Critical Infrastructure Protection: Risk-based Methods for Selecting Critical Assets

June 6, 2006
Burns & McDonnell

- 106 Years
- HQ in Kansas City
- CIP based in St. Louis
- Over 2000 employee-owners
- 18 offices worldwide
- Multidisciplinary engineering, architectural, construction and environmental service firm.
critical infrastructure protection

• Cyber
  - NERC Readiness
  - Secured SCADA/EMS/DCS Design

• Physical
  - Asset protection standards
  - Construction management

• Structural
  - Blast analysis
  - Structural hardening

• Operational
  - Risk Assessments
  - Enterprise Security for Utilities
  - Grid reliability analysis
  - Emergency Operations Procedures
Paradigm Shift

Security

Reliability

Security

Today’s World

Reliability = Security

- Uptime
- Continuation of service

Disconnect

- Guns, gates, guards
- Locks
- Hackers
- Hardened Facilities

Today’s World
NERC Reliability Readiness

Security Integrated with new Standards
CIP 002 Challenge

Each Balancing Authority shall operate such that, on a rolling 12-month basis, the average of the clock-minute averages of the Balancing Authority’s Area Control Error (ACE) divided by 10B (B is the clock-minute average of the Balancing Authority Area’s Frequency Bias) times the corresponding clock-minute averages of the Interconnection’s Frequency Error is less than a specific limit. This limit $\varepsilon_i$ is a constant derived from a targeted frequency bound (separately calculated for each Interconnection) that is reviewed and set as necessary by the NERC Operating Committee.

$$\text{AVG}_{\text{Period}} \left[ \frac{ACE_i}{-10B_i} \right] \ast \Delta F_i \leq \varepsilon_i \quad \text{or} \quad \text{AVG}_{\text{Period}} \left[ \frac{ACE_i}{-10B_i} \right] \ast \Delta F_i \leq 1$$

The equation for ACE is:

$$\text{ACE} = (N_{I_A} - N_{I_S}) - 10B (F_{A} - F_{S}) - I_{AE}$$

The risk-based assessment shall consider the following assets:

R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.

R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.

R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.
CIP = Reliability

R1 Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

- What is a Risk-based Assessment Methodology?
- What criteria will be used for selecting critical assets?
- NERC CIP only specifics limited hard metrics such as the case with blackstart.

Single-loss and/or N-1 is NEVER mentioned

No study, planning method, or overall approach is every referenced.

Why?

Because it is the grid that is critical not what is critical in the grid.
Step 1: Identification
Do you have handle on your assets?

How are you coordinating with other organizations?

What data is relevant and where is it?

How are you coordinating with all stakeholders?
Step 2: Assess & Catalogue
Step 3: Threats & Impacts
Identifying Electric System Critical Assets (ES-CAI) & Critical Cyber Assets (CCA) for NERC CIP Compliance

**Inputs**
- **ES-RAM Outputs**
  - a) Infrastructure
  - b) Drivers
  - c) Operations

- **ES-CAI Outputs**
  - a) Discovery
  - b) Interviews & Site Visits

**Activities**
- **Discovery**
- **Interviews & Site Visits**
- **Core Assessment**
- **Feedback**

**Outputs**
- 1. ES-RAM Annotated Library
  - 2. Baseline Review & Assessment

- 1. Interview Minutes
  - 2. Assessment Team Review Notes
  - 3. Site Visit Reports & Photos

- 1. Electric Sector Critical Asset Identification report
  - 2. Risk Analysis for Identified Critical Assets
  - 3. NERC CIP Critical Cyber Asset List

- 1. Updated Critical Asset Identification Report
  - 2. Updated Risk Analysis for Identified Critical Assets
  - 3. Updated NERC CIP Critical Cyber Assets (CCA)

---

A hands-on / directed approach
Additional Criteria

• Consider generating resources at 400MW capacity and greater.
• Any combination of resources which would create a .2hz drop in frequency across the system. (UFLS) - PRC-006-0
• Any combination of resources which exceed the total import/export capability across any one or multiple Interchanges (i.e. Control Areas).
• Sites designated as “super-critical” by DHS.
• Major Load Centers
• Critical Customers
Step 4: Rank Risk
Risk Formula

Risk = [Electric System Asset Criticality + (Threats * Vulnerabilities)]

- **Safeguards**

  - **Threats**: See Step 2 - Link to ES-ISAC / DHS color coded threat system

  - **Vulnerabilities**: See Step 5 - Perform baseline assessment

  - **Safeguards**: See Step 5 - Baseline assessment should identify existing mitigations and provide an overall scorecard
Step 5: Response
(Strategy for Compliance)
Transition from CIP 002 to 003

- Critical Asset list used as a supporting document in a policy-base for NERC CIP Compliance

- Need to define “Structure of Relationships” for the remainder of the process

- Create Policies as a “strategic” document
6.4 CIP-003-R4

6.4.1 Information including but not limited to, procedures, inventories, maps, detailed floor plans, equipment layouts, configurations and policies of CCAs be restricted to the personnel granted access to the physical or electronic CCAs.

6.4.2 This policy requires all electronic documents covered by this policy to be stored on a network server in directories whose access has been approved for the storage of sensitive information related to cyber security.

6.4.3 Access to electronic storage and the documents contained therein will be restricted to subgroups of individuals based upon roles outlined in the Section 5.0 Responsibilities and detailed as follows:
   - Content Owners (Read-Only)
   - Process Owners (Read-Only)
   - Approvers (Read-Only)
   - Document Owner (Read & Write)

6.4.4 All items and/or data connected to CIP-002 through CIP-0-09 must be considered as confidential. Internal and/or external distribution, except to the individuals filling the roles noted in 6.4.3 is prohibited unless otherwise approved in writing by the Senior Manager noted in Section 6.2 CIP-003 R2. The written authorization must be delivered to the Document Owner listed on the last page of this policy. Written authorization must include details regarding: Name & Title of Receiving Party, Name & Title of Requestor, Reason, and Duration of Request.

6.5 CIP-003-R5

6.5.1 Entity will restrict the ability to authorize access to CCAs to senior management associated with each critical asset identified as process owners in Section 5.0 Responsibilities.

6.5.2 Entity will identify those individuals who have the authority to grant access whether physical or electronic to CCAs.

6.5.3 Authorizing entities identified in Section 6.5.1 will be listed in a document entitled the Access Authorities List (AAL-1.0) and will be attached to this policy.

6.6 CIP-003-R6

6.6.1 Changes to CCAs must be properly evaluated, authorized, and tested.

6.6.2 The change management process must be documented and included in the System Management Document, described in CIP-007.

6.6.3 Changes requiring adherence to this policy may include but are not limited to:
   - Applying software or firmware patches and/or upgrades
   - Upgrading and/or replacing hardware components
   - Changes, fixes, upgrades to software or database components
   - Configuration changes to systems, applications, and hardware
Strategic View of Security Management
Thank You

Ben Church, CISSP
Burns & McDonnell
bchurch@burnsmcd.com