STANDARDS COMMITTEE

MIDWEST RELIABILITY ORGANIZATION

Standard Application Guide for CIP-002-5.1

MRO CIP Subject Matter Expert Team

MRO CIP V5 Workshop
February 11 and 17, 2015

Promoting RELIABILITY and Mitigating RISKS to the Bulk Power System

MRO CIP Subject Matter Expert Team Members

Sharon Koller, Chair
American Transmission Company

Ron Bender
Nebraska Public Power District

Jesse Consolatti
Alliant Energy

Marc Child, Vice Chair
Great River Energy

Marie Knox
MISO

Bruce MacKenzie
Saskatchewan Power

The MRO Standards Committee is an industry stakeholder committee which includes subject matter experts from MRO member organizations in various technical areas. Any materials, guidance, and views from stakeholder committees are meant to be helpful to industry participants; but should not be considered approved or endorsed by MRO staff or its board of directors unless specified.

MRO Standards Committee Members

Robert Thompson, Chair
Xcel Energy

Wayne Guttormson
Saskatchewan Power, Vice Chair

David Rudolph
Basin Electric Power Cooperative

Mark Buchholz
Western Area Power Administration

George Brown
Acciona Energy

Todd Komplin
WPPI Energy

Joe Knight
Great River Energy

Michael Moltane
ITC Holdings

Andrew Pusztai
American Transmission Company

Lori Frisk
Minnesota Power

The MRO Standards Committee is an industry stakeholder committee which includes subject matter experts from MRO member organizations in various technical areas. Any materials, guidance, and views from stakeholder committees are meant to be helpful to industry participants; but should not be considered approved or endorsed by MRO staff or its board of directors unless specified.

Background

- **April 2013: MRO Standards Committee (MRO SC) approved a request for a Standard Application Guide (SAG) for NERC Reliability Standard CIP-002-5.1**

- **September 2013-December 2014: The CIP Subject Matter Expert Team (SMET) developed the CIP-002-5.1 SAG**
  - Underwent a cycle of technical reviews by NERC, MRO Risk Assessment and Mitigation, and MRO SC

- **December 2014: The CIP-002-5.1 SAG approved by the MRO SC, presented to the MRO Board of Directors and published**

Purpose:

- **This presentation is intended to provide guidance to Registered Entities on how to use the SAG and companion documents**

- **In this presentation you will learn about the process to:**
  - Apply the Attachment 1 Criteria to categorize BES Assets and BES Facilities
  - Evaluate Cyber Assets to determine impact rating of BES Cyber Systems
  - Examples, important considerations, and varied approaches/interpretations that may affect the approach a given entity chooses
  - How the companion documents can help

Focus: Preparing the industry for change

- **CIP-002-5.1 Cyber Security – BES Cyber System Categorization Standards**
  - Bulk Electric System (BES) Assets and Facilities

CIP Version 3		CIP Version 5
Risk-based Assessment Methodology	→	Application of Impact Rating Criteria
Critical Assets	→	High, Medium, or Low BES Facilities & Assets

  - BES Cyber Assets and Systems

CIP Version 3		CIP Version 5
Critical Cyber Assets	→	Impact-Rating BES Cyber Systems

