SAND2009-7469C

Prioritizing Cyber-Vulnerable Critical Infrastructure Equipment and Mitigation Strategies

Jason Stamp
Energy Systems Analysis
Sandia National Laboratories
Albuquerque, New Mexico

CUEPRA Fall Meeting

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

National Nuclear Security Administration

Sandia National Laboratories

Agenda

- Project description and objectives
- Industry participation and sector benefit
- Relevance to Roadmaps
- Program approach
- Methodology approach
- Timeline and current status
- Applying the Approach – Electric Power

Critical Spares Project

- What is it? A Department of Homeland Security (DHS) study to identify and prioritize essential physical components that are "cyber-connected" and develop risk mitigation strategies
  - Also known as the "Critical Spares Project"

- Purpose: To develop and validate an all hazards methodology for measuring the level of risk to these components and determining the appropriate response

- Targeted Sectors: All sectors (with initial sectors being Electric Power and Water Distribution Systems)

Project Objective

- Identify sector-specific threats and resulting impacts
- Evaluate the consequence to sectors resulting from the failure or loss of the components
- Examine risk and cost-benefit trade-offs
- Assess the benefits of potential mitigation strategies
  - Strategic spares stockpile for components with long-lead times
  - Possible manual operations
  - Possible degraded operations
  - Development or refinement of contingency plans to include cyber

Industry Participation & Benefits

- Why Participate?
  - Gain a better understanding of the cost-benefit tradeoffs to inform response and recovery planning for cyber incidents
  - More effective use of limited resources when implementing mitigation strategies
  - Connect with national cyber security experts who can provide guidance on risk reduction activities
- What's involved?
  - Review project assumptions and approach to ensure project results are relevant and useful for industry
  - Share personal experience in defining current response and recovery plans to achieve credible results (valid input to get valid output)

Spares Project Objectives Aligned with Critical Sector Priorities

- Energy and Water Control System Roadmaps:
  - Priority: develop risk assessment tools that include vulnerability assessment methodologies, *frameworks for prioritizing control measures*, and cost justification tools

- Water Sector Annual Report 2008
  - Medium-priority gap: *identify high-consequence assets* and provide a structured approach for prioritizing protection programs based on this list of assets.

Project Approach

- Develop a general methodology for use by ALL sectors
  - System definition
  - Component filtering by consequence and threat
  - Mitigation strategies and cost-benefit tradeoff
- Conduct a pilot study to improve the methodology
  - Engage multiple utilities per sector
  - Use lessons learned to enhance the methodology
- Build on the success of pilot study and exercise the methodology from a broader stakeholder pool (state or regional focus)

Timeline and Current Status

- Industry involvement and outreach phase (Aug '09-Feb '10)
  - Water-ISAC, EPA and AWWA Meeting/24 Sept
  - EnergySec Utility Portal announcement/14 Oct
  - Initial discussions with SCE and SEL/15 Oct
  - ICSJWG/3-5 Nov
- System characterization phase (Sept-Nov '09)
  - Identified common electric distribution system components and configurations/14 Oct
  - Identified common electric distribution system functions/15 Oct
- Asset identification and assessment phase (Sept-Dec '09)
  - Identified assets critical to each electric distribution system function, along with each asset's location/15 Oct
- Risk and cost-benefit analysis phase (Dec '09-Feb '10)

Final report due out 2nd quarter FY10

Methodology Approach

Data Gathering Process (Characterization)

Asset Identification and Filtering (Assessment)

Mitigation Identification (Risk Analysis)

Understand utilities' mission(s), major systems and components, and interdepend-encies

- Current RA & VA and other documentation
- Interviews w/ operators & owners (SMEs)
- Other Sources & References (e.g., ISAC)

STEP 1: COMPONENTS
- identification of "cyber-connected" equipment
- complete list of systems controlled and/or monitored by SCADA/ process control system

STEP 2: CONSEQUENCES
- What is the consequence of the "cyber-connected" equipment coming off-line?

STEP 3: THREATS
- What is the vulnerability-attack vector?
- How easy is it to take the "cyber-connected" equipment off-line?
- What is the threat – how knowledge-able and sophisticated is the adversary to exploit the vulnerability?

STEP 4: MITIGATION
- Stockpiles
- Contingency plan improvements
- Vital few systems & assets requiring a Mitigation Strategy

Respond and Recover At Site

YES

Timely Mitigation at Site?

NO

Propose Viable Mitigation Strategies (include Regional/National/ Virtual Spares Stockpile)

Cost Effective and Reduce Risk?

