Annabelle Lee

Electric Power Research Institute (EPRI)

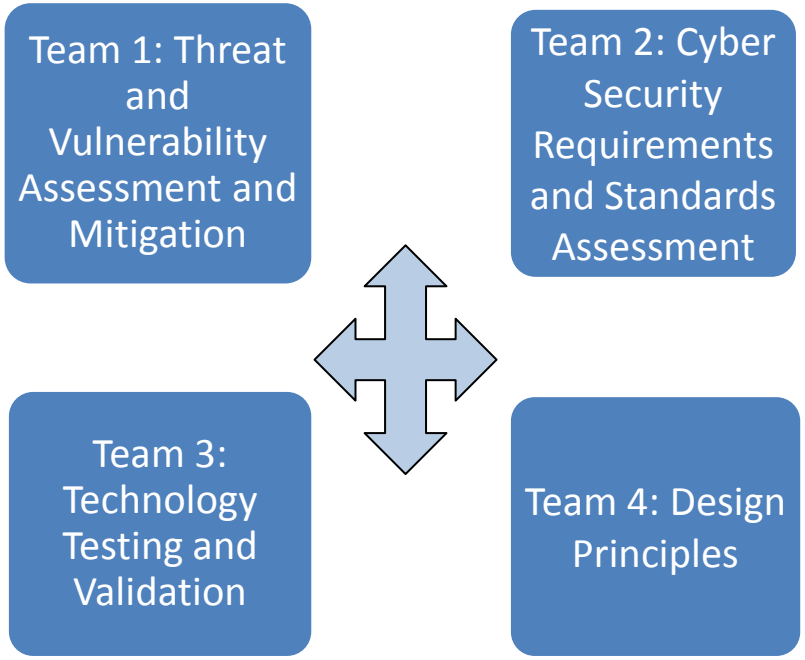
National Electric Sector Cybersecurity Organization Resource (NESCOR)

Cybersecurity for Energy Delivery Systems Peer Review

August 5-6, 2014

Summary: NESCOR

- **Objective**
  - Provide technical assessments of power system and cyber security standards to meet power system security requirements; develop specific guidance related to threats and vulnerabilities; develop test guides for performing security assessments and penetration testing.
- **Schedule**
  - 10/2010 – 06/2014
  - All deliverables completed
  - Goal: guidance and tools for assessing cyber security threats and vulnerabilities and for performing security assessments



- **Total Value of Award:** $6,779,287
- **% Funds expended to date:** 98%
- **Performer:** EPRI
- **Partners:** research organizations, universities, private sector companies, DOE labs

Advancing the State of the Art (SOA)

- **Utilities did not have available guidance and tools for specific cyber security areas**
- **The approach was to have research organizations, academia, DOE labs, vendors, and private sector collaborate in addressing cyber security for the electric sector**
  - The different perspectives provided valuable input
- **The focus was on research areas that were not being addressed**

Advancing the State of the Art (SOA) (2)

- **The products and tools may be used by utilities for:**
  - Risk assessment,
  - Planning,
  - Procurement,
  - Training,
  - Tabletop exercises, and
  - Security testing
- **The goal is to provide utilities with information and techniques to address cyber security**

Challenges to Success

- **Challenge 1: Identifying the most critical cyber security challenges for the electric sector**

  Response: Each of the technical working groups prioritized specific areas of research

- **Challenge 2: Providing technical guidance in new research areas**

  Response: Based on the prioritized research areas identified above, each team focused on useful guidance

- **Challenge: Ensuring that the products would be useful to utilities**

  Response: Electric utilities participated in all the working groups

Progress to Date

- **Major Accomplishments**
  - Completed and posted several documents on: smartgrid.epri.com/nescor.aspx
    - Electric Sector Failure Scenarios and Impact Analyses, v2.0
    - Analysis of Selected Electric Sector High Risk Failure Scenarios
    - Attack Trees for Selected Electric Sector High Risk Failure Scenarios
    - Cyber Security for DER Systems
    - WAMPAC – Standards for Cyber Security Requirements
    - Guide to Penetration Testing for Electric Utilities
    - Smart Energy Profile (SEP) 1.x Summary and Analysis

