

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Categorizing Cyber Systems: An Approach Based on BES Reliability Functions

Cyber Security Order 706 Standard Drafting
Team (Project 2008-06)

August 25, 2009

to ensure
the reliability of the
bulk power system

Presentation Outline

- Background and History
- CIP Version 3 Key Guiding Principles
- Purpose and Approach of Concept Paper
- BES Subsystems and Cyber Systems
- Proposed Categorization Methodology
- Target of Protection
- Conclusion and What's Next

- FERC's Cyber Security Order 706 directed extensive modifications of CIP-002 through CIP-009 (Version 1)
 - Address the near term specific directives → Version 2
 - Submitted to FERC for Approval (May 22, 2009)
- Current Phase – Starting to address all remaining issues from FERC Order 706 and as raised by industry in the SAR → Version 3

Initial Considerations

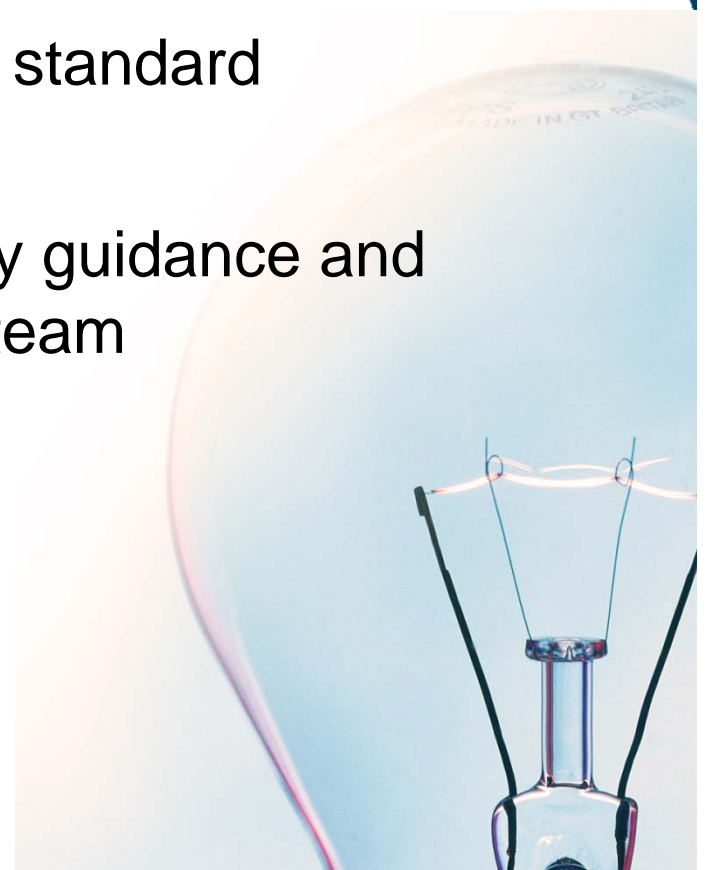
- Addressing issues with CIP-002-1 approach and methodology
 - Concept paper ***Categorizing Cyber Systems
An Approach Based on BES Reliability Functions***
- Looking at NIST and other frameworks for suggestions and guidance

