Cybersecurity for Energy Delivery Systems

2010 Peer Review

Alexandria, VA ♦ July 20-22, 2010

James F. Stevens

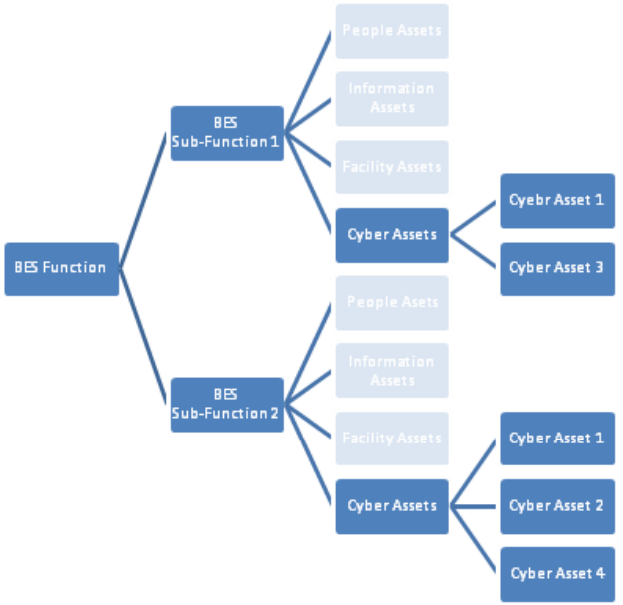
Software Engineering Institute

CERT OCTAVE BES

Summary Slide: CERT OCTAVE BES

Guidance in Identifying and Managing Electricity Sector Risk

- **Outcomes:** An operational cyber security risk assessment approach for the BES community.
- **Roadmap Challenges:** Limited ability to measure and assess cyber security posture, lack of consistent cyber security metrics, poor understanding of cyber risks, and weak business case for cyber security investments.
- **Major Successes:** Assessment methodology codified and first pilot scheduled to begin in August.



- **Schedule:** Pilot (08/10), Draft Methodology Report (09/10), Pilots 2 and 3 (10/10), Final Report and Training available (12/10).
- **Level of Effort:** $300K
- **Funds Remaining:** $234K
- **Performers:** SEI
- **Partners:** NERC CIP, AECC, and other utilities

Technical Approach and Feasibility

- **Approach**
  - Build on proven CERT® OCTAVE platform
  - Nine BES Reliability functions defined by NERC establish assessment boundary
  - Pre-defined operational risk taxonomy to ensure consistent risk coverage
  - Control catalog based on NERC CIP and DHS catalog
  - Pilot to improve and refine design and guidance

Technical Approach and Feasibility

- **Metrics for Success**
  - Minimal organizational overhead required
    - 2 days to assess one BES reliability function
  - Outcomes are consistent and repeatable
  - Actionable results
  - Guidance and training sufficient for self-application

Technical Approach and Feasibility

- **Challenges to Success**
  - Availability of industry partner staff time to participate in process development
- **Technical Achievements to Date**
  - Assessment methodology codified
  - Operational risk taxonomy defined
  - Control baseline to risk taxonomy mapping underway

Collaboration

- **Plans to gain industry input**
  - Project requires access to BES owners and operators and other subject matter experts
  - Working with ASAP-SG and NERC CIP standards development committee provides access and exposure to utilities working in this problem space

Technology Transfer

- **Plans to transfer technology/knowledge to end user**
  - BES owners and operators are the audience for this tool
  - Tool used to understand current cyber security posture and to inform cyber security risk management decisions
  - Tool does not obviate the need for an organizational continuous risk management process
  - Plan to make report detailing approach available along with online training and other support tools

Next Steps

- **Approach For the Next Year**
  - Complete piloting activities
  - Issue method guidance
  - Develop online training and other supporting tools for transition support
  - Explore results federation (within and between stakeholders)

OCTAVE BES Process

Inputs:
An up to date enterprise technical architecture showing the cyber assets that are used by the selected BES Reliability function(s).

Steps:

1. Select BES Reliability Function
2. Profile BES sub-function
3. Develop impact evaluation criteria
4. Profile cyber assets
5. Identify cyber asset failures
6. Identify risks
7. Identify controls
8. Analyze risks

Process Tools:

- The list of the BES reliability functions
- A risk taxonomy
- A control elucidation questionnaire
- NERC CIP system classification criteria
- Process worksheets
- List of standard controls
- Controls to risk mapping

Outputs:
Analysis of operational cyber security risks to BES functions

BES Reliability Functions

1. *Dynamic response.*
2. *Balancing Load and Generation*
3. *Controlling Frequency (real power)*
4. *Controlling Voltage (reactive power)*
5. *Managing Constraints*
6. *Control & Operation*
7. *Restoration of BES*
8. *Situational awareness*
9. *Inter-Entity coordination and communication*