



Critical Asset Criteria for ERCOT – Discussion Paper

Bill Bojorquez
Director, ERCOT System Planning

Discussion Paper
November 1, 2006

NERC Cyber Security Standards

On May 2, 2006 NERC's Board of Trustees adopted 8 new Reliability Standards with respect to Cyber Security effective June 1, 2006.

- CIP-002-1: Critical Cyber Asset Identification
- CIP-003-1: Security Management Controls
- CIP-004-1: Personnel & Training
- CIP-005-1: Electronic Security Perimeter(s)
- CIP-006-1: Physical Security
- CIP-007-1: Systems Security Management
- CIP-008-1: Incident Reporting & Response Planning
- CIP-009-1: Recovery Plans for Critical Cyber Assets

These new standards, along with CIP-001-0: Sabotage Reporting (effective 4/1/2005) comprise NERC's Physical and Cyber Security standards.

Focus of this presentation will be on CIP-002-1: Critical Cyber Asset Identification.

CIP-002-1: Critical Cyber Asset Identification

Applicability:

- Reliability Coordinator
- Balancing Authority
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generation Owner
- Generation Operator
- Load Serving Entity
- NERC
- Regional Reliability Organizations

Exempt:

- Facilities regulated by the US Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
- Cyber Assets associated with communication networks & data communication links between discrete Electronic Security Perimeters.

Requirements:

- Identify & document a risk based assessment methodology to identify Critical Assets.
- Identify list of Critical Assets based on the risk based assessment methodology.
- Using list of Critical Assets, develop a list of associated Critical Cyber Security Assets essential to the operation of the Critical Asset.
- Senior management review and approval of list of Critical Assets and Critical Cyber Security Assets annually.

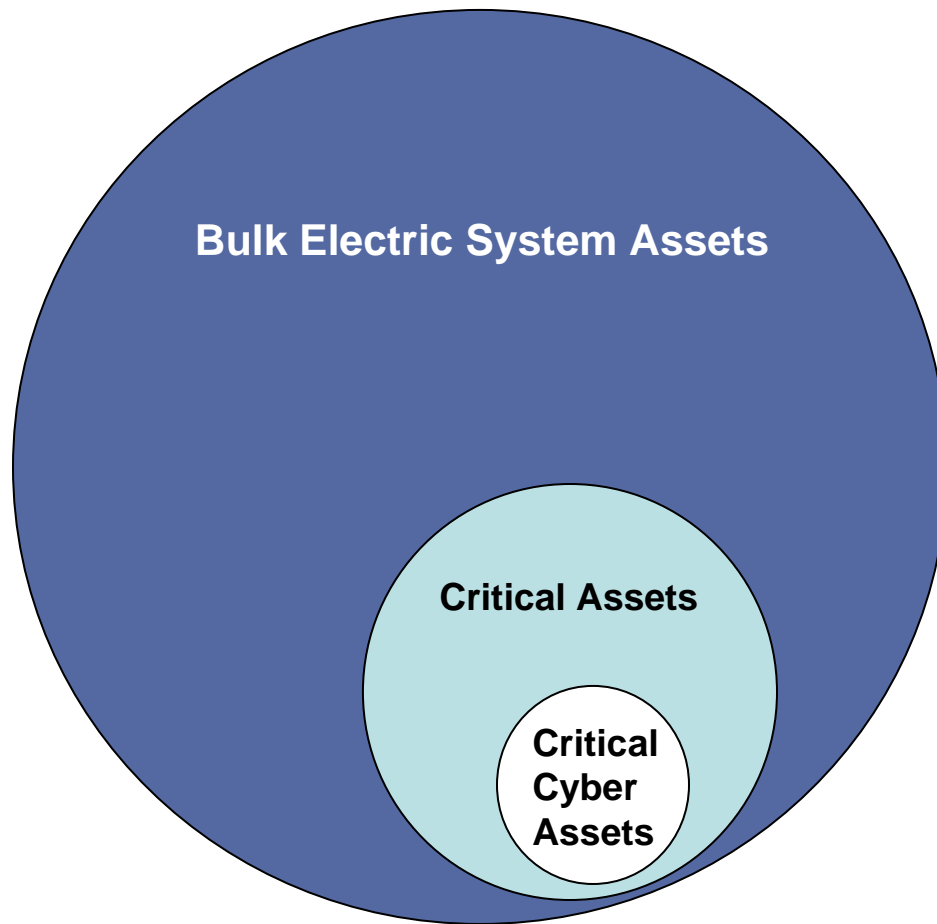
Key NERC Definitions

Bulk Electric System:	The electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included.
Critical Assets:	Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.
Cyber Assets:	Programmable electronic devices and communication networks including hardware, software, and data.
Critical Cyber Assets:	Cyber Assets essential to the reliable operation of Critical Assets.

