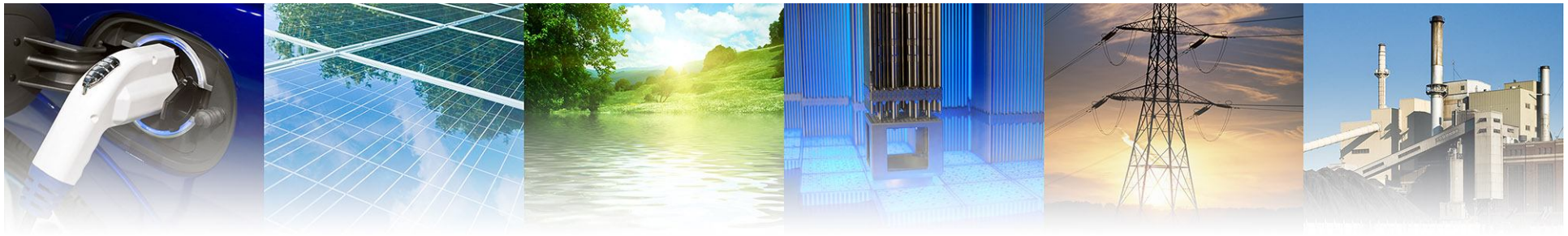


EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Failure Scenarios for the Electric Sector

Annabelle Lee

Senior Technical Executive

SmartSec 2014

January 2014

National Electric Sector Cybersecurity Organization Resource (NESCOR)

Build an industry collaboration

- Public/private partnership funded by DOE
- Utilities, vendors, academia, consultants, regulators