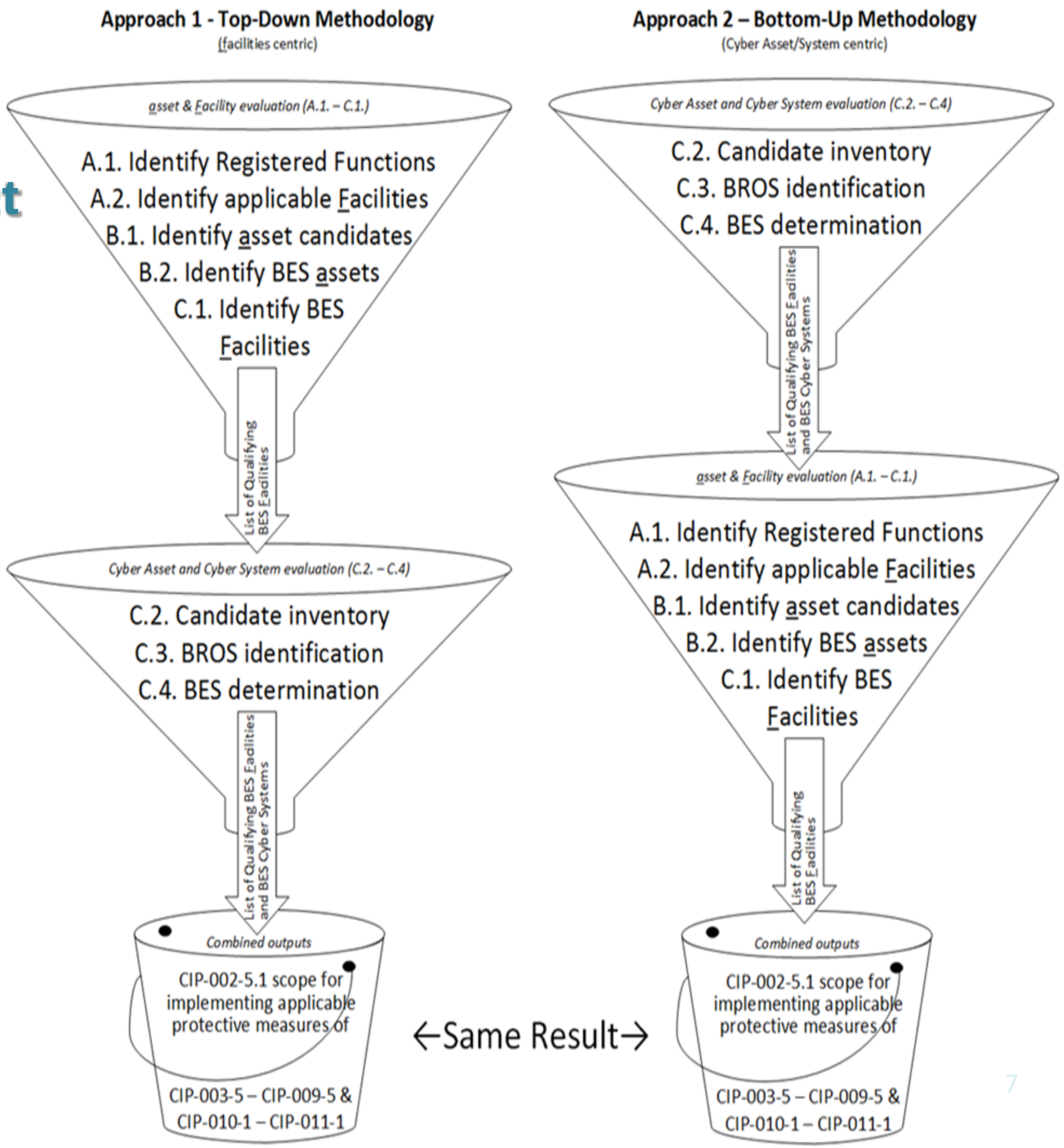
GOAL:

Take the mystery out of a complex subject

- **Two approaches (flexibility)**
  1. Facility centric (recommended)
  2. Cyber Asset/System centric

- **Filters and buckets (simplicity)**

Applicable BES Assets
Qualifying BES Facilities
+ BES Cyber Assets & Systems
= CIP-002-5.1 Scope



Approach 1 - Top-Down Methodology
(facilities centric)

asset & Facility evaluation (A.1. – C.1.)

A.1. Identify Registered Functions
A.2. Identify applicable Facilities
B.1. Identify asset candidates
B.2. Identify BES assets
C.1. Identify BES Facilities

List of Qualifying BES Facilities

Cyber Asset and Cyber System evaluation (C.2. – C.4)

C.2. Candidate inventory
C.3. BROS identification
C.4. BES determination

List of Qualifying BES Facilities and BES Cyber Systems

Combined outputs

CIP-002-5.1 scope for implementing applicable protective measures of CIP-003-5 – CIP-009-5 & CIP-010-1 – CIP-011-1

←Same Result→

Approach 2 – Bottom-Up Methodology
(Cyber Asset/System centric)

Cyber Asset and Cyber System evaluation (C.2. – C.4)

C.2. Candidate inventory
C.3. BROS identification
C.4. BES determination

List of Qualifying BES Facilities and BES Cyber Systems

asset & Facility evaluation (A.1. – C.1.)

