ABB NERC CIP v? Special Interest Group

August, 27 2015

Agenda

- Reference to where we have been
- CIP Magicians
- Are you audit ready?
- How much evidence do you need?
  - Trust us approach
  - Trust and verify approach
  - Verified and demonstrated approach

CIP V5 Special Interest Group

Methodology

Developed and delivered a common framework and workflow to perform CIP V 5 Methodology

Addressed generation specific system segmentation approach, benefits and risks

BES Systems

Developed and delivered a requirement mapping spreadsheet addressing numerous filtered approaches

Addressed impacts of ERC and BES Cyber System grouping strategy benefits and risks

Low Impact

Developed and delivered an analysis spreadsheet with the differences between the V5 and V6 Lows as they stand in the process today

Addressed some of the current relevant activity impacting NERC CIP regulation

Process Items

CIPv6 / v7 status update, ongoing SDT activity, RAI, Lessons Learned, RFI's, anticipated FERC response, and Transition Plan items

CIP Update (1)

- CIP v6 NOPR
  - Order likely this year
  - CIP v6 Standards likely effective 4/1/16
  - Comment period open through Sept 21
  - Intention to direct changes to CIP-006-6 and standards activity on supply chain risk
  - Questions on Remote access controls and vagueness of LERC definition

https://www.sans.org/webcasts/cip-v6-nopr-about-100707

http://www.securingthehuman.org/blog/2015/07/23/to-nerc-cip-version-6-and-beyond

https://www.ferc.gov/whats-new/comm-meet/2015/071615/E-1.pdf

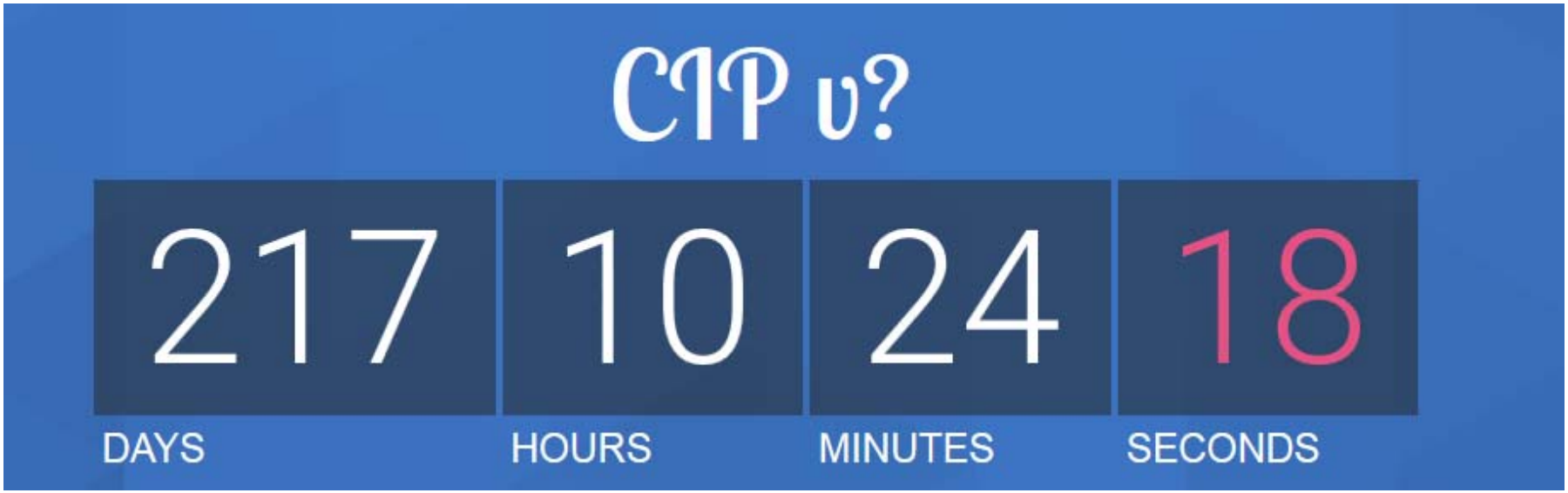
CIP Update (2)

- Implementation Guidance

Standard	Transition Study	Lessons Learned	Memo	Transition Update
• Clarity needed	• Areas identified	• FAQ's	• Removed Some Lessons Learned	• Repealed Memo
Nov 2013	Oct 2014	Jan 2015 - ongoing	Apr 2015	Jul 2015

http://www.securingthehuman.org/blog/2015/07/14/the-internet-of-cip-things-ioct

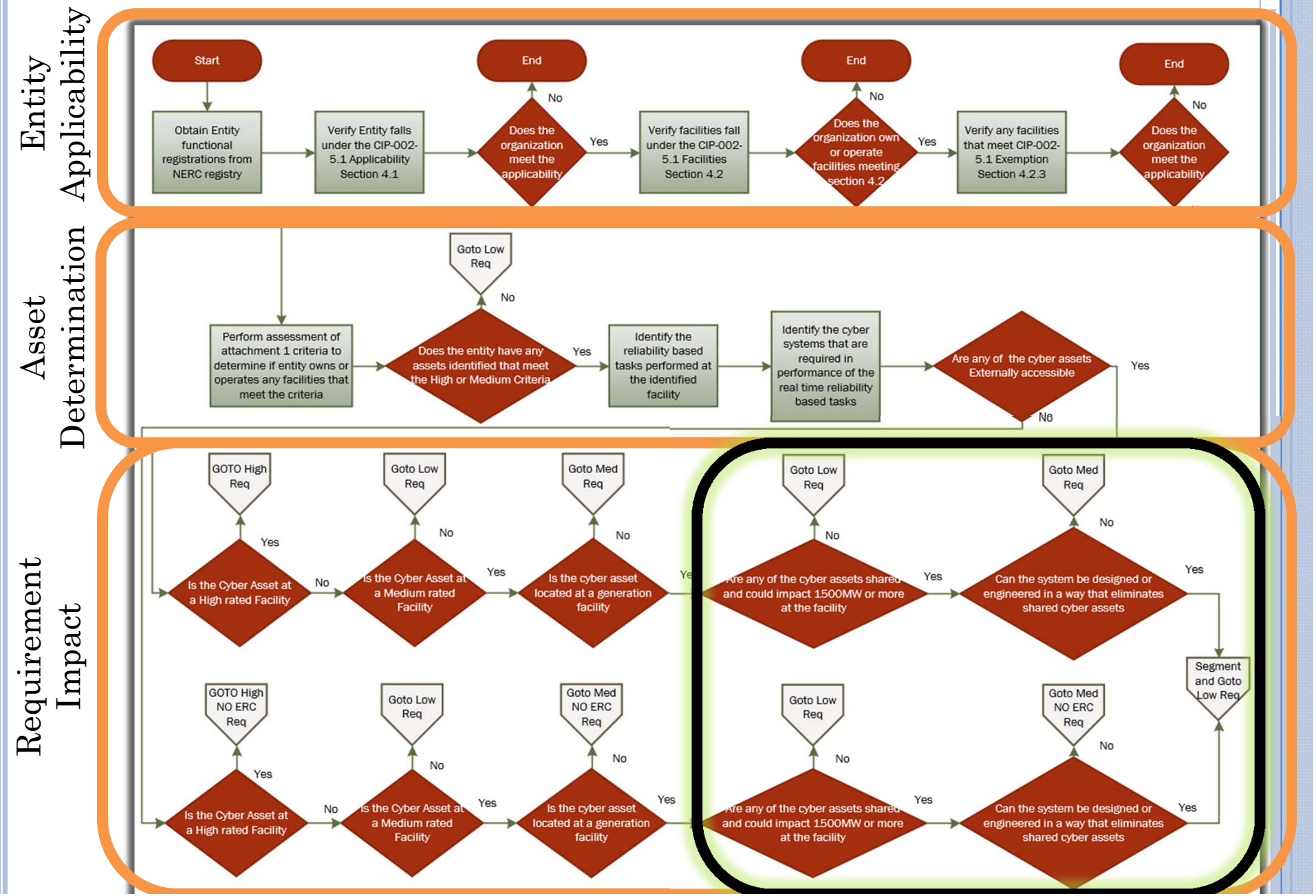
CIP Update (3)