CIP Version 3 Key Guiding Principles

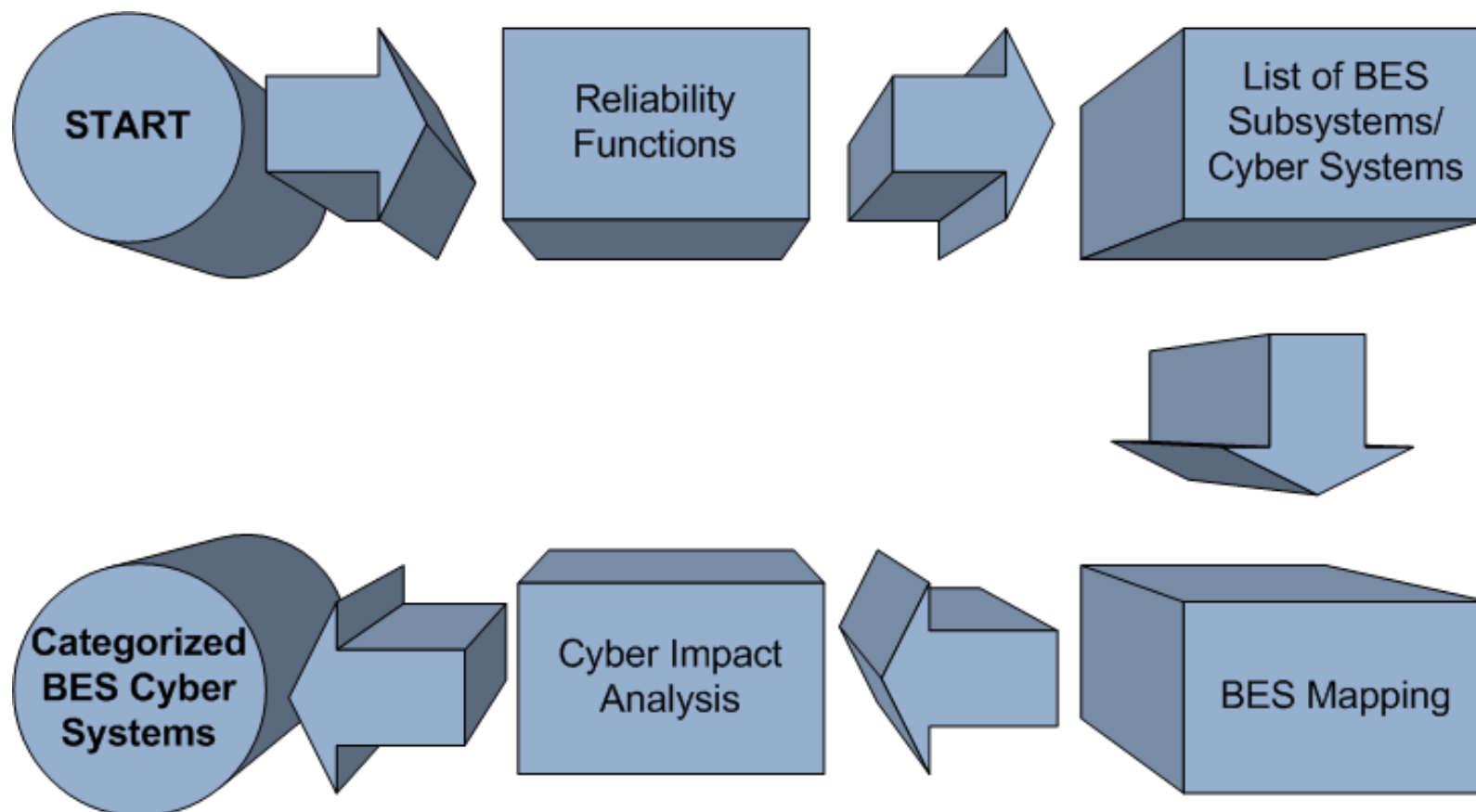
- The CIP Standards will:
 - Build on work already done complying with Version 1, including industry's experience and investment
 - Address the complex nature of BES functions and interconnected Cyber Systems, both within and between multiple organizations
 - Provide Entities with reasonable flexibility in applying equivalent security controls on the basis of compensating controls, cyber system characteristics, and operating environment considerations
 - Include all Cyber Systems impacting the reliability of the BES in scope

Concept Paper Purpose

- The purpose of the concept paper is:
 - Address foundational issues at a high level
 - Create an approach for Version 3 standard development
 - Provide an opportunity for industry guidance and direction to the standard drafting team



Concept Paper Approach



Differences Between Versions

Version 1 / Version 2

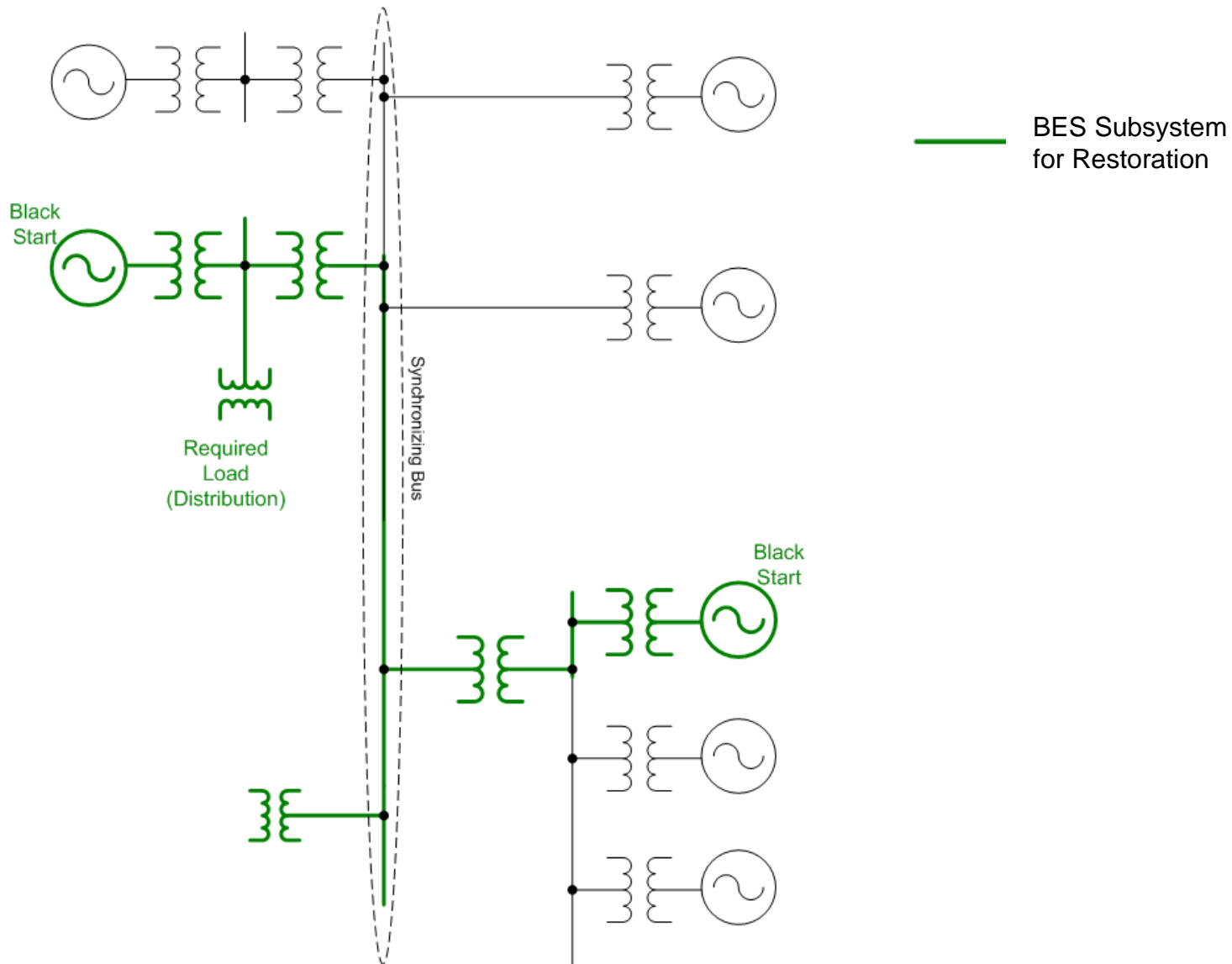
- Asset types to consider
- Critical Assets
- Critical Cyber Assets
- Critical / Not Critical
- “One size fits all” security