A.1. Identify Registered Functions
A.2. Identify applicable Facilities
B.1. Identify asset candidates
B.2. Identify BES assets
C.1. Identify BES Facilities

List of Qualifying BES Facilities

Combined outputs

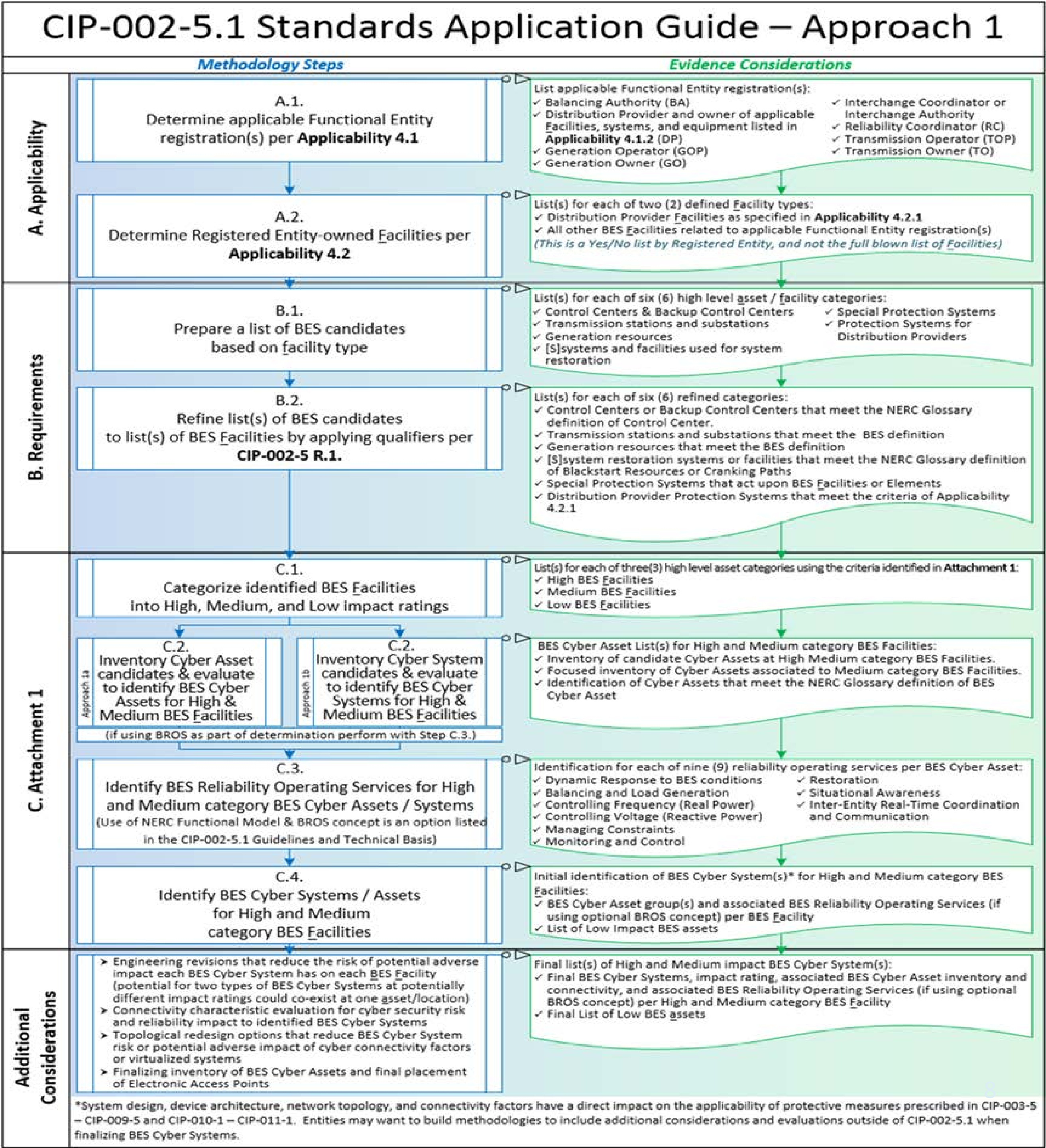
CIP-002-5.1 scope for implementing applicable protective measures of CIP-003-5 – CIP-009-5 & CIP-010-1 – CIP-011-1

Approach 1:

- **Provide Step-by-Step Instruction**
  - Methodology (doing it)
  - Evidence (proving it)

- **Break it down visually: Usability**
  - A. Applicability
  - B. Requirements
  - C. Attachment 1
  - D. Additional Considerations