NO

YES

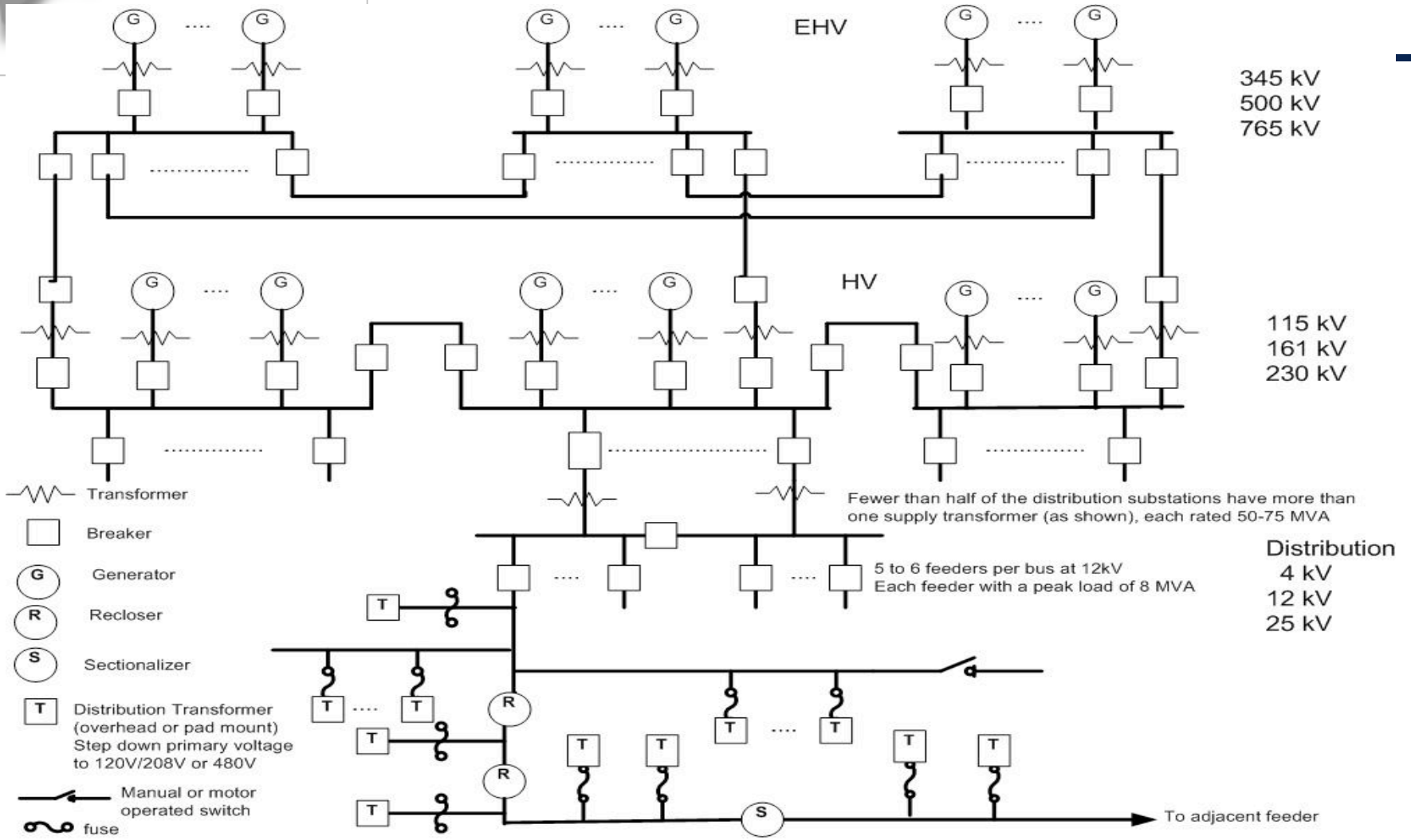
Report

Decreasing no. of assets to protect at national level

Sandia National Laboratories

Methodology Approach – Electric Power(1)