CIP Magicians

Turning a Medium Impact Generation Site Into a Site With Low Impact BES Cyber Systems

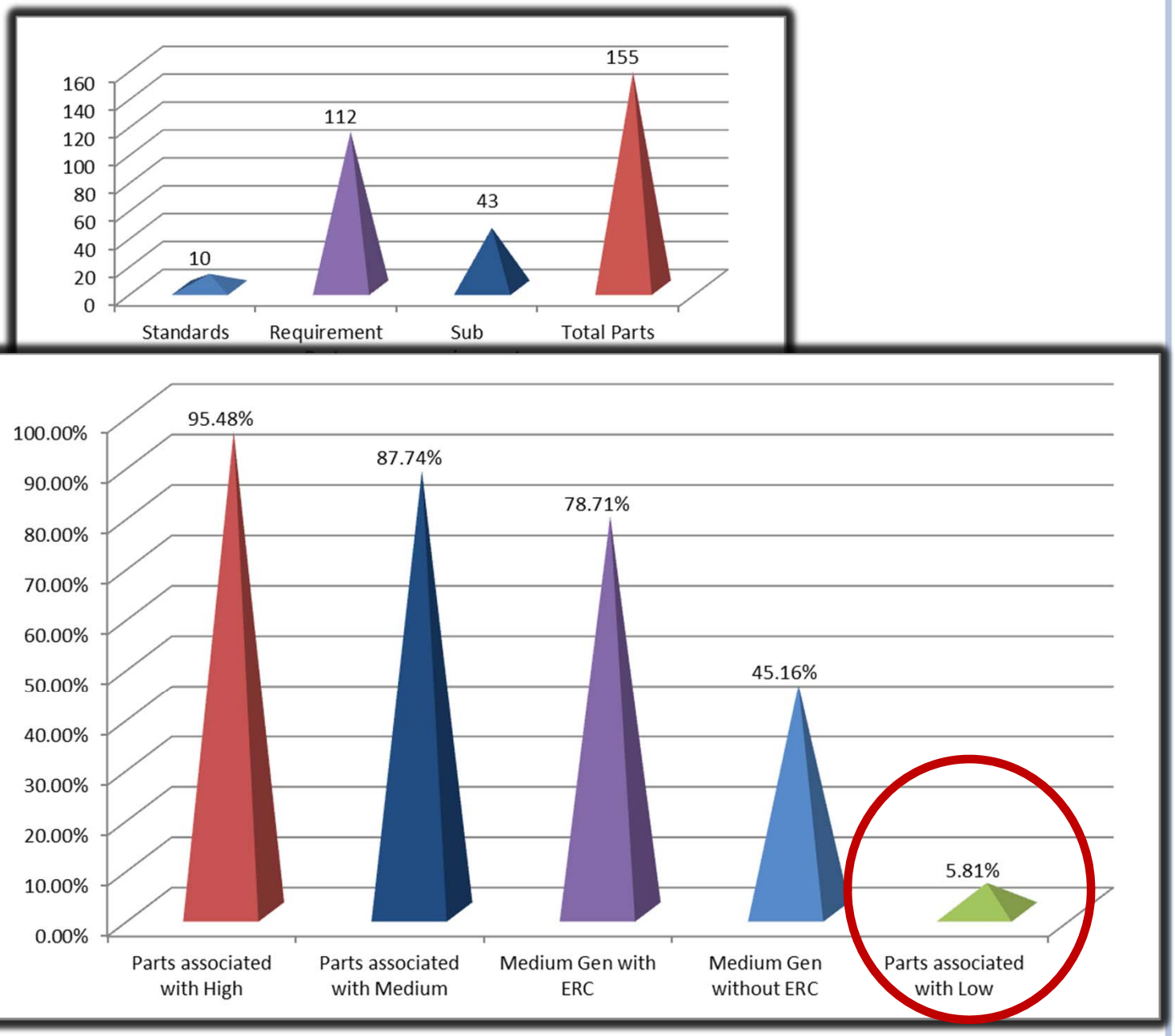
Big Picture


Entity Applicability
Start
Obtain Entity functional registrations from NERC registry
Verify Entity falls under the CIP-002-5.1 Applicability Section 4.1
End
Does the organization meet the applicability
No
Yes
Verify facilities fall under the CIP-002-5.1 Facilities Section 4.2
End
Does the organization own or operate facilities meeting section 4.2
No
Yes
Verify any facilities that meet CIP-002-5.1 Exemption Section 4.2.3
End
Does the organization meet the applicability
No
Asset Determination
Perform assessment of attachment 1 criteria to determine if entity owns or operates any facilities that meet the criteria
Goto Low Req
Does the entity have any assets identified that meet the High or Medium Criteria
No
Yes
Identify the reliability based tasks performed at the identified facility
Identify the cyber systems that are required in performance of the real time reliability based tasks
Are any of the cyber assets Externally accessible
Yes
No
Requirement Impact
GOTO High Req
Is the Cyber Asset at a High rated Facility
Yes
No
Goto Low Req
Is the Cyber Asset at a Medium rated Facility
No
Yes
Goto Med Req
Is the cyber asset located at a generation facility
No
Goto Low Req
Are any of the cyber assets shared and could impact 1500MW or more at the facility
No
Yes
Goto Med Req
Can the system be designed or engineered in a way that eliminates shared cyber assets
No
Yes
Segment and Goto Low Req
GOTO High NO ERC Req
Is the Cyber Asset at a High rated Facility
Yes
No
Goto Low Req
Is the Cyber Asset at a Medium rated Facility
No
Yes
Goto Med NO ERC Req
Is the cyber asset located at a generation facility
No
Yes
Goto Low Req
Are any of the cyber assets shared and could impact 1500MW or more at the facility
No
Yes
Goto Med NO ERC Req
Can the system be designed or engineered in a way that eliminates shared cyber assets
No
Yes

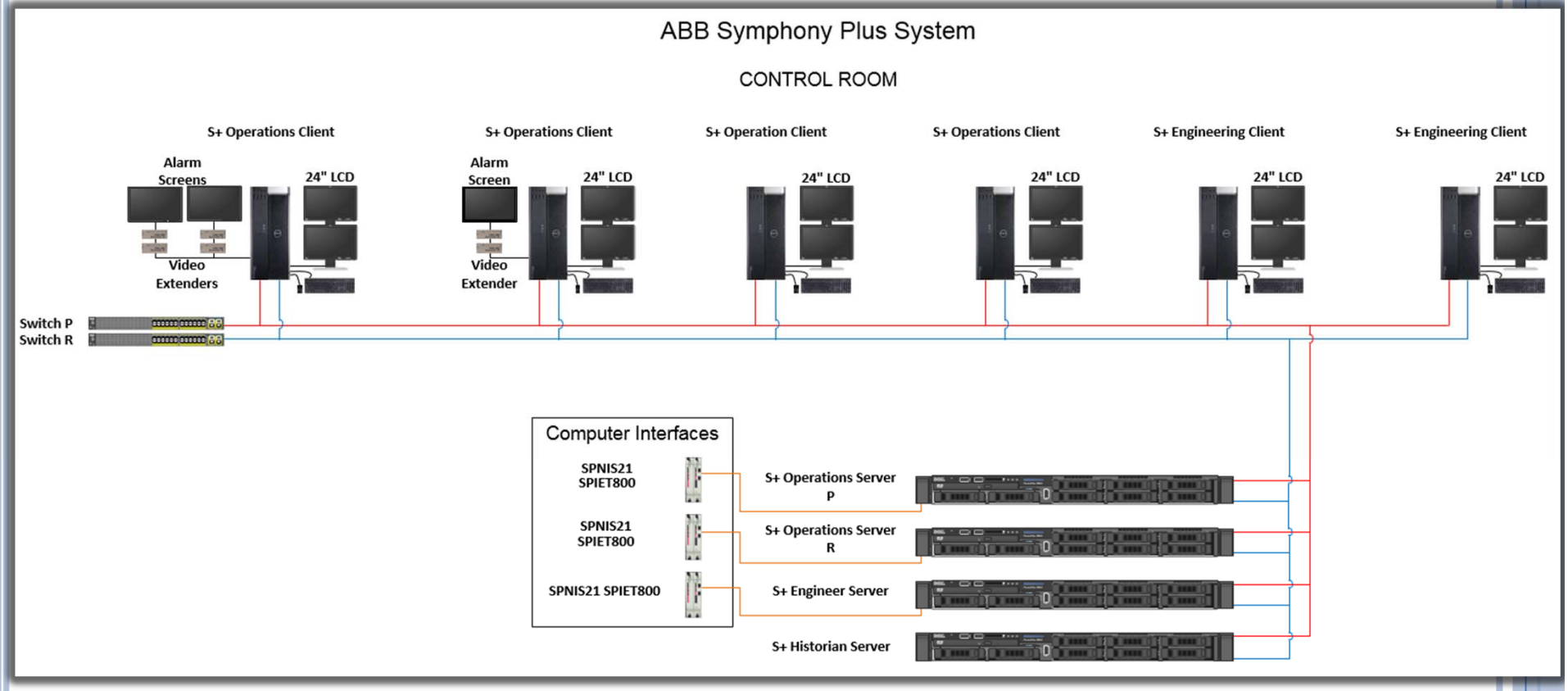
Segmentation Concept

- Generation aggregate of 1500MW or more
- Multiple units with shared cyber assets
- Segment to eliminate any shared cyber assets that could impact 1500MW or more
- May not be ideal at some facilities
- Needs to address Operations Level assets and Control Level assets