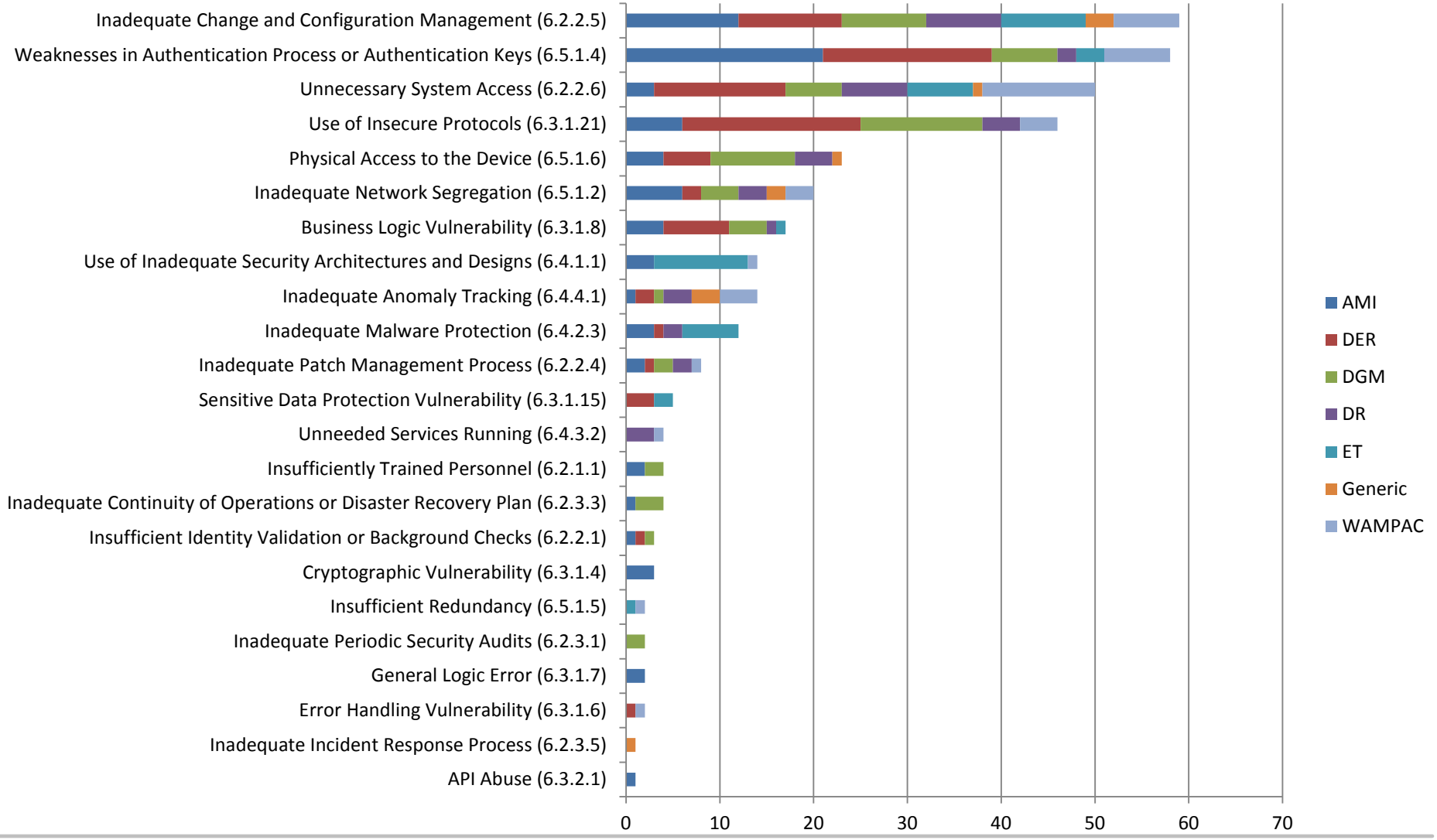
Collaboration/Technology Transfer

- **Plans to transfer technology/knowledge to end user**
  - The targeted end user is primarily the electric utilities
    - The other recipients are vendors, research organizations, and federal agencies
  - What are your plans to gain industry acceptance?
    - All of the deliverables have been vetted by utilities and utilities participated in the development of the various deliverables