Address critical industry needs

- Failure scenarios and impact analyses

Multi-year effort

- Identify key research topics and develop products

Collaboration across all participants

Failure Scenarios for the Electric Sector

http://www.smartgrid.epri.com/NESCOR.aspx

Describing Failure Scenarios

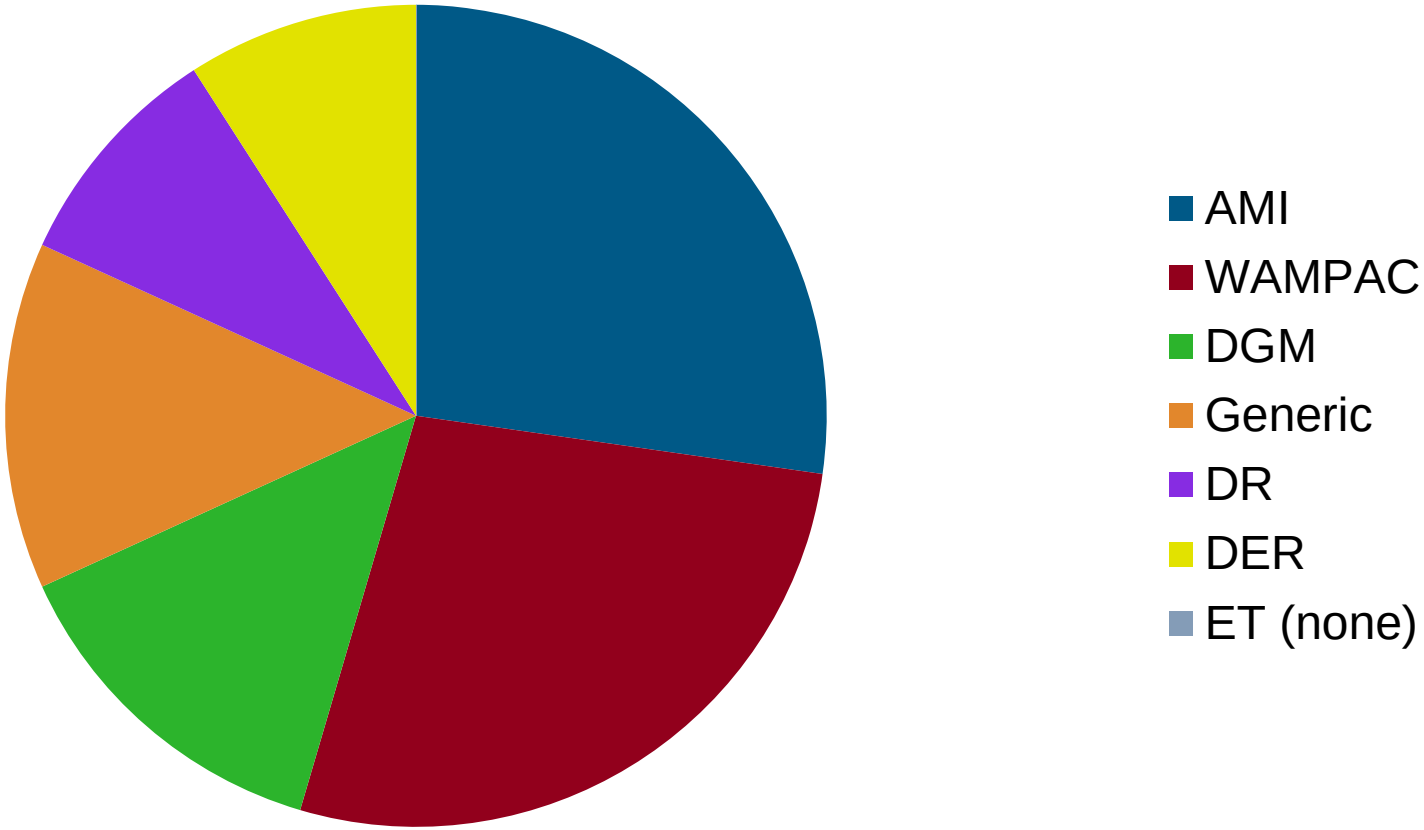
Example of a Failure Scenario

Malicious Code Injected into Substation Equipment via Physical Access

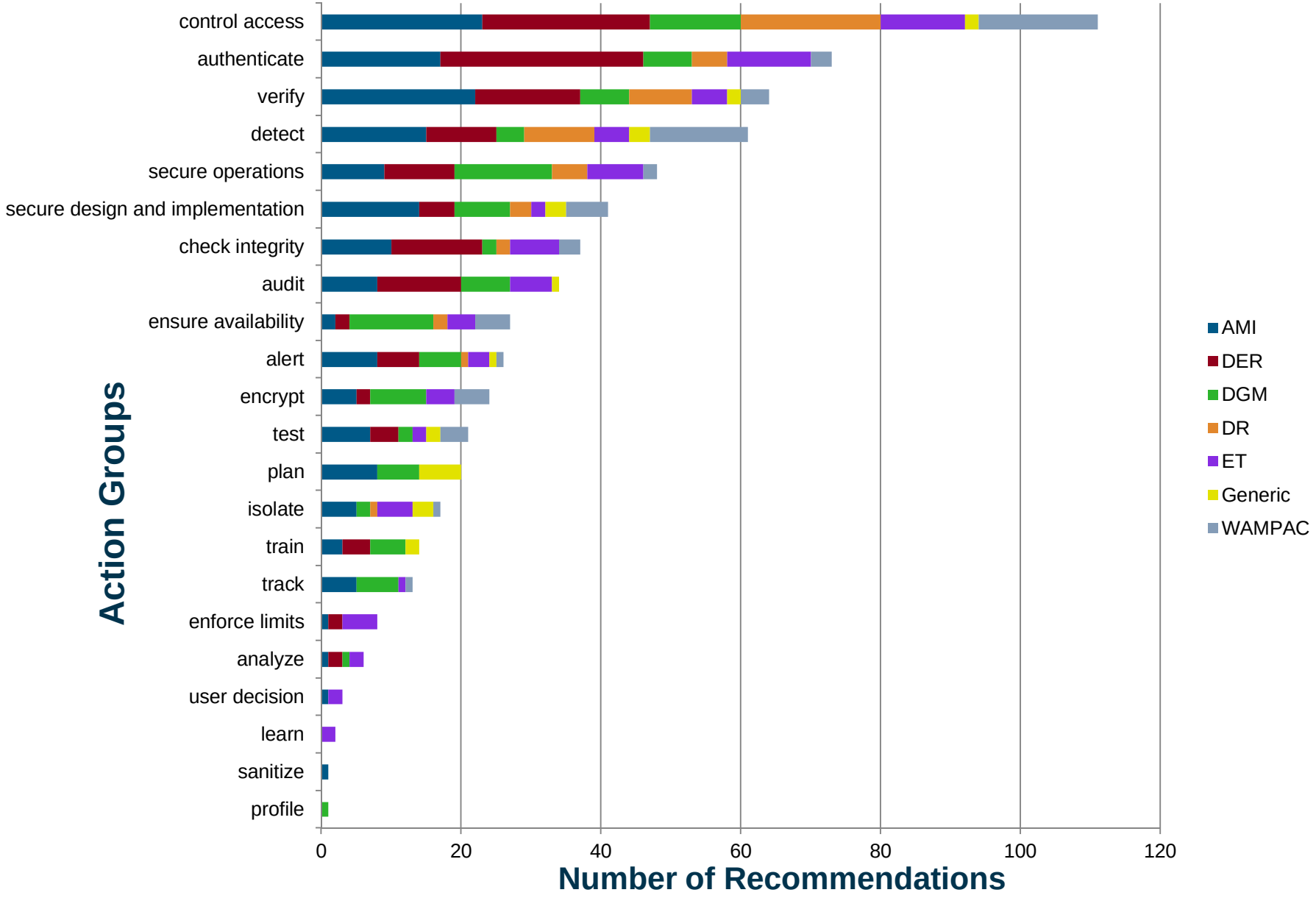
Description	**What is the incident?**
Relevant Vulnerabilities	**How does the incident occur?**
Impact on Power System	**How does it affect survivability/ reliability/resiliency?**
Potential Mitigations	**How do we reduce the risk?**

