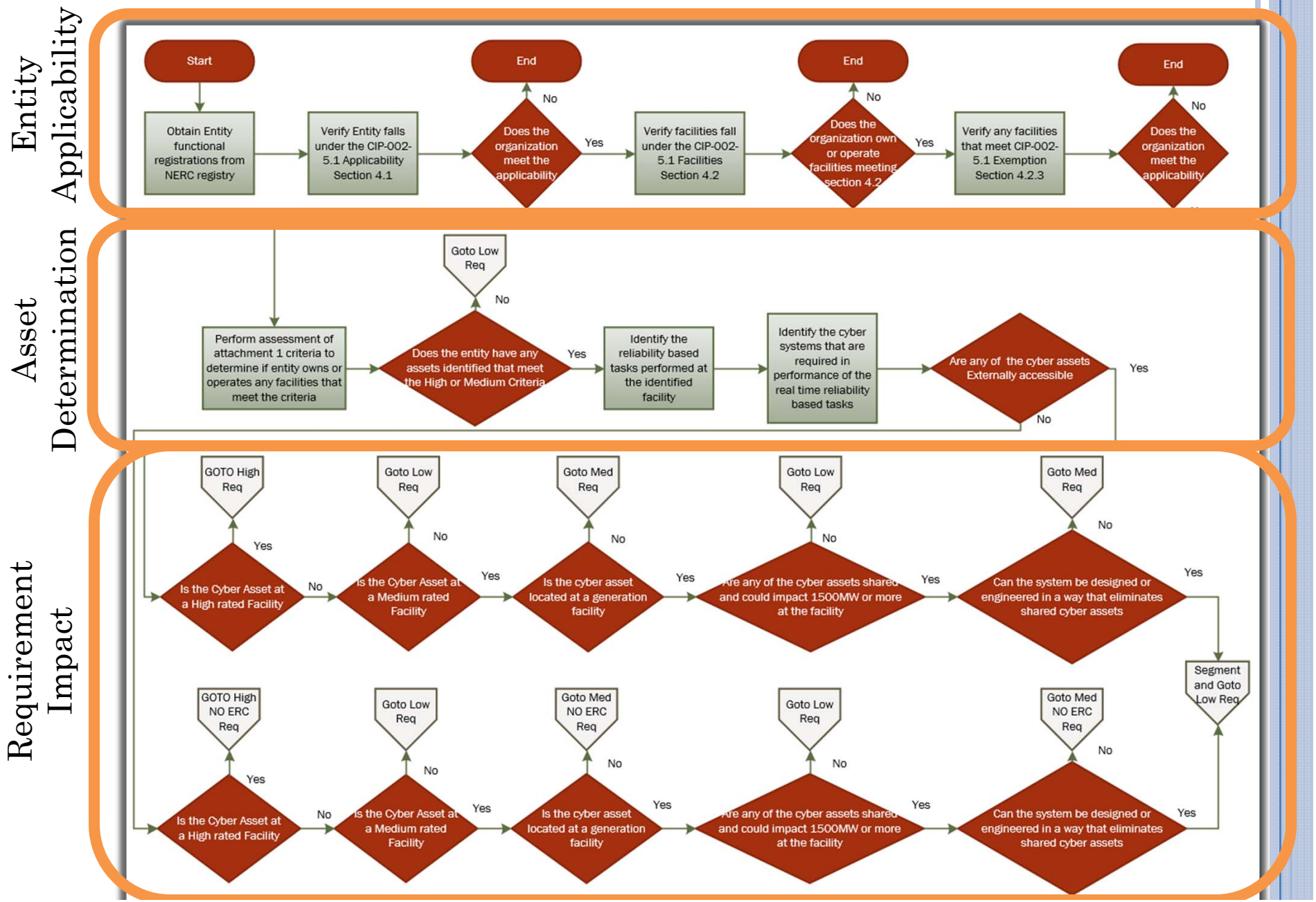
ABB NERC CIP v5 Special interest group
BES Cyber System Asset grouping

October 23, 2014

Agenda

- Quick review of first session
- Words with friends
- Requirement mapping effort
- Requirement mapping analysis
- BES Cyber Asset grouping discussion