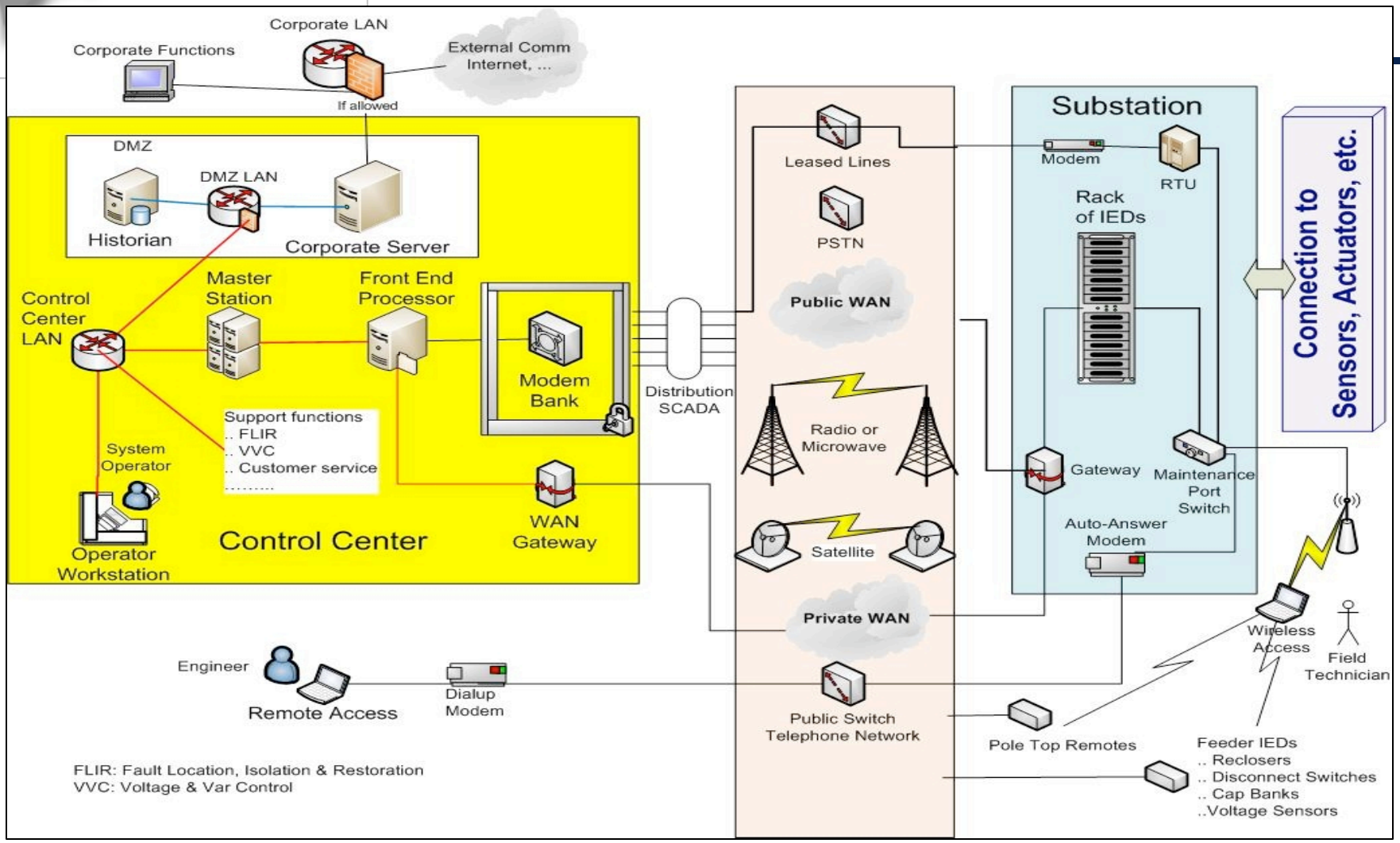
Characterization



Sandia National Laboratories

Methodology Approach – Electric Power(2)

Characterization



Sandia National Laboratories

Methodology Approach – Electric Power(3)