Failure Scenario Prioritization Results

Distribution Across Domains - Top 20% of Failure Scenarios



Common Mitigation Analysis Results



Common Mitigation Analysis Results (2)

- Converted 445 bulleted mitigations to the new form
- Some conversions created multiple Common Actions
- Identified *171 Common Actions*
  - 110 will require automated means to implement and the rest can be implemented manually
- Automated and manual Common Actions were recommended evenly across all scenarios
- Defined 22 Action Groups (illustrated above)

Impact on Industry

- Utilities
  - Leveraged failure scenarios for utility risk assessment
  - Members anticipate value in common mitigations
    - Communicate cyber security priorities to utility upper management

- Related industry efforts
  - Brazil InMetro organization used failure scenario template
    - Developed own failure scenarios
  - Failure scenarios document was reference in DOE ES-C2M2 effort
  - Failure scenarios basis for EPRI funded project with the University of Illinois

AMI Failure Scenario Example

- **AMI.1 Authorized Employee Issues Unauthorized Mass Remote Disconnect**
  - **Description:** An employee within the utility having valid authorization, issues a “remote disconnect” command to a large number of meters. The employee may be bribed, disgruntled, or socially engineered.
  - **Relevant Vulnerability**
    - Inadequate system and process checks for disconnect commands.

AMI Failure Scenario Example (2)

- Common mitigations
  - Detect anomalous commands
  - Use RBAC
  - Generate alarms
  - Create audit log
  - Require 2-person rule
  - Validate data
- Expanded for specific scenario
  - *Validate data* to ensure reasonableness of changes
  - *Generate alarms* for changes to sensitive data

Incident Rating Categories

Category	
High	Requires immediate attention, recommendation to not proceed without mitigation
Moderate	Requires attention, recommendation to proceed with caution (Limit Exposure) or further mitigate
Low	Requires consideration and prioritization
Negligible	No mitigation required

Impact Criteria - Examples

Criterion	How to score
System scale	0: single utility customer, 1: neighborhood, town, 3: all ET, DER or DR customers for a utility, 9: potentially full utility service area and beyond
Public safety concern	0: none, 1:10-20 injuries possible, 3: 100 injured possible, 9: one death possible
Financial impact of compromise on utility	0: Petty cash or less, 1: up to 2% of utility revenue, 3: up to 5%, 9: Greater than 5%

Likelihood and Opportunity - Examples

Criterion	How to score
Skill required	0: Basic domain understanding and computer skills, 1: Special insider knowledge needed, 3: Domain knowledge and cyber attack techniques, 9: Deep domain/insider knowledge and ability to build custom
Common vulnerability among others	0: Nearly all utilities, 1: Half or more of power infrastructure, 3: More than one utility, 9: Isolated occurrence
Accessibility (logical, assume have physical access)	0: common knowledge or none needed, 1: publicly accessible but not common knowledge, 3: not readily accessible, 9: high expertise to gain access

Discussion

alee@epri.com

Together…Shaping the Future of Electricity