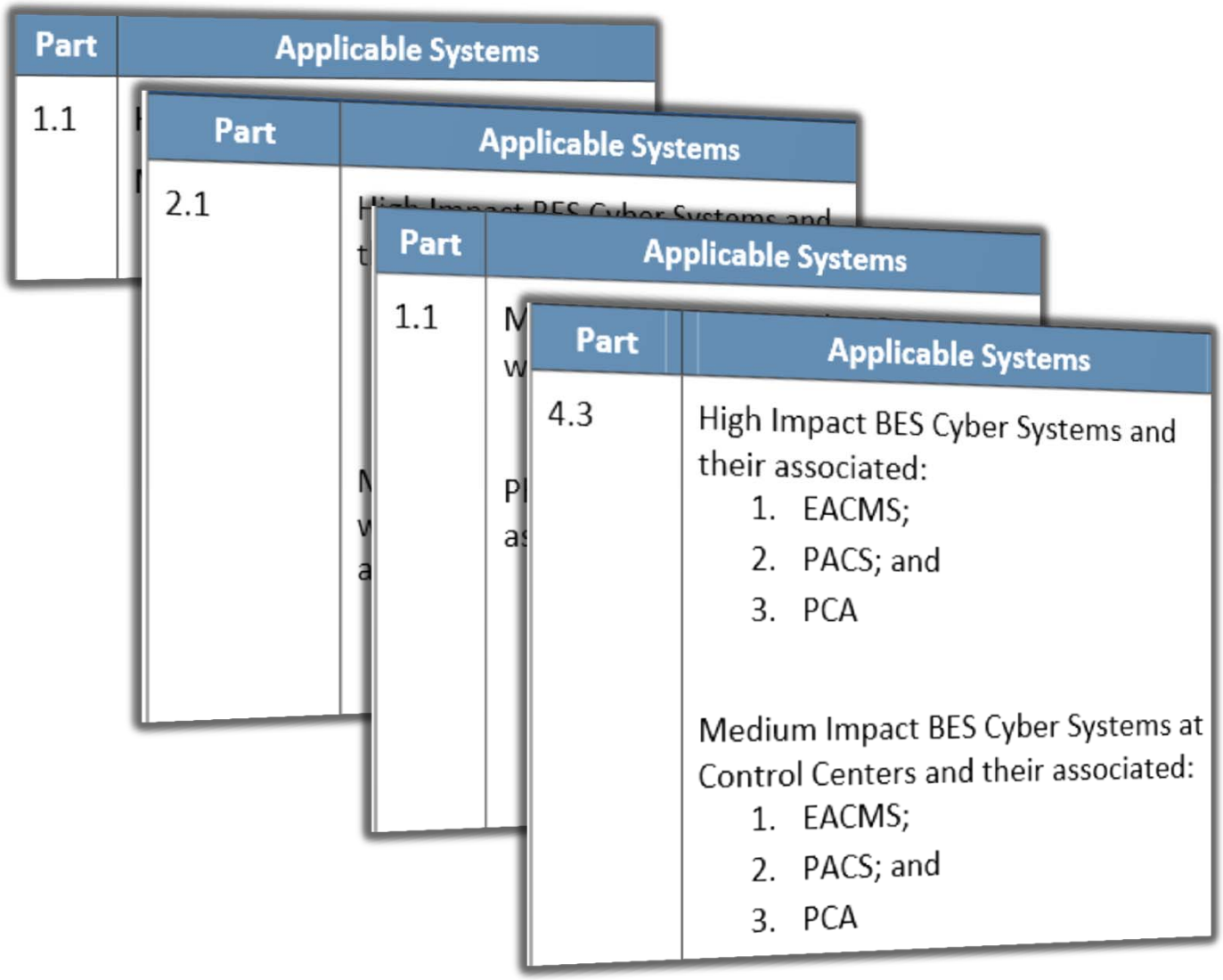
Previous Discussion



- **EAP** - A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.
- **EACMS** - Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.
  - EAP, Intermediate Systems, authentication servers, security event monitoring, intrusion detection systems
- **PACS** - Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

- **PCA** - One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. A Cyber Asset is not a Protected Cyber Asset if, for 30 consecutive calendar days or less, it is connected either to a Cyber Asset within the ESP or to the network within the ESP, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
- **ERC** - The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.
- **Intermediate System** - A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.