- **Support with narratives, tips, and examples**



CIP-002-5.1 Standards Application Guide – Approach 1

Methodology Steps | *Evidence Considerations*

A. Applicability

A.1. Determine applicable Functional Entity registration(s) per **Applicability 4.1**

List applicable Functional Entity registration(s):
- ✓ Balancing Authority (BA)
- ✓ Distribution Provider and owner of applicable Facilities, systems, and equipment listed in **Applicability 4.1.2** (DP)
- ✓ Generation Operator (GOP)
- ✓ Generation Owner (GO)
- ✓ Interchange Coordinator or Interchange Authority
- ✓ Reliability Coordinator (RC)
- ✓ Transmission Operator (TOP)
- ✓ Transmission Owner (TO)

A.2. Determine Registered Entity-owned Facilities per **Applicability 4.2**

List(s) for each of two (2) defined Facility types:
- ✓ Distribution Provider Facilities as specified in **Applicability 4.2.1**
- ✓ All other BES Facilities related to applicable Functional Entity registration(s)

(This is a Yes/No list by Registered Entity, and not the full blown list of Facilities)

B. Requirements

B.1. Prepare a list of BES candidates based on facility type

List(s) for each of six (6) high level asset / facility categories:
- ✓ Control Centers & Backup Control Centers
- ✓ Transmission stations and substations
- ✓ Generation resources
- ✓ [S]systems and facilities used for system restoration
- ✓ Special Protection Systems
- ✓ Protection Systems for Distribution Providers

B.2. Refine list(s) of BES candidates to list(s) of BES Facilities by applying qualifiers per **CIP-002-5 R.1.**

List(s) for each of six (6) refined categories:
- ✓ Control Centers or Backup Control Centers that meet the NERC Glossary definition of Control Center.
- ✓ Transmission stations and substations that meet the BES definition
- ✓ Generation resources that meet the BES definition
- ✓ [S]system restoration systems or facilities that meet the NERC Glossary definition of Blackstart Resources or Cranking Paths
- ✓ Special Protection Systems that act upon BES Facilities or Elements
- ✓ Distribution Provider Protection Systems that meet the criteria of Applicability 4.2.1

C. Attachment 1

C.1. Categorize identified BES Facilities into High, Medium, and Low impact ratings

List(s) for each of three(3) high level asset categories using the criteria identified in **Attachment 1**:
- ✓ High BES Facilities
- ✓ Medium BES Facilities
- ✓ Low BES Facilities

Approach 1a — C.2. Inventory Cyber Asset candidates & evaluate to identify BES Cyber Assets for High & Medium BES Facilities

Approach 1b — C.2. Inventory Cyber System candidates & evaluate to identify BES Cyber Systems for High & Medium BES Facilities

(if using BROS as part of determination perform with Step C.3.)

BES Cyber Asset List(s) for High and Medium category BES Facilities:
- ✓ Inventory of candidate Cyber Assets at High Medium category BES Facilities.
- ✓ Focused inventory of Cyber Assets associated to Medium category BES Facilities.
- ✓ Identification of Cyber Assets that meet the NERC Glossary definition of BES Cyber Asset

C.3. Identify BES Reliability Operating Services for High and Medium category BES Cyber Assets / Systems (Use of NERC Functional Model & BROS concept is an option listed in the CIP-002-5.1 Guidelines and Technical Basis)

Identification for each of nine (9) reliability operating services per BES Cyber Asset:
- ✓ Dynamic Response to BES conditions
- ✓ Balancing and Load Generation
- ✓ Controlling Frequency (Real Power)
- ✓ Controlling Voltage (Reactive Power)
- ✓ Managing Constraints
- ✓ Monitoring and Control
- ✓ Restoration
- ✓ Situational Awareness
- ✓ Inter-Entity Real-Time Coordination and Communication

C.4. Identify BES Cyber Systems / Assets for High and Medium category BES Facilities

Initial identification of BES Cyber System(s)* for High and Medium category BES Facilities:
- ✓ BES Cyber Asset group(s) and associated BES Reliability Operating Services (if using optional BROS concept) per BES Facility
- ✓ List of Low Impact BES assets

Additional Considerations

- ➢ Engineering revisions that reduce the risk of potential adverse impact each BES Cyber System has on each BES Facility (potential for two types of BES Cyber Systems at potentially different impact ratings could co-exist at one asset/location)
- ➢ Connectivity characteristic evaluation for cyber security risk and reliability impact to identified BES Cyber Systems
- ➢ Topological redesign options that reduce BES Cyber System risk or potential adverse impact of cyber connectivity factors or virtualized systems
- ➢ Finalizing inventory of BES Cyber Assets and final placement of Electronic Access Points