Version 3

- Reliability Functions
- BES Subsystems
- BES Cyber Systems
- Impact Levels
- Security commensurate with BES reliability impact

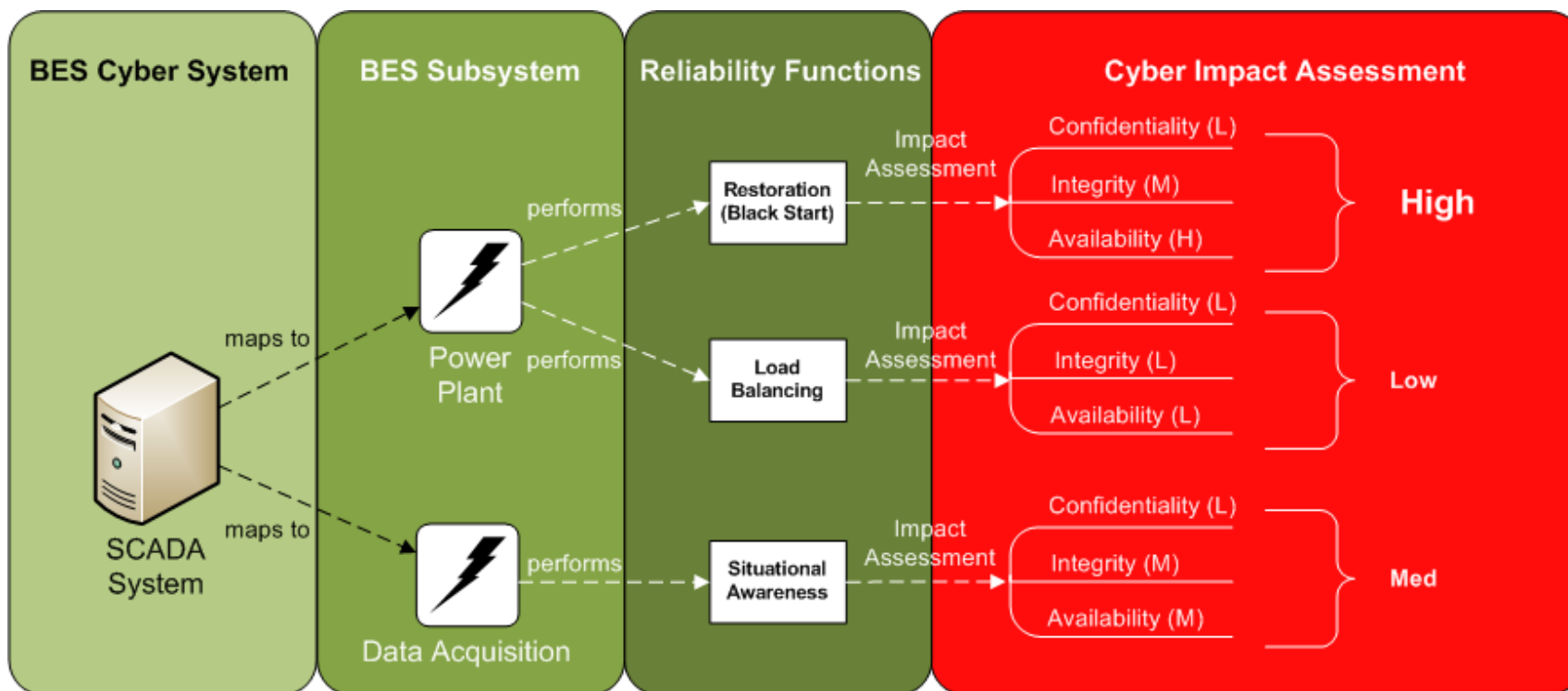
- **BES Subsystem:** The set of BES assets necessary to perform or support function(s) necessary to maintain an Adequate Level of Reliability (ALR)
 - May be defined as a piece of equipment, facility or system
- **Cyber Systems** performing or supporting functions necessary to maintain an ALR will be considered as both a BES Subsystem and a Cyber System
 - Captures both the reliability impact and the cyber impact
- **BES Subsystem Examples**
 - Restoration System (Black Start generators, cranking path elements – transformers, lines, reactive devices, load)
 - Load Control System (centralized, automated, programmable)