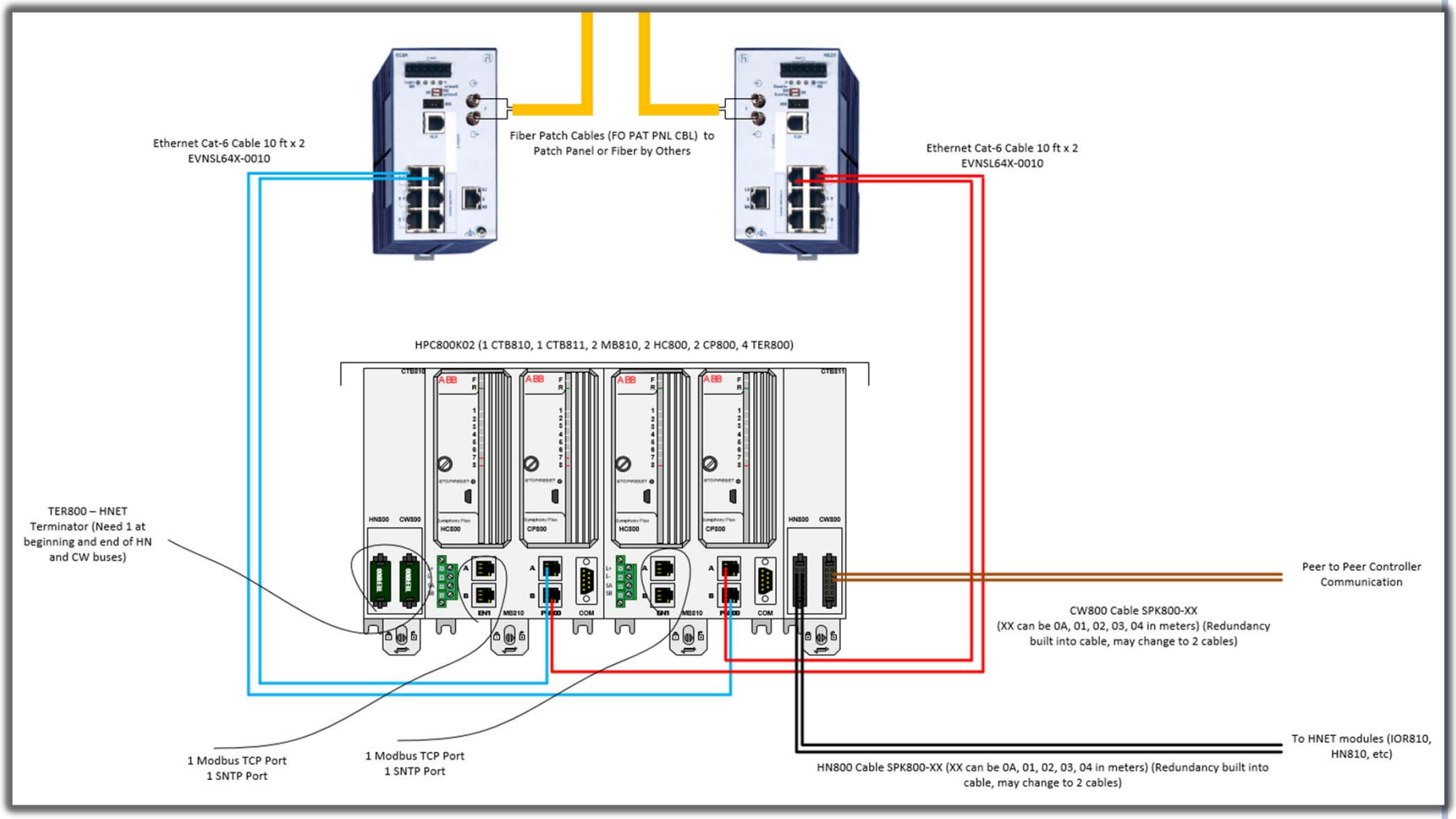
DATA


160
140
120
100
80
60
40
20
0
10
112
43
155
Standards
Requirement
Sub
Total Parts
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