Final list(s) of High and Medium impact BES Cyber System(s):
- ✓ Final BES Cyber Systems, impact rating, associated BES Cyber Asset inventory and connectivity, and associated BES Reliability Operating Services (if using optional BROS concept) per High and Medium category BES Facility
- ✓ Final List of Low BES assets

*System design, device architecture, network topology, and connectivity factors have a direct impact on the applicability of protective measures prescribed in CIP-003-5 – CIP-009-5 and CIP-010-1 – CIP-011-1. Entities may want to build methodologies to include additional considerations and evaluations outside of CIP-002-5.1 when finalizing BES Cyber Systems.

SMET Goal = Comprehensive content

- **Explain use of defined terms vs. SMET terms or interpretations**
- **Requirements / Attachment 1 Analysis and Interpretation**
  - Interpretations on “associated”
- **Narrative to guide through details of steps A, B and C**
- **Visual aids to support the narrative**

SMET Goal = Comprehensive content (continued)

- **Tips, Notes, and Evidence considerations throughout**
  - Guidance on the gray areas
  - Concept of BES Reliability Operating Services (BROS)
  - Consideration of the 15-minute impact parameter
  - High-watermarking concept
  - Joint-owner scenarios, communications, and other considerations
  - Impact of operating agreements / contracts
  - Real-world examples to support the guidance
- **Companion documents**

“Associated”

- **Two interpretations**
  - Requirement R1.2 says “at”
  - Attachment 1 Section 2, Medium impact says “Associated with”
- **Interpretation 1**
  - Cyber Assets/Systems must be both at and associated with the BES Facilities
- **Interpretation 2**
  - Cyber Assets/Systems must be at and/or associated with the BES Facilities
  - Cyber Assets/Systems at in addition to those associated with the BES Facilities
  - Cyber Assets/Systems at plus those associated with the BES Facilities
- **Both are viable; however, interpretation 2 is more conservative and covers some unique situations**

The MRO Standards Committee is an industry stakeholder committee which includes subject matter experts from MRO member organizations in various technical areas. Any materials, guidance, and views from stakeholder committees are meant to be helpful to industry participants; but should not be considered approved or endorsed by MRO staff or its board of directors unless specified.

15-minute impact parameter

- **Considerations for determining Adverse Impact**
  - Cyber Asset being unavailable, degraded, or misused
  - BES Facility experiencing loss, compromise, or misoperation as a result

1. Choose not to use it, and apply protections independent of the 15-minute parameter
2. Consider those functions that are automated that could avoid Adverse Impact
3. "…Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact."
4. GOs must consider 15 minute impact in Attachment 1 Criterion 2.1 (1500 MW) regardless