BES Subsystem Example - Restoration



- A discrete set of Cyber Assets organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
- Entities define their Cyber Systems to maximize efficiency in secure operations
- Cyber System Examples
 - EMS/SCADA System
 - Generation Control System (at the Plant)
 - Substation RTU/PLC
 - Microprocessor–based Relay

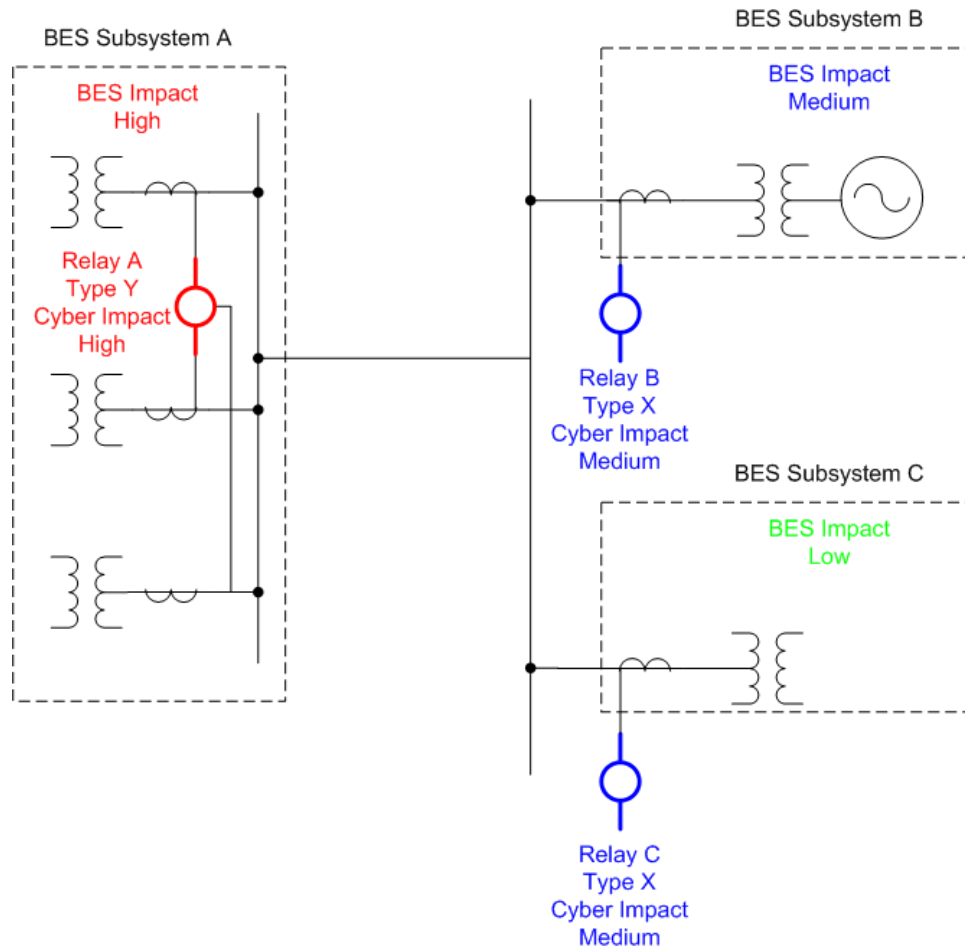
Sample Categorization of Cyber Systems



Example Final Impact Categorization

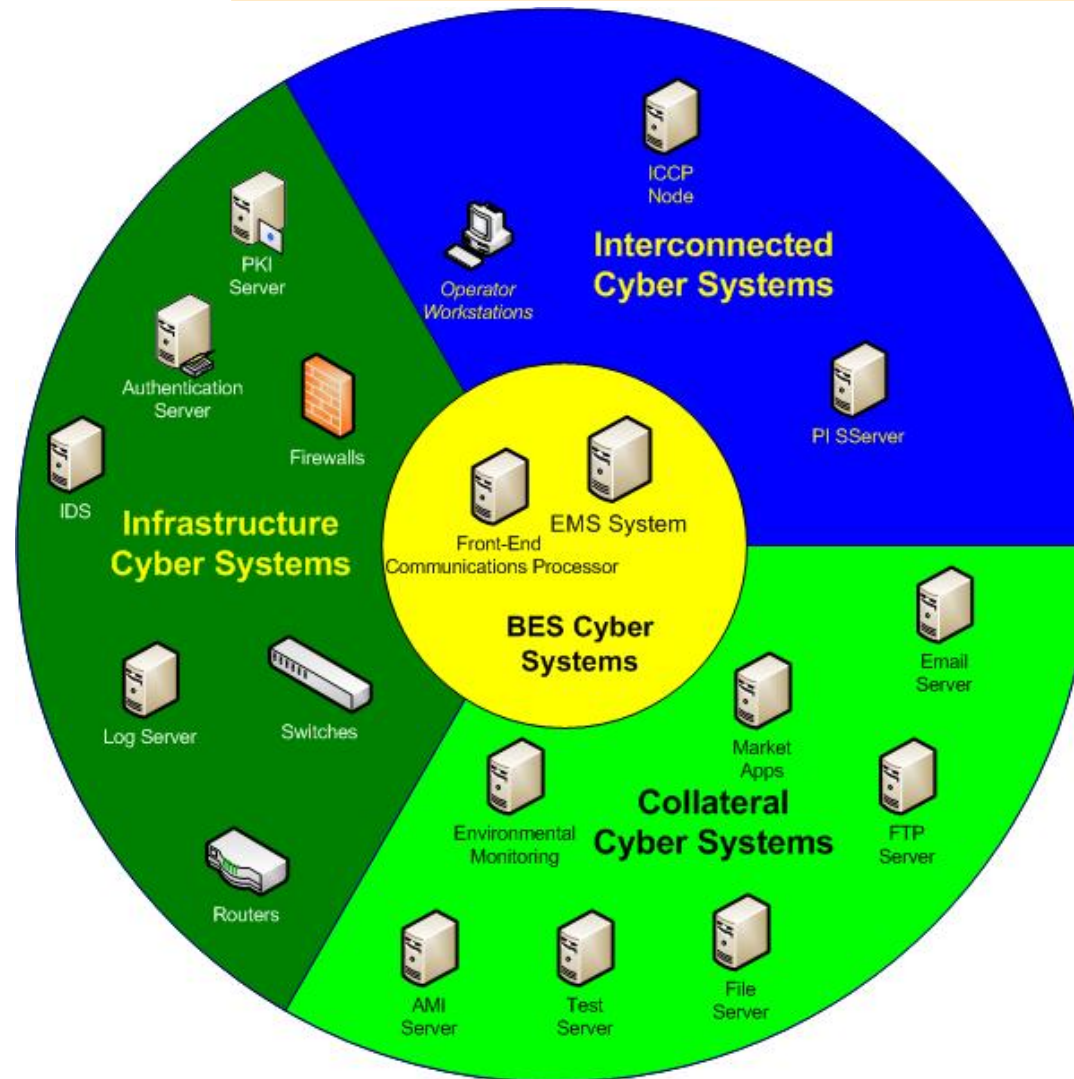
Asset Impact		Cyber Impact		
		High	Medium	Low
High	H	H	H	
Medium	H	M	M	
Low	H	M	L	

Final Impact Categorization Diagram



Identical Cyber Systems (Relay X) with the same cyber impact used in the same manner may be ultimately assigned different final categorizations, based on impact of the BES Subsystem they support

Target of Protection



Target of Protection – Control Center

- Apply to *Target of Protection* based on Final Impact Category (High, Medium, Low)
- Develop a library of security controls modeled after NIST 800-53 concepts appropriate to the degree and type of protection needed
- Consider operating environment differences in substations, generating plants and control centers
- Allow flexibility while ensuring adequate protection from dynamic and evolving threats and vulnerabilities

- All Bulk Electric System Subsystems inventoried and mapped to impact categories based on pre-determined criteria
- All Cyber Systems supporting real-time reliability and operability of BES Subsystems inventoried and categorized
- Final Impact Categorization links the Cyber System to the reliability of the BES
- Final product: Categorized list of Cyber Systems to be protected

- Standards Drafting Team (SDT) reviews comments to concept paper – September 2009
- SDT drafts CIP-002-3 with consideration of comments (September to December 2009)
 - Help from NERC Operating and Planning Committees members for BES functions and pre-determined engineering impact criteria
- First draft of CIP-002-3 posting for comment: December 2009/January 2010
- SDT continues work on library of security controls and application criteria

- Important step towards a more holistic approach to BES cyber security
- Industry stakeholder input and participation is key for all steps in the standards development from concept paper to final version and implementation plan
- **Remember: Industry Comments on the Concept Paper are due on September 4, 2009.**

(http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html)



Question & Answer

Contacts:

Joe Bucciero
Project Manager
joe.bucciero@gmail.com
(267) 981-5445

NERC

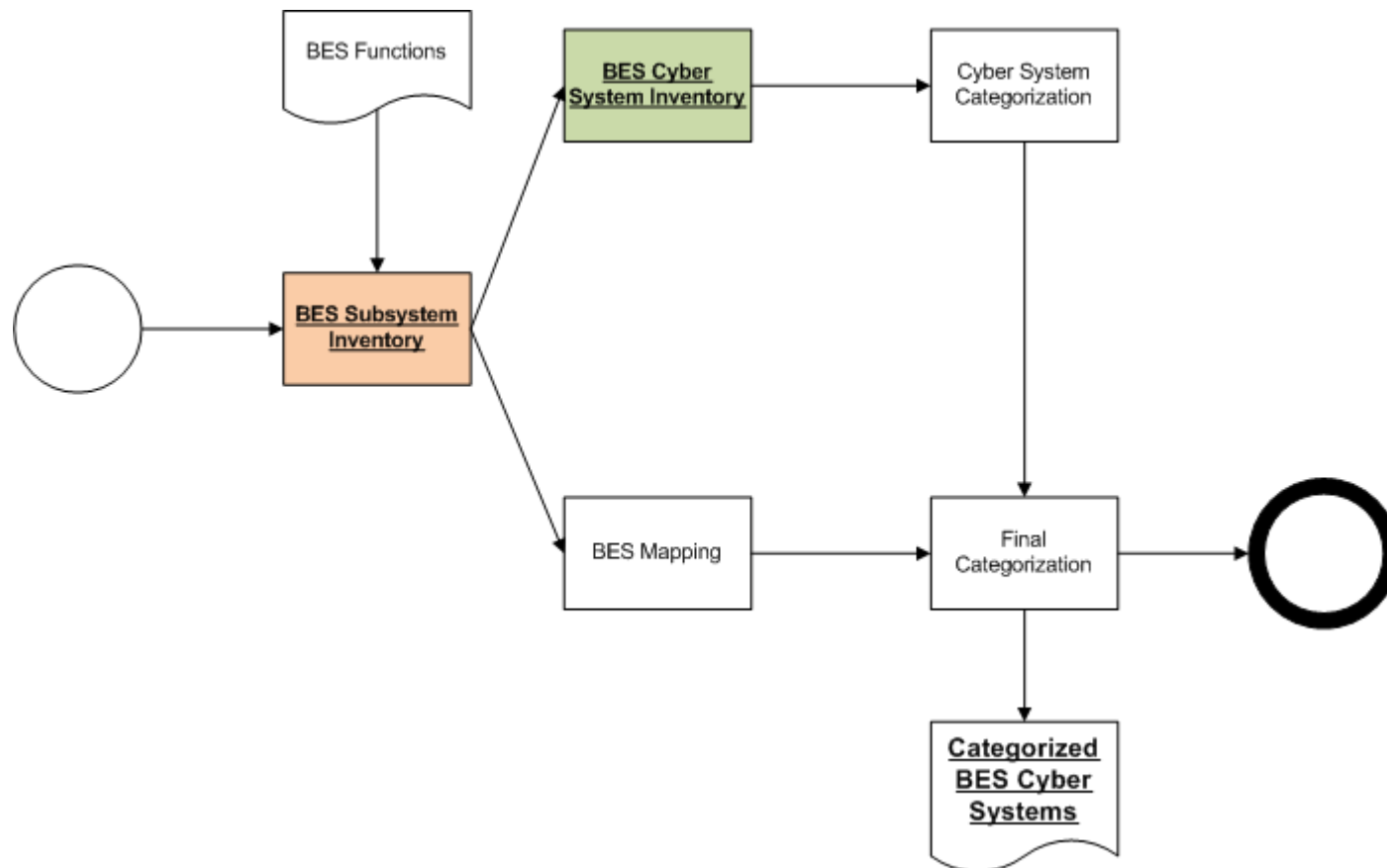
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Supplemental Slides for Q&A