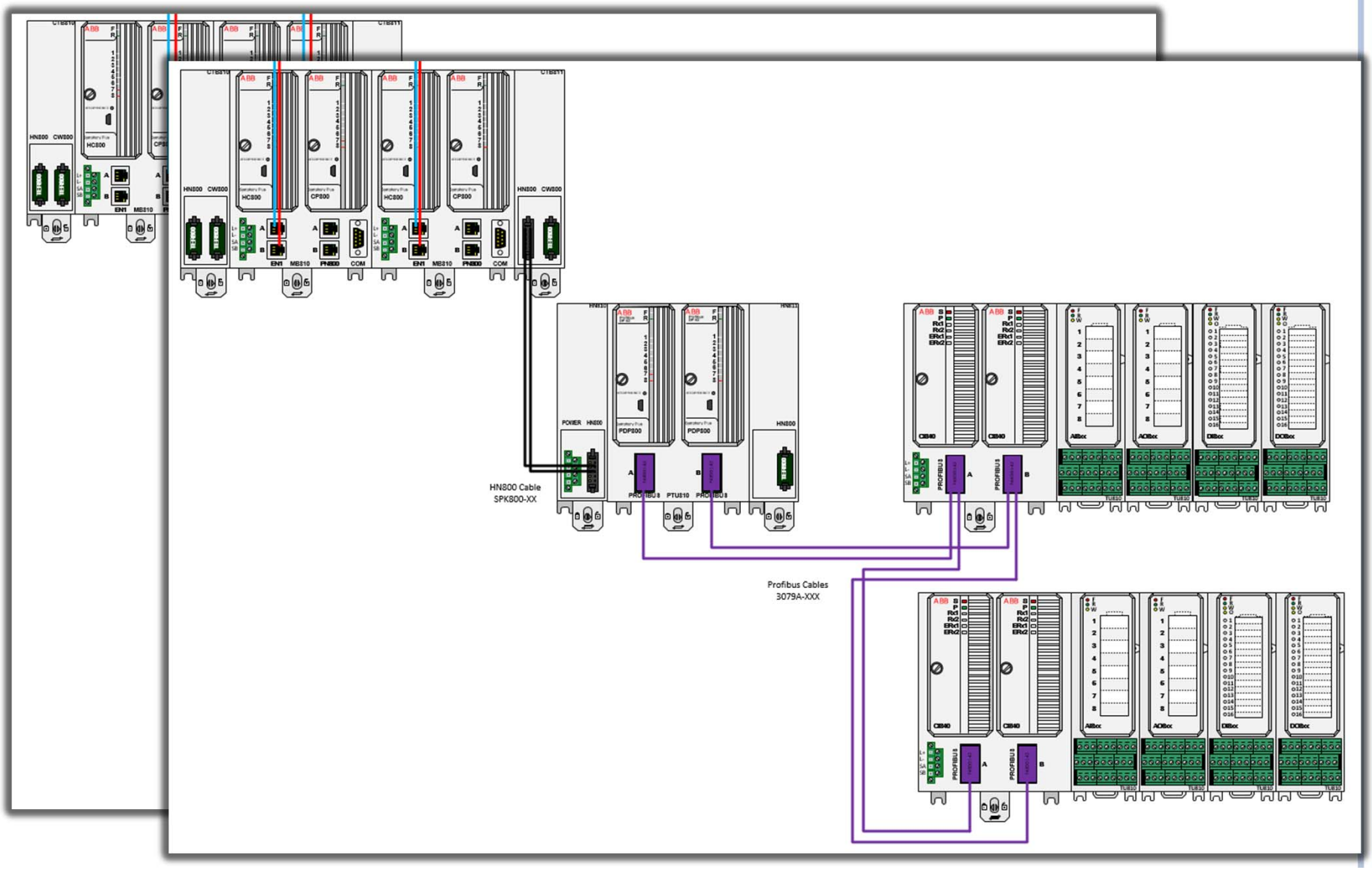
Operations Segments



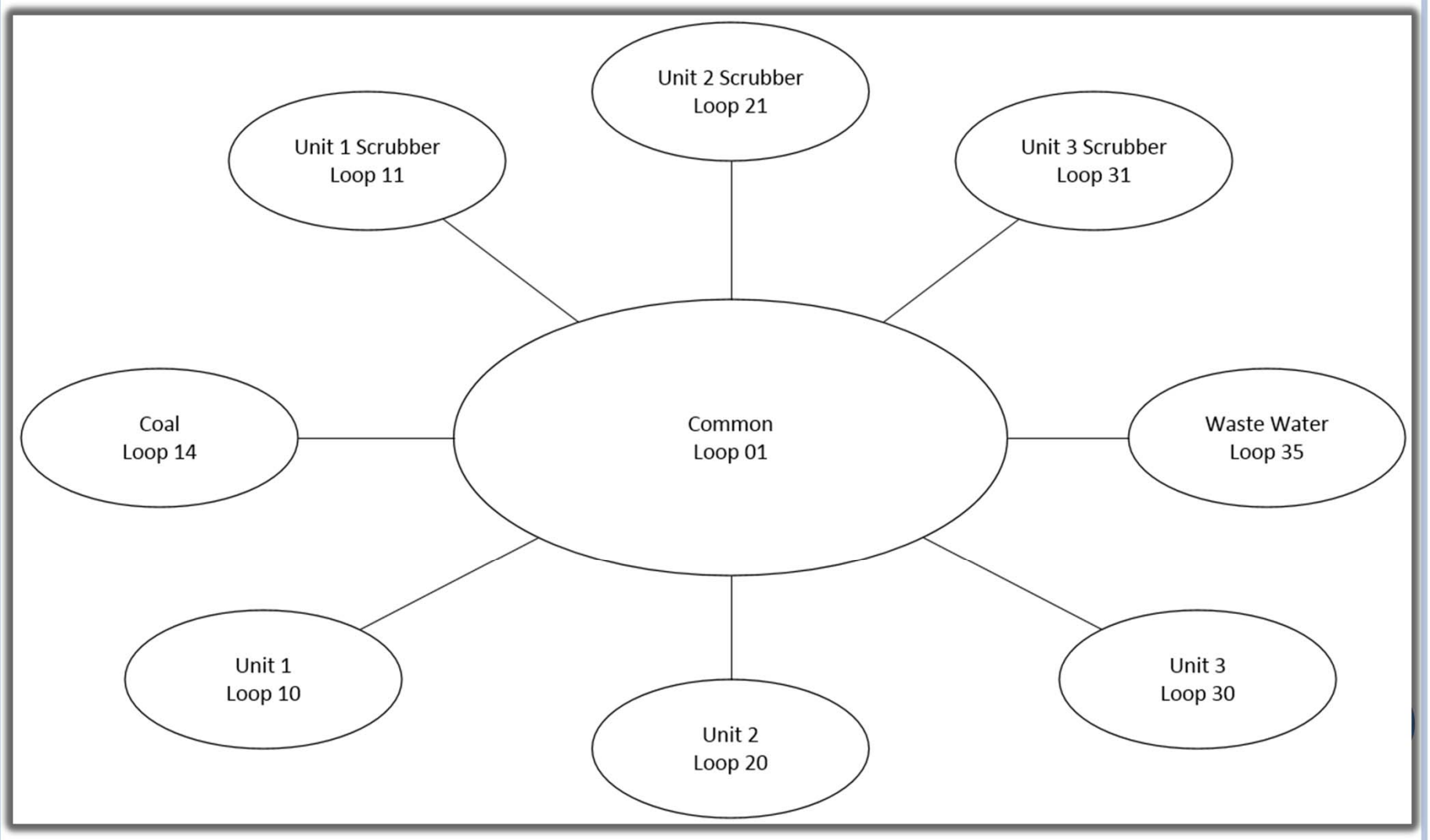
CONTROLLER LEVEL



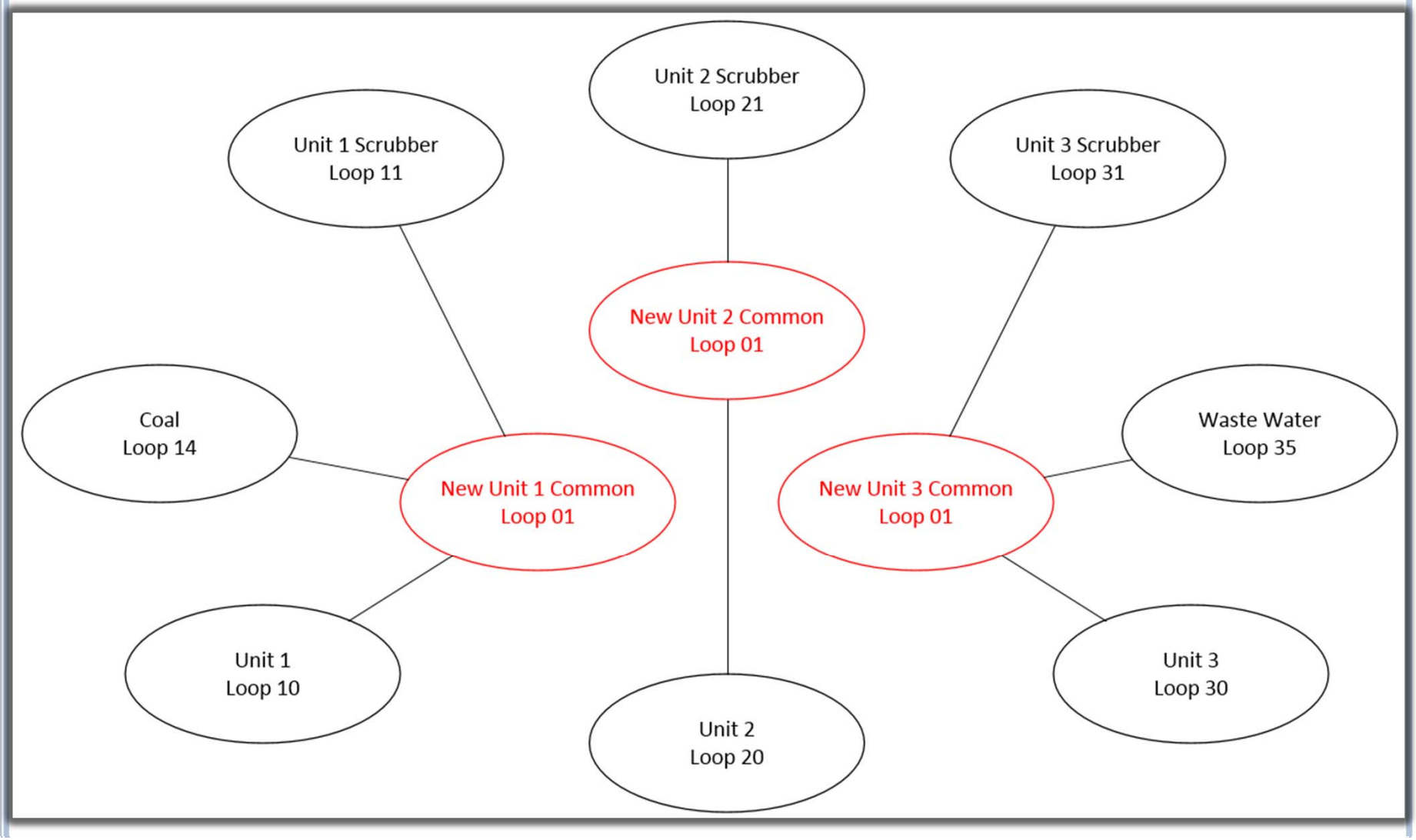
I/O Level



SHARED LOOP


Unit 2 Scrubber
Loop 21
Unit 1 Scrubber
Loop 11
Unit 3 Scrubber
Loop 31
Coal
Loop 14
Common
Loop 01
Waste Water
Loop 35
Unit 1
Loop 10
Unit 2
Loop 20
Unit 3
Loop 30

Segmented Loop



COMPLETE?

- Segmentation complete
  - All analysis performed
  - Operational and leadership review to ensure no negative impact on safety, or reliability
  - New configuration tested
  - Outage scheduled
  - New design implemented
  - Up and running in new segmented architecture

- No worries until April 1, 2017….. Right?

Are you audit ready?

What if your audit was April 4, 2016

- Nothing but Lows on April 1, 2016
  - CIP-002-5.1