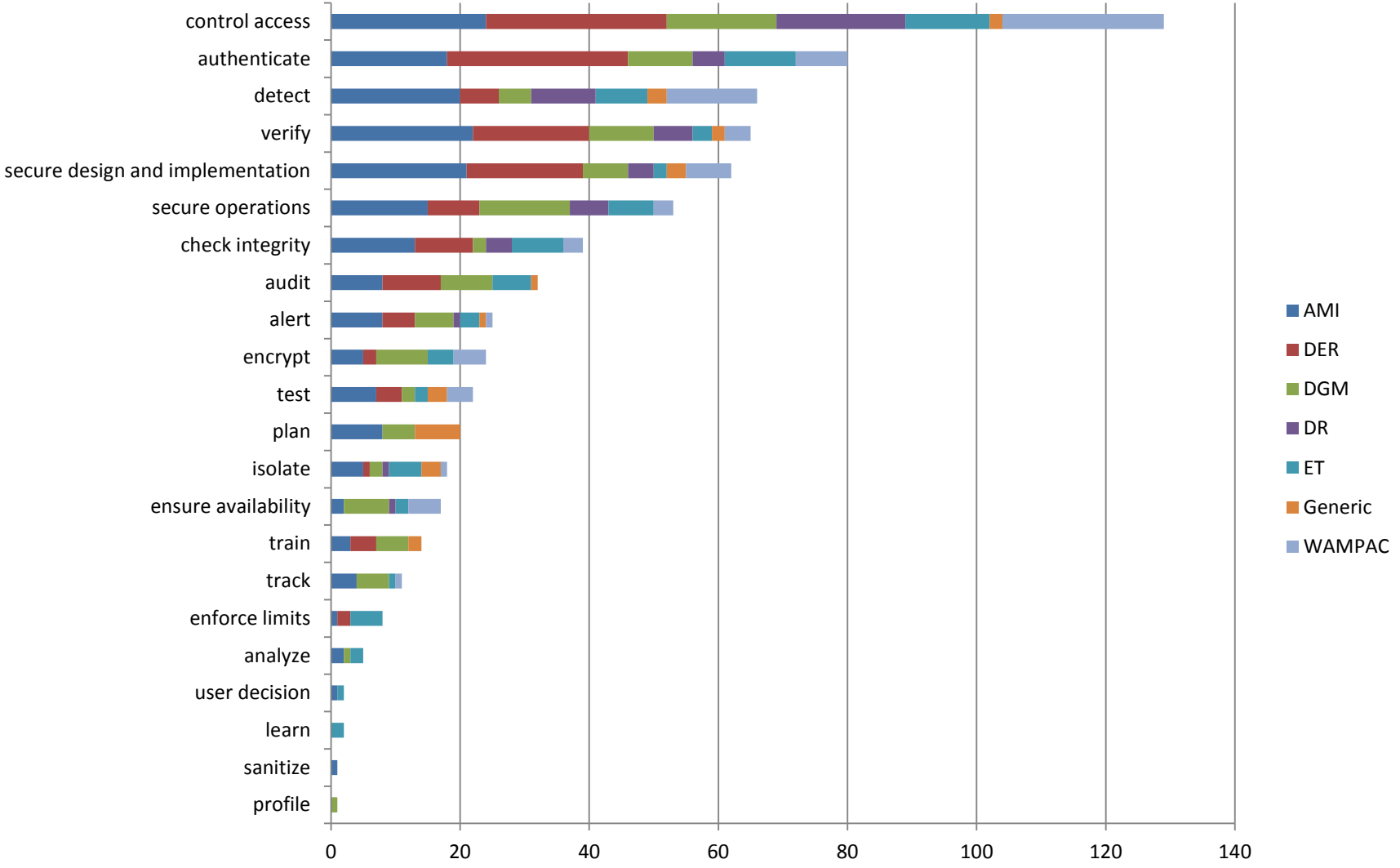
Next Steps for this Project

- **Approach for the next year or to the end of project**
  - Although the project is complete, the failure scenarios continue to be used and referenced internationally
  - The failure scenarios are included in ongoing EPRI projects and other research projects, such as TCIPG
  - EPRI has established a share-point site to continue the collaboration with the team NESCOR team members

Observed Frequency of Vulnerability Classes



Observed Frequency of Mitigation Action Groups



Failure Scenarios Risk Ranking Graph