Matching Game



Requirements Mapping

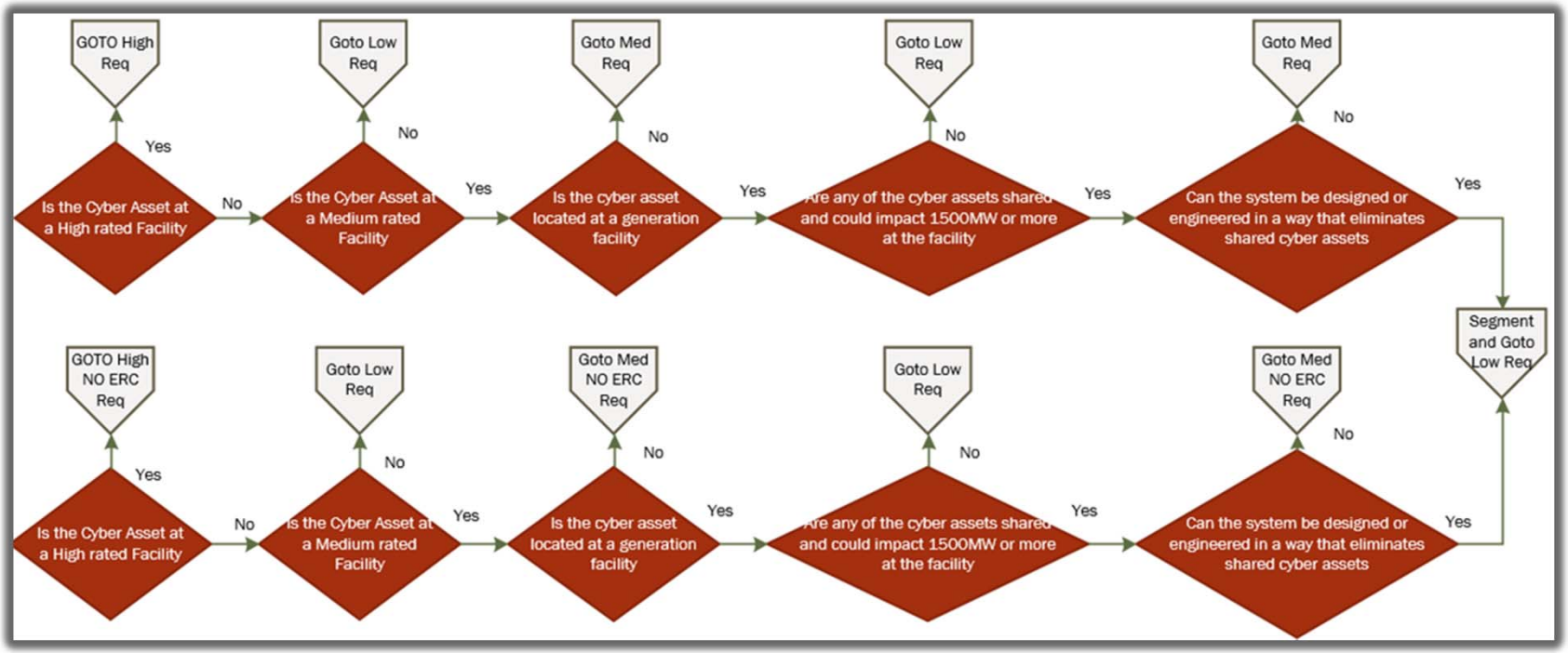
Standard	Requirement Part	Sub Parts	High	High and associated EACM and PAC	High and associated PAC	High and associated EACM	High with ERC and associated PCA	High and associated PCA	High EAP	High with Dial-up and associated PCA	High and associated Local hardware or devices at the PSP	Medium	Medium at control centers	Me cont cen asso EAC
CIP-002-5.1														
	R1 - 1.1		x											
	R1 - 1.2											x		
	R1 - 1.3													
	R2 - 2.1		x									x		
	R2 - 2.2		x									x		
CIP-003-5														
	R1 - 1.1		x									x		
	R1 - 1.2		x									x		
	R1 - 1.3		x									x		
	R1 - 1.4		x									x		
	R1 - 1.5		x									x		
	R1 - 1.6		x									x		
	R1 - 1.7		x									x		
	R1 - 1.8		x									x		
	R1 - 1.9		x									x		
	R2 - 2.1													
	R2 - 2.2													
	R2 - 2.3													
	R2 - 2.4													
	R3		x									x		
	R4		x									x		
CIP-004-5.1														
	R1 - 1.1		x									x		
	R2 - 2.1			x										
		R2 - 2.1.1		x										
		R2 - 2.1.2		x										
		R2 - 2.1.3		x										
		R2 - 2.1.4		x										
		R2 - 2.1.5		x										
		R2 - 2.1.6		x										
		R2 - 2.1.7		x										
		R2 - 2.1.8		x										
		R2 - 2.1.9		x										
	R2 - 2.2			x										
	R2 - 3			x										