  - Attachment 1 Criteria 2.1 and 2.2
  - CIP-003-5 or 6
- Process Review
- Sample High, Medium, and Low
- Review adequacy of Low determinations

What if your audit was April 4, 2016

- Low determination by April 1, 2016

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts ~~1.1 through 1.3~~: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

i. Control Centers and backup Control Centers;
ii. Transmission stations and substations;
iii. Generation resources;
iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and
vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

What if your audit was April 4, 2016

- Low determination by April 1, 2016

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

What if your audit was April 4, 2016

- Low determination by April 1, 2016

R2. The Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

What if your audit was April 4, 2016

- Low determination by April 1, 2016

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Now Start at the End (The RSAW)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-002-5.1 — Cyber Security — BES Cyber System Categorization

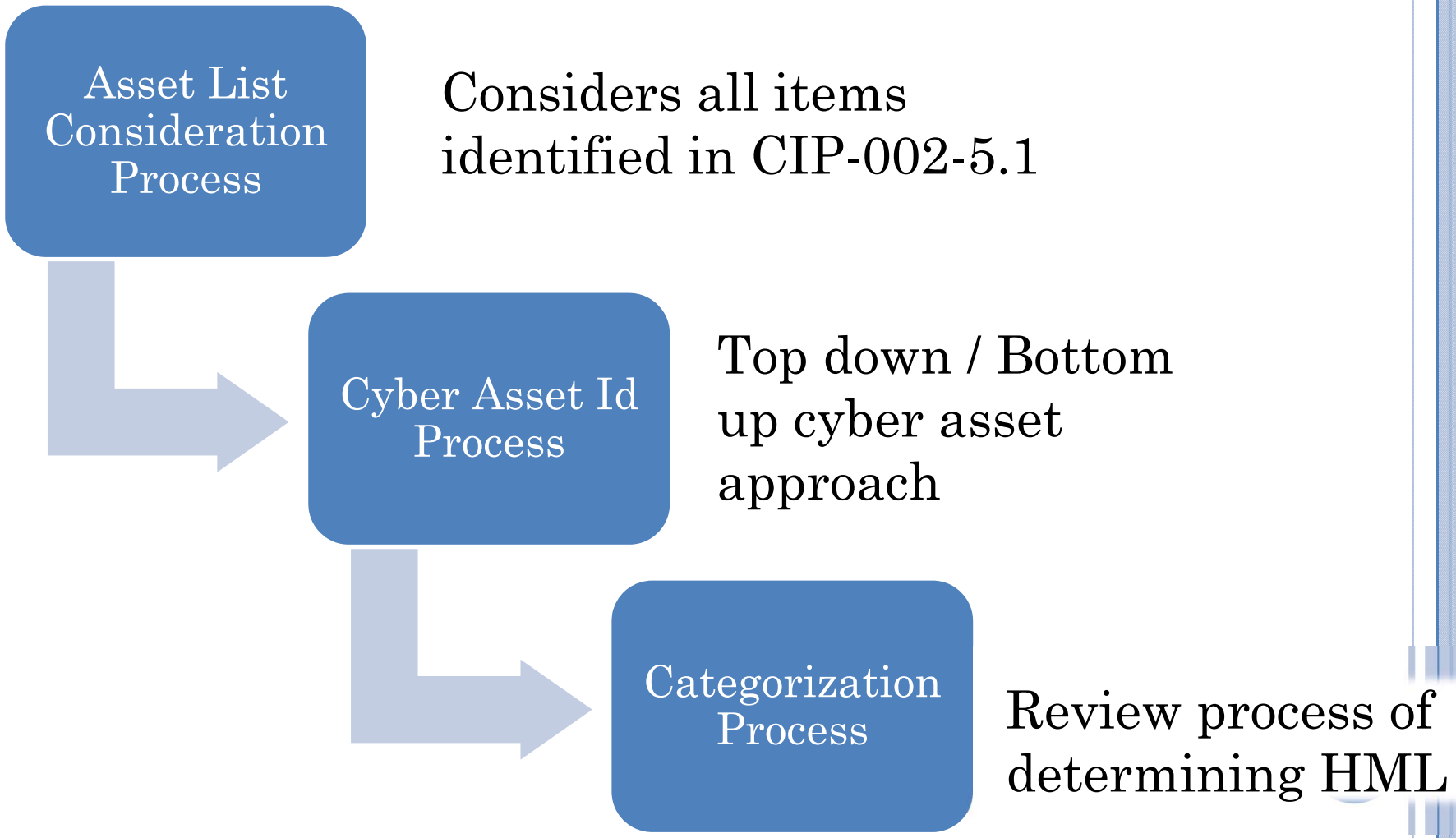
This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	X	X	X	X				X			X	X		
R2	X	X	X	X	X				X			X	X		

Process Reviews



Data Request

- Provide the process implemented that considers R1 i through vi
- List of all assets considered including:
  - Identification (name, number, etc.) of the asset.
  - The type of asset (generation resource, substation, etc.).
  - An indication if there is a low impact BES Cyber System at the asset.