It is a scoping factor, if Registered Entities use it, be prepared

Its All Connected

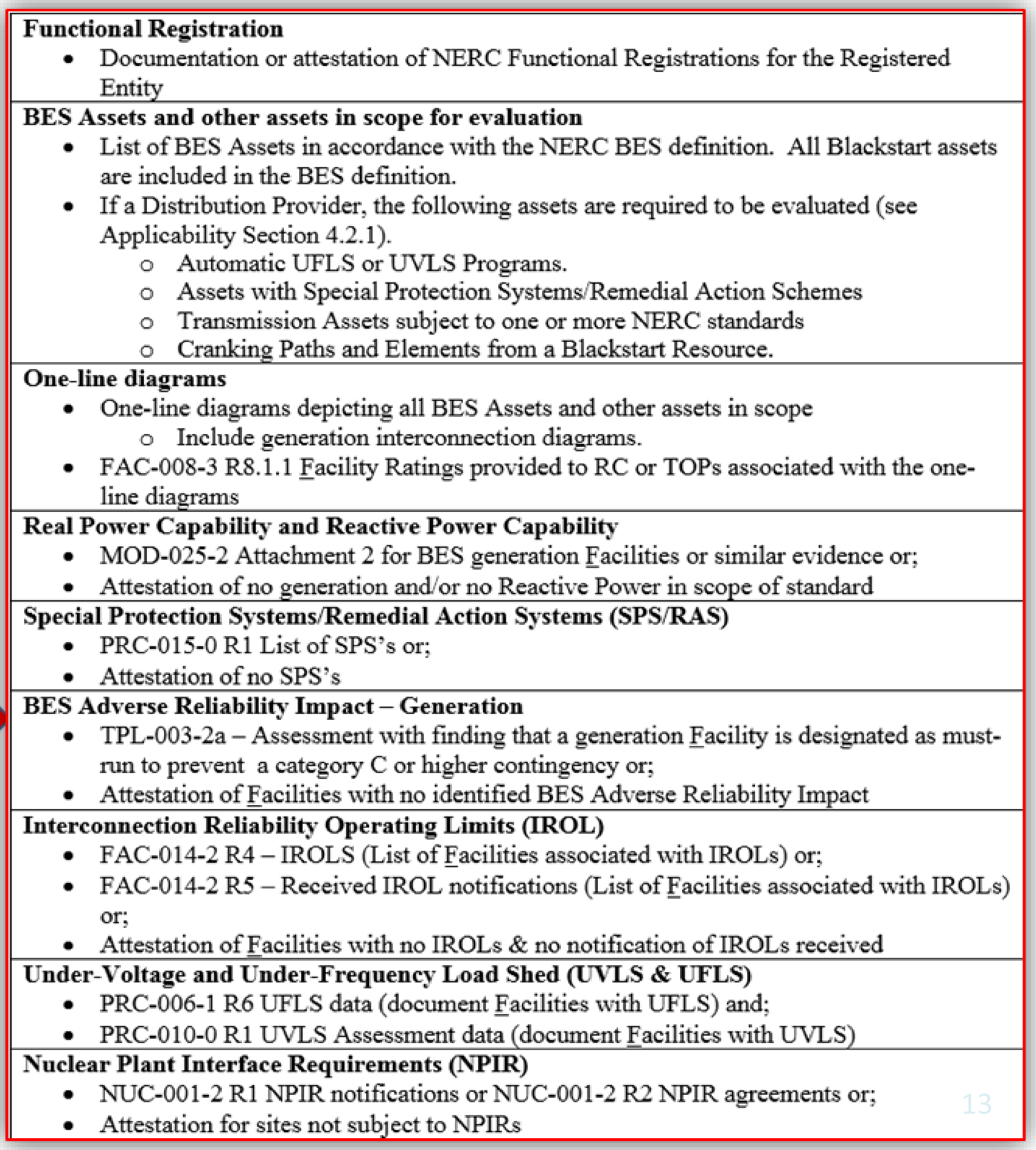
Requirements and Impact Rating Analysis

- Unpacked the Standard, Requirement by Requirement
- Provided detail for each of the Individual Impact Rating Criterion

Efficiencies:

- Leveraging existing data as process inputs
- Identifying dependencies between criterion and how the order of application can save time. Start with Medium Impact!

Input from other Reliability Standards



Functional Registration

- Documentation or attestation of NERC Functional Registrations for the Registered Entity

BES Assets and other assets in scope for evaluation

- List of BES Assets in accordance with the NERC BES definition. All Blackstart assets are included in the BES definition.
- If a Distribution Provider, the following assets are required to be evaluated (see Applicability Section 4.2.1).
  - Automatic UFLS or UVLS Programs.
  - Assets with Special Protection Systems/Remedial Action Schemes
  - Transmission Assets subject to one or more NERC standards
  - Cranking Paths and Elements from a Blackstart Resource.

One-line diagrams

- One-line diagrams depicting all BES Assets and other assets in scope
  - Include generation interconnection diagrams.
- FAC-008-3 R8.1.1 Facility Ratings provided to RC or TOPs associated with the one-line diagrams

Real Power Capability and Reactive Power Capability

- MOD-025-2 Attachment 2 for BES generation Facilities or similar evidence or;
- Attestation of no generation and/or no Reactive Power in scope of standard

Special Protection Systems/Remedial Action Systems (SPS/RAS)

- PRC-015-0 R1 List of SPS's or;
- Attestation of no SPS's

BES Adverse Reliability Impact – Generation

- TPL-003-2a – Assessment with finding that a generation Facility is designated as must-run to prevent a category C or higher contingency or;
- Attestation of Facilities with no identified BES Adverse Reliability Impact

Interconnection Reliability Operating Limits (IROL)