Requirements Mapping

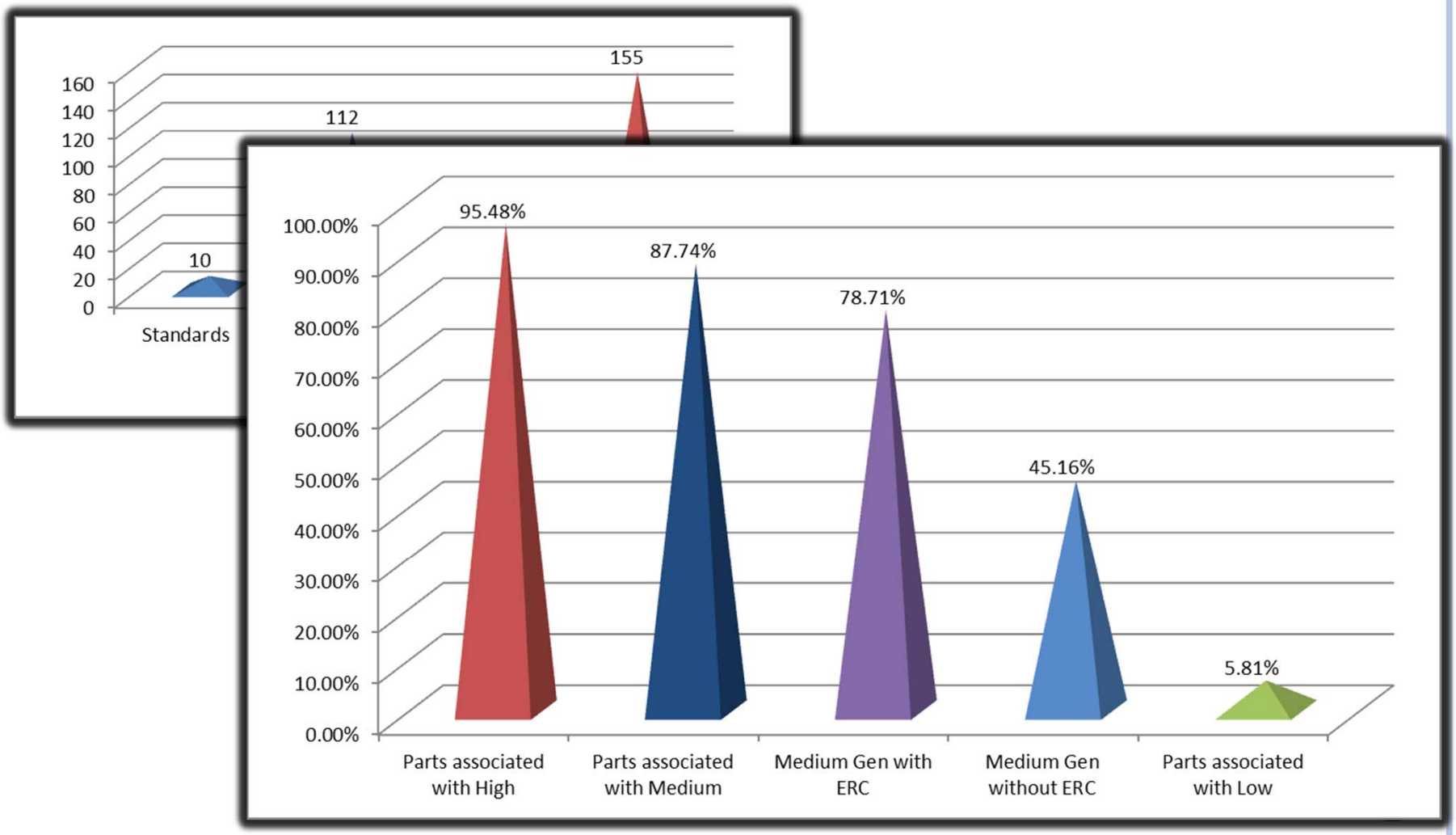
CIP-002 | CIP-003 | CIP-004 | CIP-005 | CIP-006 | CIP-007 | CIP-008 | CIP-009 | CIP-010 | CIP-011