Asset Identification	Asset Type	Shared Asset	High Impact BES Cyber System	Medium Impact BES Cyber System	Low Impact BES Cyber System	Date of Commissioning	Date of De-commissioning
Big Gen 1	Generation Resource	No	No	No	Yes	1994	NA
Peaker Plant 2	Generation Resource	No	No	No	Yes	1980	NA
Super Sub 3	Transmission Substation	No	No	No	Yes	2000	NA
Little Sub 4			No	No	Yes	2003	NA

Control Center
Backup Control Center
Transmission Station
Transmission Substation
Generation Resource
System Restoration Facility
Special Protection System
UFLS

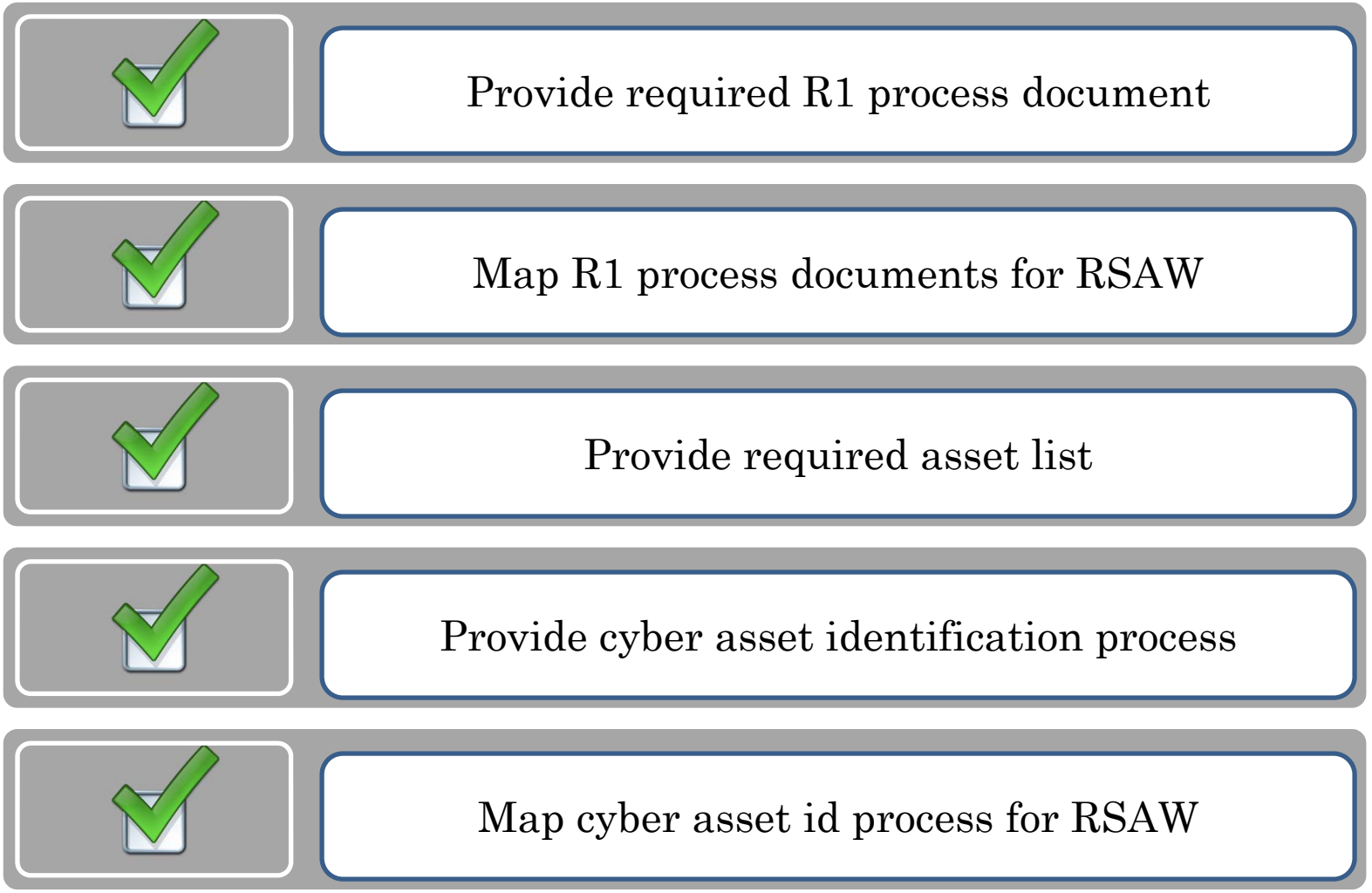
Auditor Tasks

- List Sampling
- For the sample of assets, provide:
  - Evidence that the process required by R1 was implemented to determine the list of assets containing low impact BES Cyber Systems
- Verify
  - Process considers R1 i through vi
  - Ensures all assets of each type are considered
  - Process identifies and assigns correct HML
  - CIP Senior Manager or delegate approval of HML identified BES Cyber Systems