Key NERC Definitions

Bulk Electric System:	The electrical generation resources , transmission lines , interconnections with neighboring systems, and associated equipment , generally operated at voltages of 100 kV or higher . Radial transmission facilities serving only load with one transmission source are generally not included.
Critical Assets:	Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System .
Cyber Assets:	Programmable electronic devices and communication networks including hardware, software, and data.
Critical Cyber Assets:	Cyber Assets essential to the reliable operation of Critical Assets.

Critical Asset Relationships



**Critical Assets
are a subset of
the Bulk Electric
System Assets**

**Critical Cyber
Assets support
the reliable
operation of
Critical Assets**

Critical Asset Selection Process

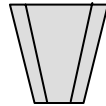
Steps --

1

Bulk Electric
System Assets

Inputs - List of generating resources; control centers & backup control centers; system restoration, automatic load shedding, & system protection assets, etc.

2



Filtering - Risk Based Assessment
(*Required Document*)



Critical
Assets

Output - List of Critical Assets
(*Required Document*)

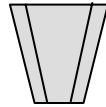
3

Cyber
Assets

Inputs - Cyber assets supporting Critical Assets



4



Filtering - Essential to operation of critical asset and meet CIP 002 R3










Critical
Cyber
Assets

Output - List of Critical Cyber Assets
(*Required Document*)

This presentation
will discuss only
Steps 1 & 2

Step 1: Develop a List of Bulk Electric System Assets

Per CIP-002, R1.2; the following assets must be considered as input in ERCOT's risk based assessment:

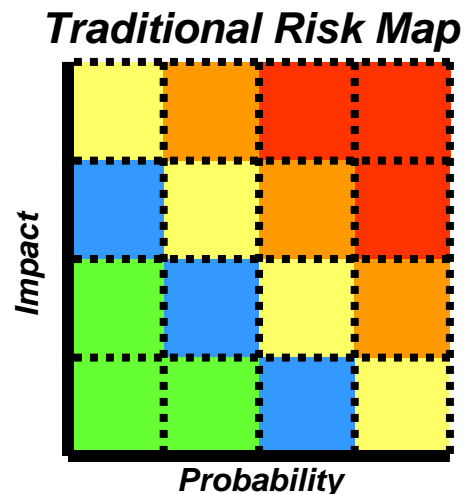
-  Control Centers and backup Control Centers;
-  Transmission substations that support the reliable operation of the Bulk Electric System;
-  Generation resources that support the reliable operation of the Bulk Electric System;
-  Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration;
-  Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more;
-  Special Protection Systems that support the reliable operation of the Bulk Electric System; and
-  Any additional assets that support the reliable operation of the Bulk Electric System.

Step 2: Perform a Risk Based Assessment

ERCOT could perform a series of Risk Based Assessments on the assets of the Bulk Electric System to identify ERCOT's Critical Asset inventory.

Types of risk based assessments to be utilized:

- Calculation based
- Study based
- Experienced based
- Combination of the above



Risk Assessment Basis: If the asset were to be compromised or removed from service, what would be the impact, either direct or indirect to bulk electric system reliability or operability?

Identify & document a risk based assessment methodology ...

ERCOT proposes the following components for a risk-based assessment methodologies to identify Critical Assets:

Lines and Substations

- Annual Voltage and Transient Stability Survey
 - Determine the performance of power system under normal and fault conditions
 - Determine list of events that might result significant loss of transmission, load or generation due to
 - Voltage collapse
 - Transient instability (generator angle separation or voltage recovery violation)

Generators

- Generation Must Run Analysis
- Generation Black Start Analysis

Control Centers

- ERCOT and TO Control Centers are included in CIP-002
- QSE Scheduling Centers and backup Centers which would affect the reliability or operability of the Bulk Electric System.

Identify list of Critical Assets based on the risk based assessment methodology ...

DRAFT minimum list based on the methodology above:

- ERCOT Control Center and backup Control Center;
- TDSP Control Center and backup Centers controlling facilities over 100kV
- QSE Scheduling Centers and backup Centers as follows:
 - QSE Scheduling Centers of Must Run, Nuclear Plants and Black Start units
 - QSE Level 4 Scheduling Centers
 - QSE Level 3 Scheduling Centers controlling over X,XXX MW of generation
- Substations deemed critical due to a series of planning/operating Voltage Stability and Transient Stability Analysis

ERCOT will work with stakeholders to review methodology and promulgate new Protocol or Operating Guide Revisions necessary to comply with the requirements of CIP-002.

Questions