Standard	Requirement Part	Sub Parts	High	High and associated PAC	High and associated EACM	High and associated PCA	Medium at control centers	Medium at control centers and associated EACM and PCA	Medium at Control Centers and associated EACM, PAC, and PCA	Medium and associated EACM, PAC, and PCA	Medium With ERC and associated EACM and PAC	Medium with ERC and associated PAC	Medium with ERC and associated PCA	Medium with ERC and associated EACM and PCA
CIP-007-5														
	R1 - 1.1			x	x	x						x		x
	R1 - 1.2		x				x							
	R2 - 2.1			x	x	x				x				
	R2 - 2.2			x	x	x				x				
	R2 - 2.3			x	x	x				x				
	R2 - 2.4			x	x	x				x				
	R3 - 3.1			x	x	x				x				
	R3 - 3.2			x	x	x				x				
	R3 - 3.3			x	x	x				x				
	R4 - 4.1			x	x	x				x				
		R4 - 4.1.1		x	x	x				x				
		R4 - 4.1.2		x	x	x				x				
		R4 - 4.1.3		x	x	x				x				
	R4 - 4.2			x	x	x					x		x	
		R4 - 4.2.1		x	x	x					x		x	
		R4 - 4.2.2		x	x	x					x		x	
	R4 - 4.3			x	x	x		x						
	R4 - 4.4				x	x								
	R5 - 5.1			x	x	x			x		x		x	
	R5 - 5.2			x	x	x				x				
	R5 - 5.3			x	x	x					x		x	
	R5 - 5.4			x	x	x				x				
	R5 - 5.5			x	x	x				x				
		R5 - 5.5.1		x	x	x				x				
		R5 - 5.5.2		x	x	x				x				
	R5 - 5.6			x	x	x					x		x	
	R5 - 5.7			x	x	x			x					

Requirements Mapping



DATA


160
140
120
100
80
60
40
20
0
155
112
10
Standards
100.00%
90.00%
80.00%
70.00%
60.00%
50.00%
40.00%
30.00%
20.00%
10.00%
0.00%
95.48%
87.74%
78.71%
45.16%
5.81%
Parts associated with High
Parts associated with Medium
Medium Gen with ERC
Medium Gen without ERC
Parts associated with Low

The Story Behind the data

- Medium generation Facility BES Cyber Systems with ERC must comply with the majority of the requirements – 78%
- Medium generation Facility BES Cyber Systems without ERC must comply with less than half of the requirements – 45%
- Many of the items in scope for Generation Non-ERC include: governance, procedural or programmatic requirements within CIP-002, 003, 004, 008, and 011. Comprising 33 parts, leaving 37 requirements for Non-ERC (approx. 24%)

Approach Discussion

- Develop accurate inventory
- Develop operational logic flow

- Can you segment and reduce to low?
- Can you eliminate ERC requirements?

- Analyze BES Cyber System grouping strategies

BES Cyber System Grouping

Cyber Asset

- Programmable electronic devices, including the hardware, software, and data in those devices.