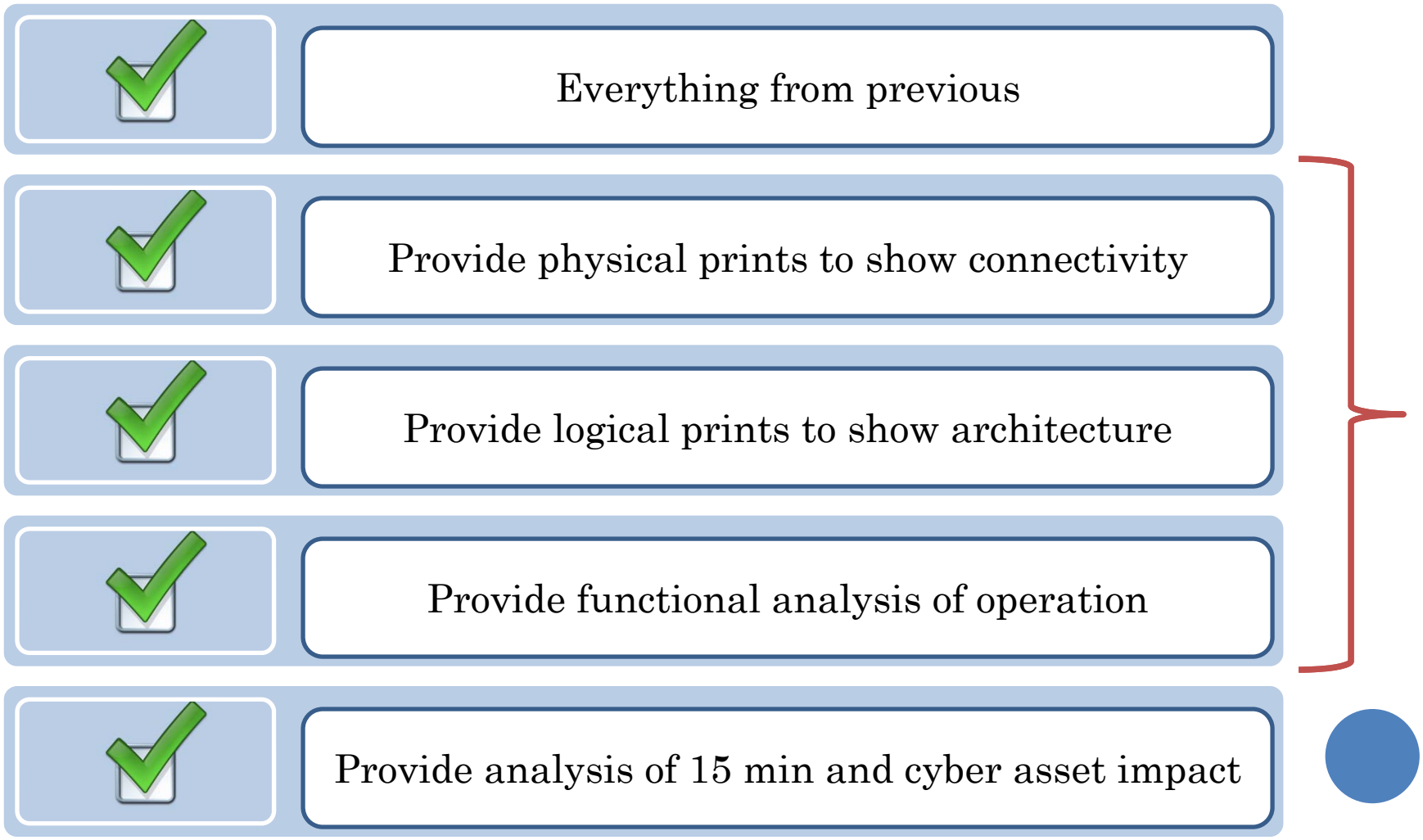
How much evidence do you need?

Tell, Show, and Prove

TRUST US APPROACH



TRUST AND VERIFY APPROACH

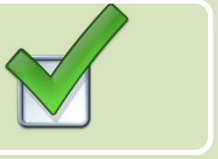


VERIFIED AND DEMONSTRATED APPROACH

Everything from previous two

Network infrastructure artifacts reflecting connectivity (switch level)

Perimeter and host artifacts reflecting logical connectivity (Firewall and traffic level)

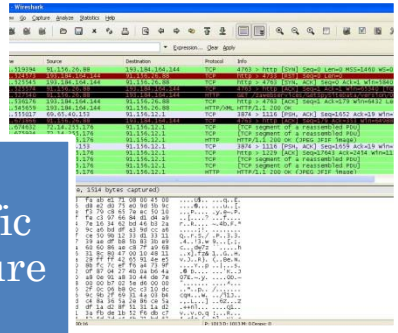


Control system artifacts of system operation (Tag, database, and display level)

Embedded device artifacts of performance (unavailability, degradation, and misuse)

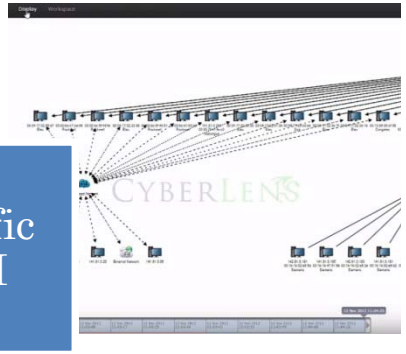
Tools for Proving a Negative

Traffic Capture

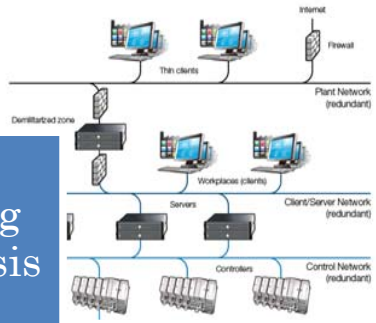


Traffic Anomaly

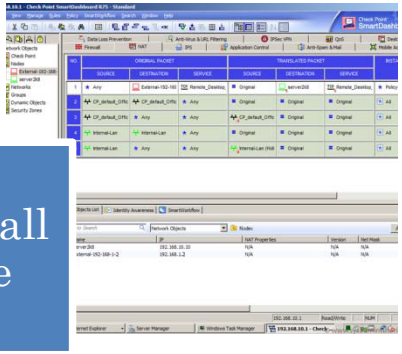
Traffic DPI



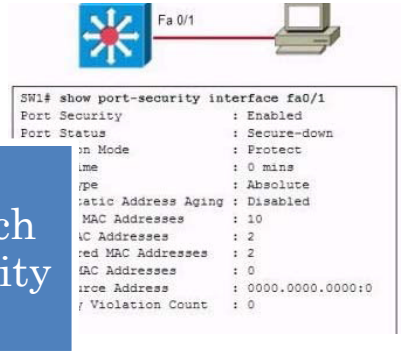
Config Analysis



Firewall Rule



Switch Security



Presentation Matters

Tell

- RSAW Narrative response

Show

- Provide process documents and map to RSAW
- Provide prints that represent a condition

Prove

- Provide configuration data and captured artifacts that demonstrate a condition exists

Provide your evidence in a manner that is clear, do not try to drown the auditor with data and hope they determine you have no violations – **prove you have no violations!**


QUESTIONS