Component Filter

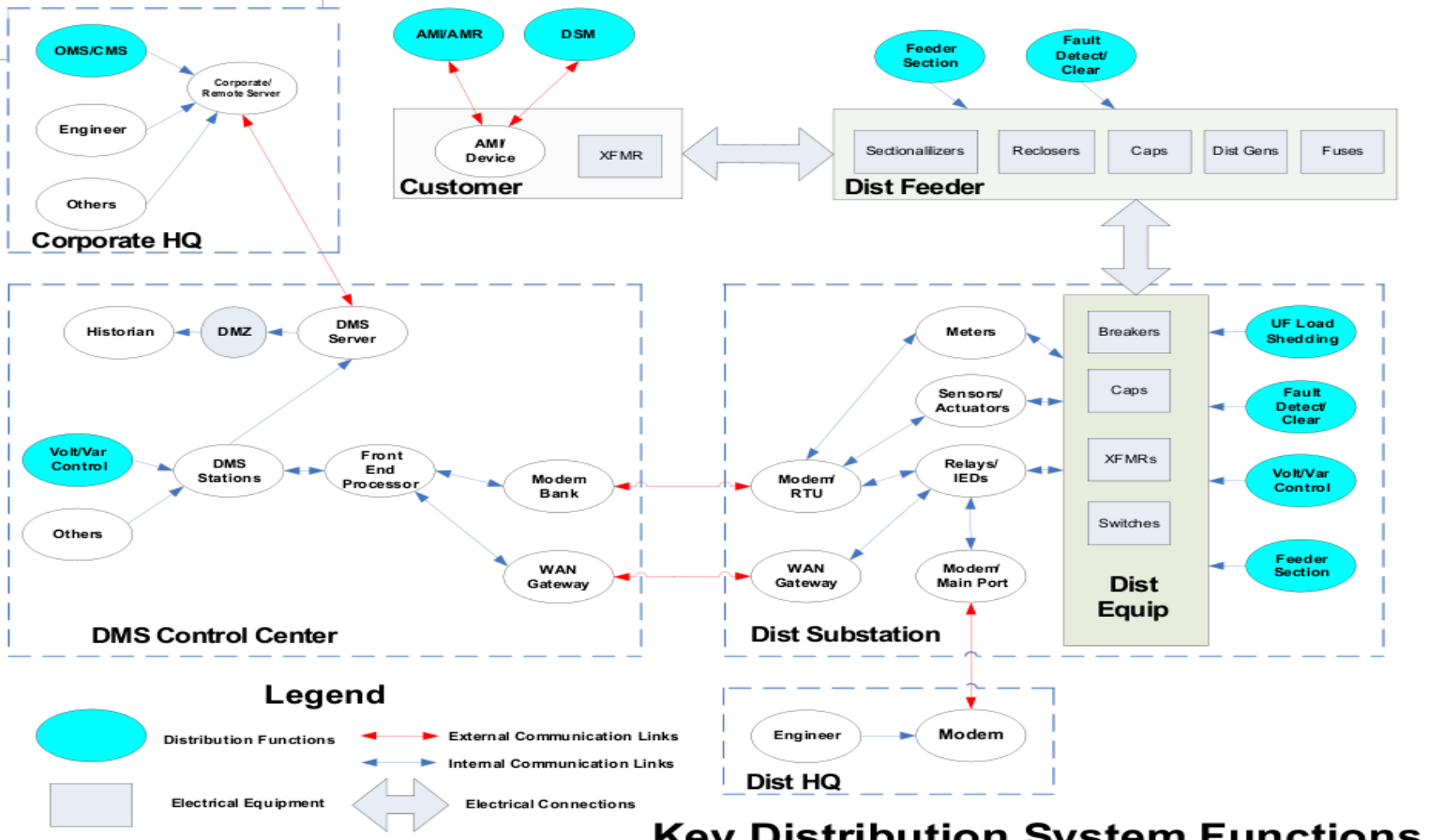
Functions

Locations	SCADA and Protection Engineering	Feeder Sectionalizing and Service Restoration	Direct Load Control	Outage and Call Management System	Under Frequency Load Shedding	AMI/AMR	Integrated Volt/Var Control	Fault Detection and Clearing	Other
Corporate EMS Control Center	Engineering Interface to SCADA		Demand Side Management					Distribution Management System	Interfaces to External Systems (billing, etc)
Corporate AMI/AMR				Outage Management		AMI Head End			
Regional DMS Control Center	Engineering Interface to SCADA, Engineering Interface to Relays	Distribution Management System					Distribution Management System		Interfaces to Transmission Systems
Regional Outage Management Call Center		Distribution Management System		Outage Management					
Substation	Engineering Interface to Relays, Transformer Relays, Line Relays, Bus Relays, Generation Relays	RTUs, Switches, Breakers			Metering, RTUs, Line Relays, Breakers		Voltage Regulation, Metering, Switches, Transformers, Breakers	Metering, Transformer Relays, Line Relays, Bus Relays, Breakers, Sectionalizers, Reclosers	Substation Service Generation
Distribution System (OH/UG)		Switches, Sectionalizers, Reclosers					Transformers	Sectionalizers, Reclosers	
Customer			Demand Side Management	Demand Side Management		Advanced Metering Infrastructure			Distributed Generation

Sandia National Laboratories

Methodology Approach – Electric Power(4)

Component Filter



Key Distribution System Functions

Sandia National Laboratories

Methodology Approach – Electric Power(5)

Consequences – Threat Filter

- **System**
  - Operations/Personnel
  - Connectivity
- **Physical/Spatial**
  - Location
  - Access
- **Functional/Logical**
  - Operations/Capabilities
  - Roles
  - Access
- **Lifecycle**
  - Interactions (who/what)
- **Temporal**
  - Operational Sequences
  - Time Requirements
    - Normal Operations
    - Attack and Restoration
- **Consequence**
  - Vulnerabilities
  - Attack Vectors

Sandia National Laboratories

Consequences of Interest

- Attacks that propagate into electrical transmission and/or generation, OR
- Attacks with long-term (cannot be mitigated within 24 hours) impacts that go beyond a single substation, OR
- Attacks that significantly impact other critical infrastructures, OR
- Attacks whose impacts are significant (>10% worse load loss per interruption) and can easily be replicated

Questions?