BES Cyber Asset

- A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System.

BES Cyber System

- One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

Quick Note on BES Cyber System

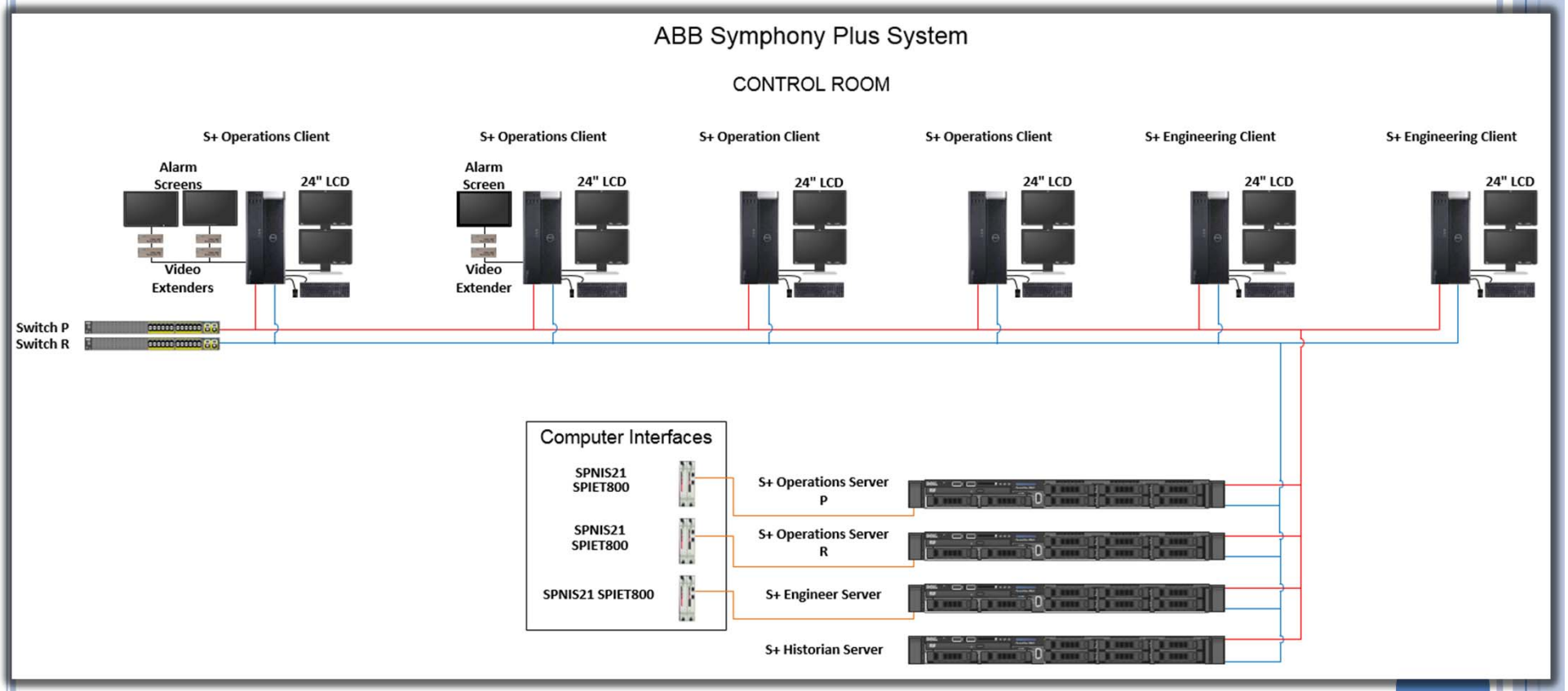
- The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Open Items

