a botnet. The compromised EVSEs could simultaneously charge or discharge all the plugged EVs, thus overloading the distribution transformer. Alternatively, they may launch an attack directly to a charging station management system or to a distribution operator system that controls the transformer and the substation.

Relevant Vulnerabilities:

- *System permits installation of malware* in the EVSE during charging between the EV and the EVSE (ET.3),
- *System permits installation of malware* due to the malware spreading between EVSEs on the network hosting the EVSEs for the charging station,
- *System permits unauthorized changes* to the in-vehicle system,
- *System permits installation of malware* in public charging station systems,
- *Shared credentials are used for access* to nearby EVSEs,
- *Design, implementation, or maintenance permits system to enter a hazardous state* by allowing overloading of the distribution transformer.

Impact:

- Potential to overpower and damage transformer in a neighborhood,
- Temporarily loss of capability for charging station to service customers,
- Potential damage to electric vehicles,
- Revenue loss of the owner of the charging stations due to their damage,
- Violation of customer contracts and loss of customer confidence.

Demand Response (DR)

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.

Relevant Vulnerabilities:

- *Physical access may be obtained by unauthorized individuals* to communications channel components,
- *Unnecessary access is permitted to the communications channel,*
- *Publicly accessible and/or third party controlled links used* in DRAS/customer communication channels,
- *System relies on communications that are easy to jam* in wireless DRAS/customer communications channels,
- *System permits unauthorized changes* to the messaging interface components of the DRAS,
- *System permits unauthorized changes* to the messaging components of the customer systems,
- *Users lack visibility of threat activity* specifically unusual traffic load on the communications channel from the DRAS to customer systems or interactions with channel components not originated by the DRAS.

Impact:

- The effects would be correlated to the extent of blockage:
  - If the blockage is local, the impact may be limited to increased energy charges to consumers,
  - Blockage of DR messages on a larger scale, particularly messages to large industrial customers, may cause outages at a local or regional level if demand is too great and increased energy costs to customers over a larger area,
- In sell-back or brokerage scenarios, the blockage of DR signals may result in increased prices for electricity for the utility company and be instrumented for considerable financial gain for parties selling electricity back to the utility company.

DR.4 Improper DRAS Configuration Causes Inappropriate DR Messages

Description: A threat agent 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.

Relevant Vulnerabilities:

- *System permits unauthorized changes* to DRAS configuration,
- *Users lack visibility that unauthorized changes were made* in the DRAS configuration,
- *Unnecessary network access is permitted* to the network on which the DRAS resides,
- *System relies on credentials that are easy to obtain for access* to the DRAS configuration.

Impact:

- A false message may deliver information indicating lower prices to consumers, which encourages them to increase power consumption during on-peak periods,
- Damage to the smart grid infrastructure with possible service impacts from small to large scale,
- Potential power loss,
- The utility may have financial impacts,
- In sell-back or brokerage scenarios, withholding of DR signals at the source DRAS may result in increased prices for electricity to the utility and be instrumented for considerable financial gain for parties selling electricity back to the utility company,
- Loss of public confidence in utility and DR program,
    - The customer, receiving an unintended DR message, may reduce power consumption without seeing any benefit applied in their bill.

Distribution Grid Management (DGM)

DGM.6 Spoofed Substation Field Devices Influence Automated Responses

Description: Threat agent spoofs data inputs from field devices at substations and below to cause the DMS to report a false system state. This could cause operator or automated responses that are inappropriate.

Relevant Vulnerabilities:

- *System permits messages to be modified by unauthorized individuals* in the communications between field devices and the DMS,
- *Message modified by an adversary is either difficult or infeasible to distinguish from a valid message* in the communications between field devices and the DMS,
- *System makes messages accessible to unauthorized individuals.*

Impact:

- Inappropriate fault-clearing actions, feeder sectionalization, and overuse of remedial capabilities leading to loss of power to customers,
- Volt/VAR controls are wrongly applied or adjusted based on erroneous data, possibly triggering over/under voltage trips,
- Collected meter data is incorrect or inaccurate, leading to possible loss in revenue.

NESCOR Cybersecurity Failure Scenarios Evaluation Sheet

Group Name:

Scenario	AMI.9 Invalid Disconnect Messages to Meters Impact Customers and Utility				
Impact	0	1	3	7	9
Adversary Cost	0.1	1	3	7	9

Scenario	AMI.32 Power Stolen by Reconfiguring Meter via Optical Port				
Impact	0	1	3	7	9
Adversary Cost	0.1	1	3	7	9

Scenario	DER.7 Incorrect Clock Causes Substation DER System Shut Down During Critical Peak				
Impact	0	1	3	7	9
Adversary Cost	0.1	1	3	7	9

Scenario	DER.16 DER SCADA System Issues Invalid Commands				
Impact	0	1	3	7	9
Adversary Cost	0.1	1	3	7	9

Scenario	DER.20 Compromised DERMS Weather Data Modifies DER Output Forecasts				
Impact	0	1	3	7	9
Adversary Cost	0.1	1	3	7	9

Scenario	WAMPAC.6 Compromised Communications between PMUs and Control Center				
Impact	0	1	3	7	9
Adversary Cost	0.1	1	3	7	9

Scenario	ET.16 An EV is Exploited to Threaten Transformer or Substation				
Impact	0	1	3	7	9
Adversary Cost	0.1	1	3	7	9

Scenario	DR.1 Blocked DR Messages Result in Increased Prices or Outages				
Impact	0	1	3	7	9
Adversary Cost	0.1	1	3	7	9

Scenario	DR.4 Improper DRAS Configuration Causes Inappropriate DR Messages				
Impact	0	1	3	7	9
Adversary Cost	0.1	1	3	7	9

Scenario	DGM.6 Spoofed Substation Field Devices Influence Automated Responses				
Impact	0	1	3	7	9
Adversary Cost	0.1	1	3	7	9