to ensure
the reliability of the
bulk power system

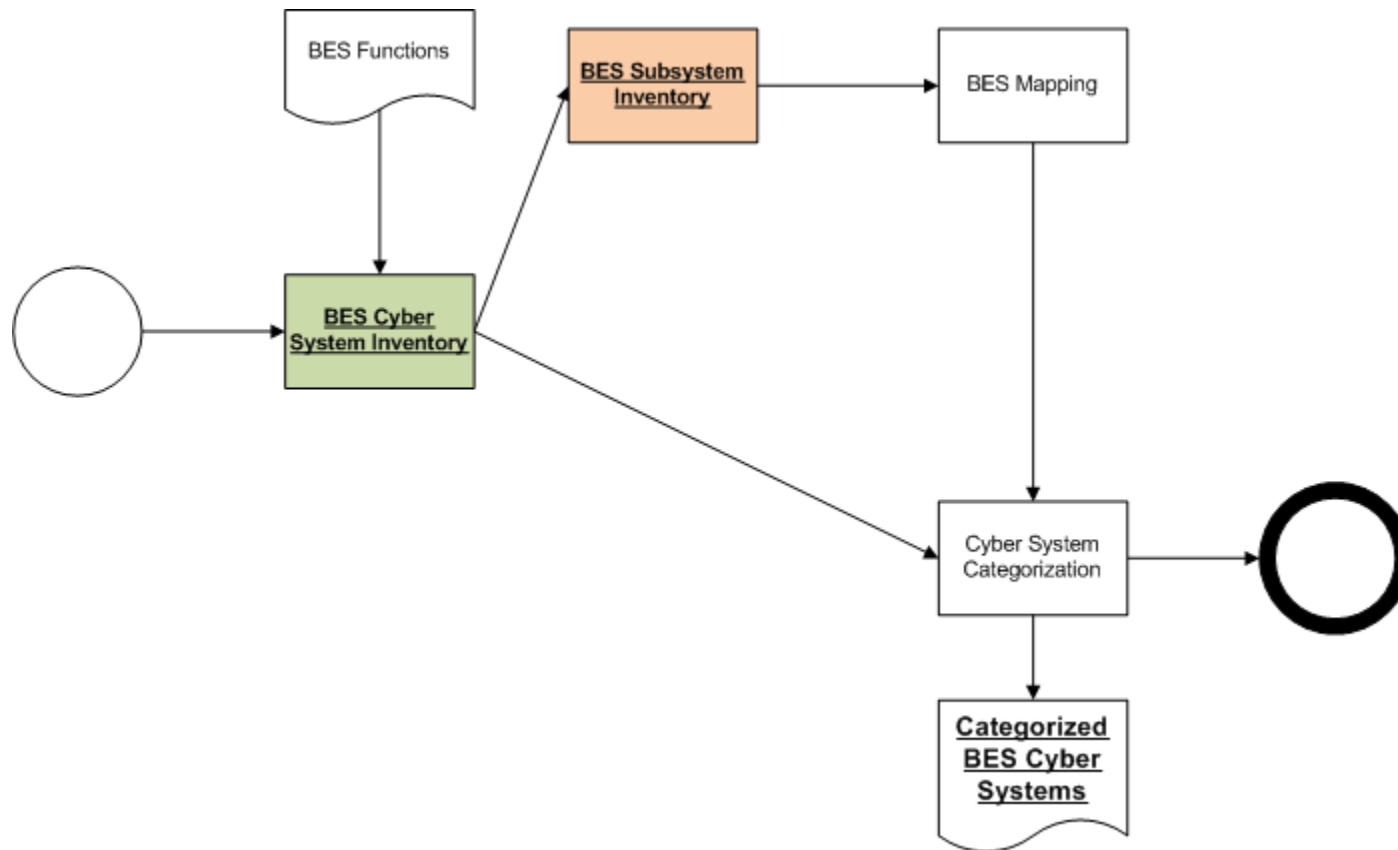
Summary Process Diagram (1/2)