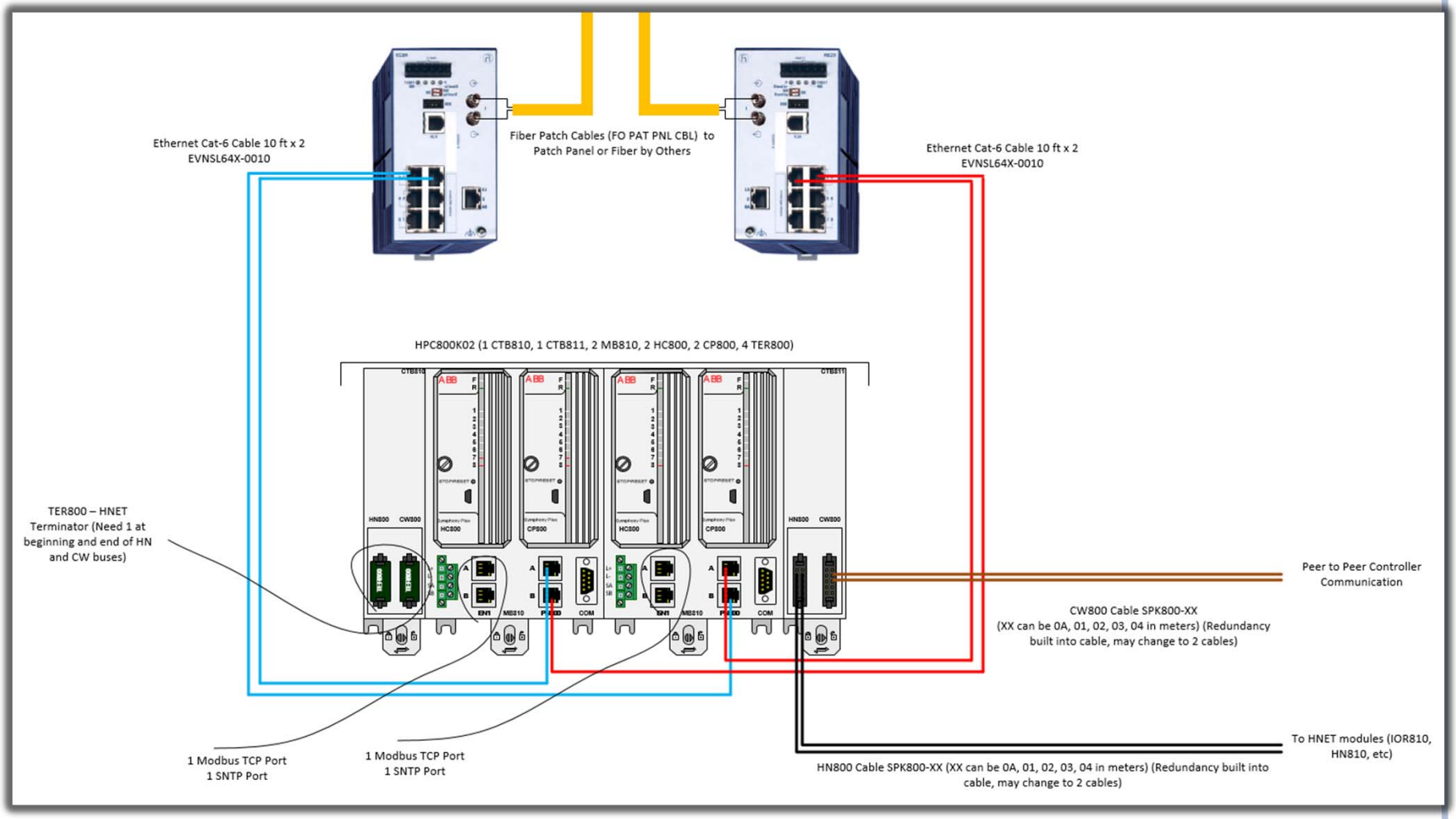
- Clarity on Programmable
- Clarity on 15 min impact – FERC directed NERC to conduct an industry survey regarding the scope of the term BES Cyber Asset. NERC has provided an Update and intends to leverage the study participants to respond to FERC
- Joint ownership