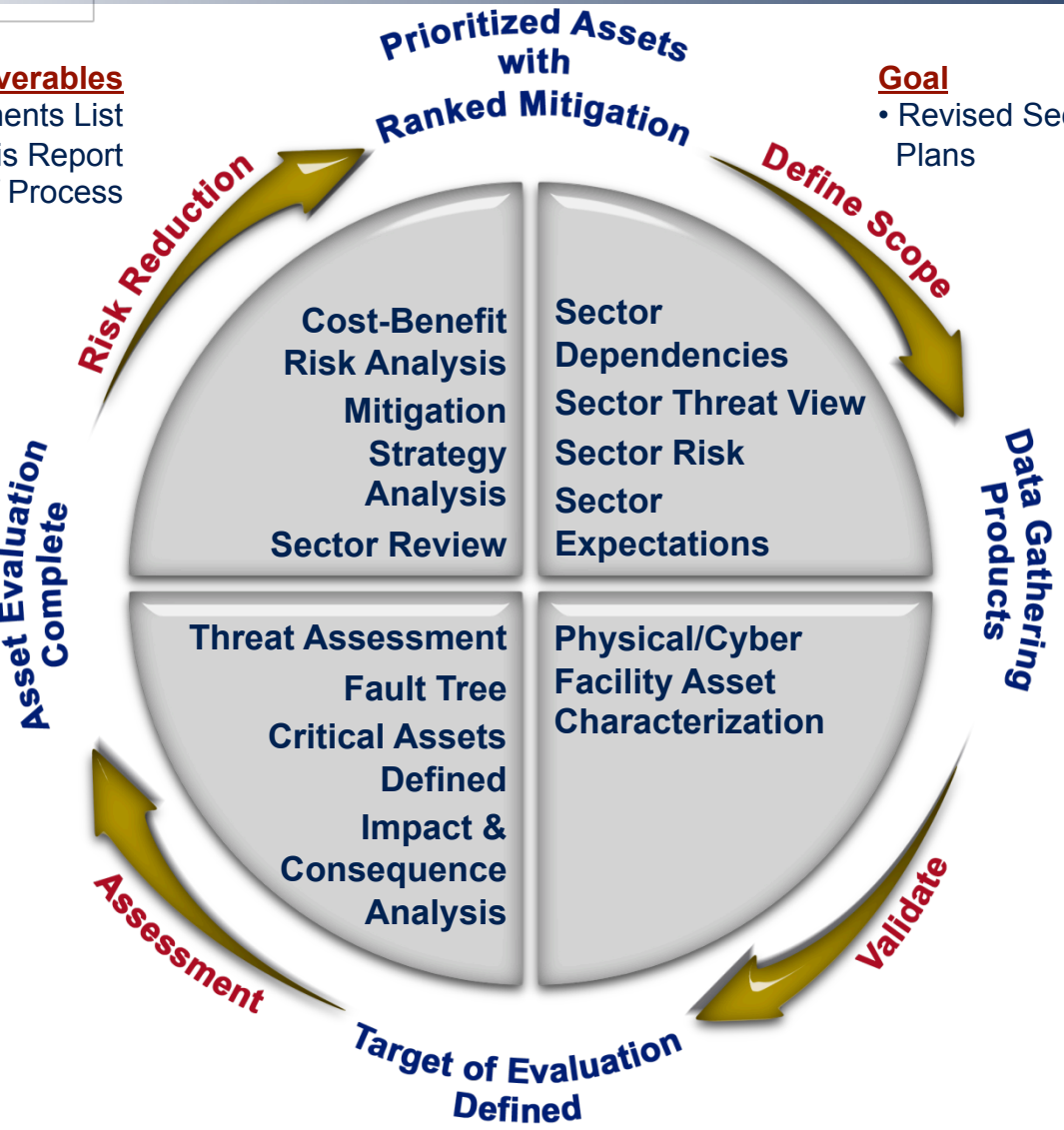
Jason Stamp
jestamp@sandia.gov

Sandia National Laboratories

Critical Asset-Mitigation Strategy Assessment Process

Product Deliverables
- Critical Components List
- Risk Reduction Analysis Report
- Description of Process

Goal
- Revised Sector Response/Recovery Plans



Sandia National Laboratories