BES Subsystem Centric

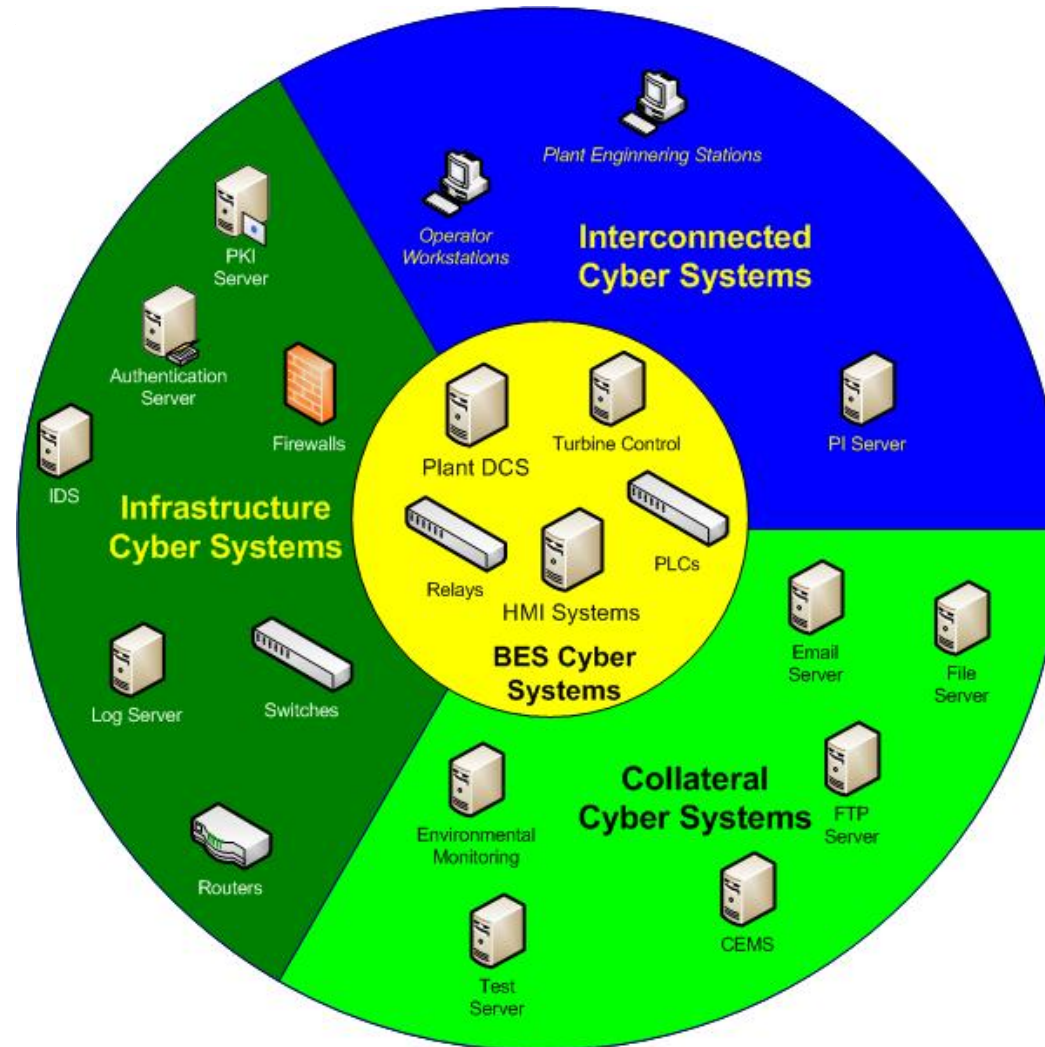


Summary Process Diagram (2/2)

Cyber System Centric

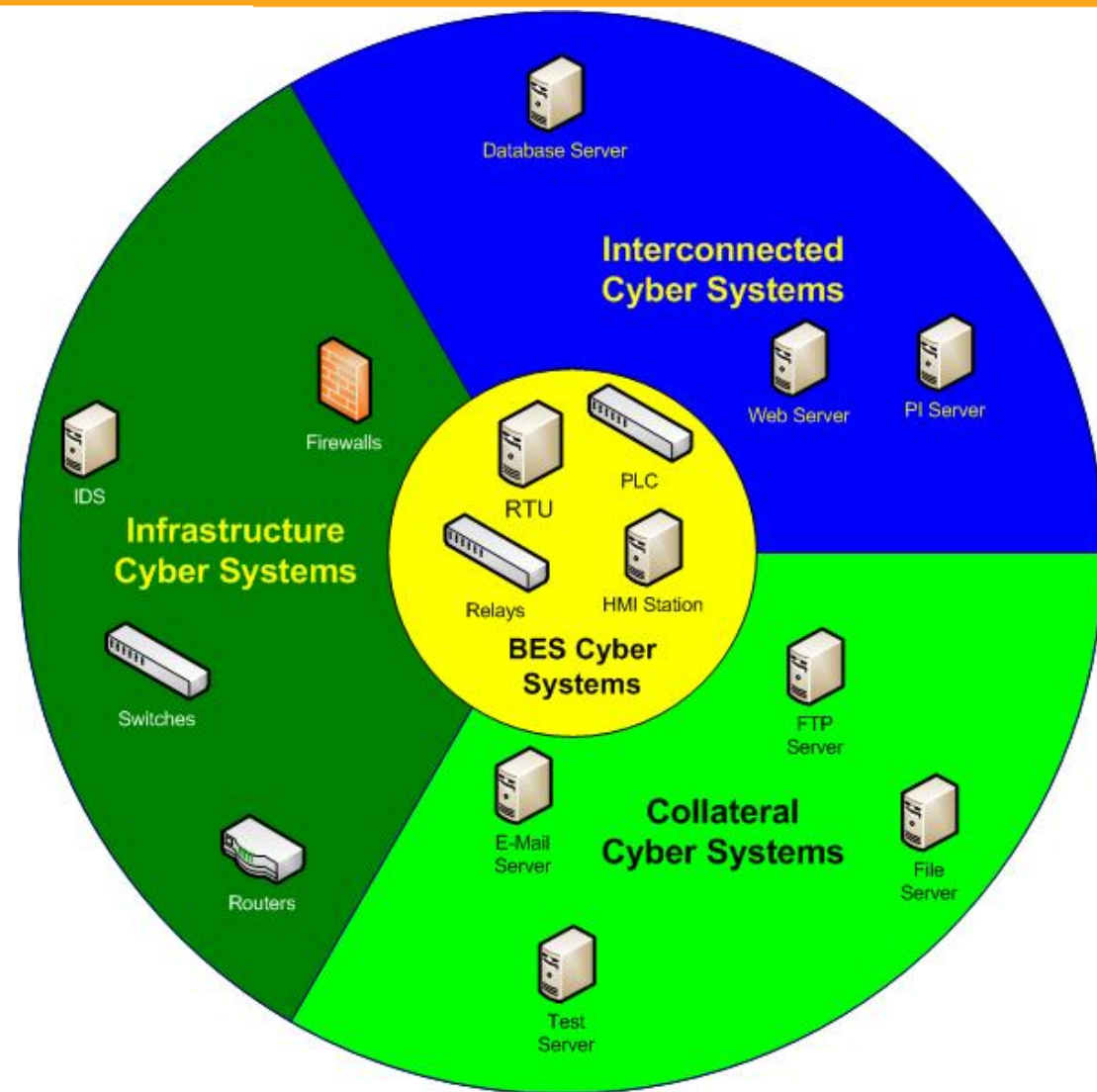


Target of Protection – Generation



Target of Protection – Generation

Target of Protection – Substation



Target of Protection – Transmission Substations

Reliability Impact of Cyber Systems