http://www.nerc.com/pa/CI/Pages/Transition-Program.aspx

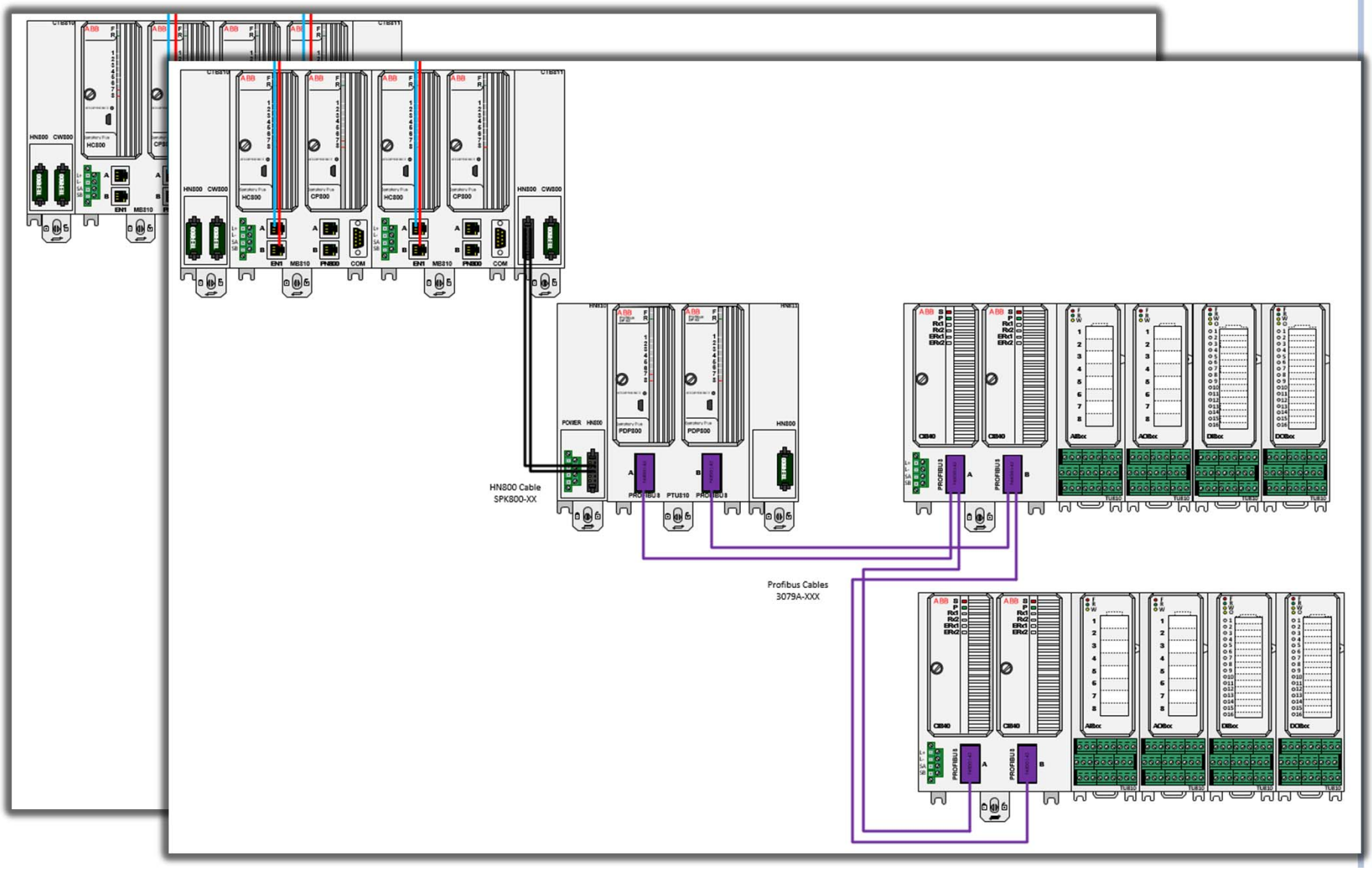
ABB Specific Discussions



CONTROLLER LEVEL



I/O Level



STRATEGY

- It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems.

Next Session

- Low and recently balloted CIP V 6
- Survey participants to gauge need for additional sessions on specific requirement struggles
- Schedule additional sessions if needed depending on survey feedback
- Hold as needed deep dive conversations with customers who have specific questions or areas of concern


QUESTIONS