- FAC-014-2 R4 – IROLS (List of Facilities associated with IROLs) or;
- FAC-014-2 R5 – Received IROL notifications (List of Facilities associated with IROLs) or;
- Attestation of Facilities with no IROLs & no notification of IROLs received

Under-Voltage and Under-Frequency Load Shed (UVLS & UFLS)

- PRC-006-1 R6 UFLS data (document Facilities with UFLS) and;
- PRC-010-0 R1 UVLS Assessment data (document Facilities with UVLS)

Nuclear Plant Interface Requirements (NPIR)

- NUC-001-2 R1 NPIR notifications or NUC-001-2 R2 NPIR agreements or;
- Attestation for sites not subject to NPIRs

Tools to Apply the Attachment 1 Criteria

- **Companion Worksheets to apply the methodology for:**
  - High Impact Rating Criteria
  - Medium Impact Rating Criteria
  - Low Impact Rating Criteria
- **Eight (8) Examples**
  - Generation at a single plant location
  - Generation Facility
  - Reactive Resources at a single Transmission location
  - Transmission Facilities at a single substation or station
  - Transmission Facilities
  - SPS, RAS, or automated switching systems
  - Automatic Load Shedding
  - Control Center

STANDARDS COMMITTEE

SAMPLE ASSESSMENT WORKSHEETS

Example 1: Generation at a single plant location

Form G-1

Generation at a Single Plant Location

Single Generation Plant Location

Analysis By:

Date:

BES Facility Consideration
Does the generation at this single plant location contain at least one BES generation asset?

Yes/No

Note 1: If no, then this Facility is does not apply to CIP-002-5

Unit ID	Net Real Power Capability (MW)	Critical to IROL Derivation (Yes/No)

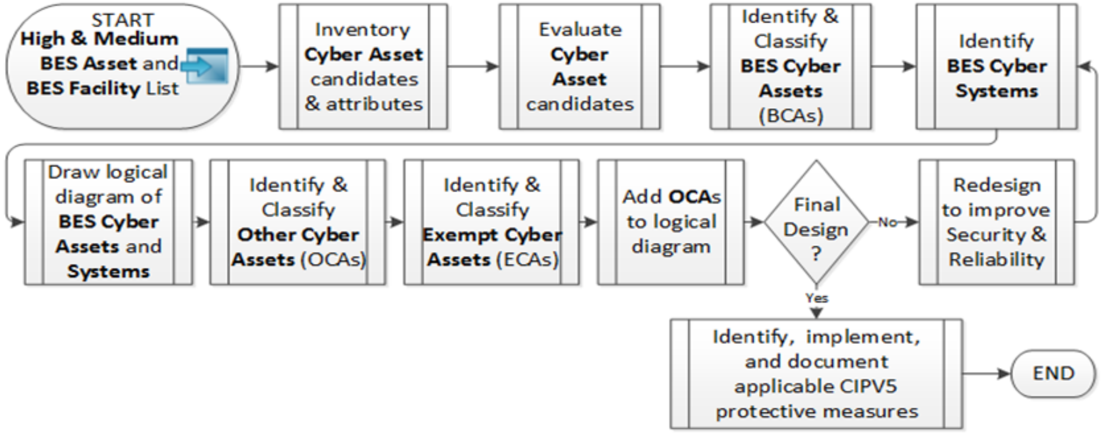
Aggregate Real Power Capability ______ MW

Aggregate Real Power Capability at Single Plant Location

Note 4: If yes, then identify the BES cyber assets that are associated with each generating unit in the single plant location.

Tools to Identify BES Cyber Assets/Systems

- **Sample Methodologies**
  - High-Level Methodology Diagrams
    - ✓ High and Medium Impact
    - ✓ Low Impact
  - Supporting Narratives and Rationale per step
  - Registered Entity definitions
  - Considerations for Inventorying Cyber Asset Candidates
    - ✓ Attribute data
    - ✓ Physical Inspections
    - ✓ Cyber Connectivity Reviews



START High & Medium BES Asset and BES Facility List

Inventory Cyber Asset candidates & attributes

Evaluate Cyber Asset candidates

Identify & Classify BES Cyber Assets (BCAs)

Identify BES Cyber Systems

Draw logical diagram of BES Cyber Assets and Systems

Identify & Classify Other Cyber Assets (OCAs)

Identify & Classify Exempt Cyber Assets (ECAs)

Add OCAs to logical diagram

Final Design ?

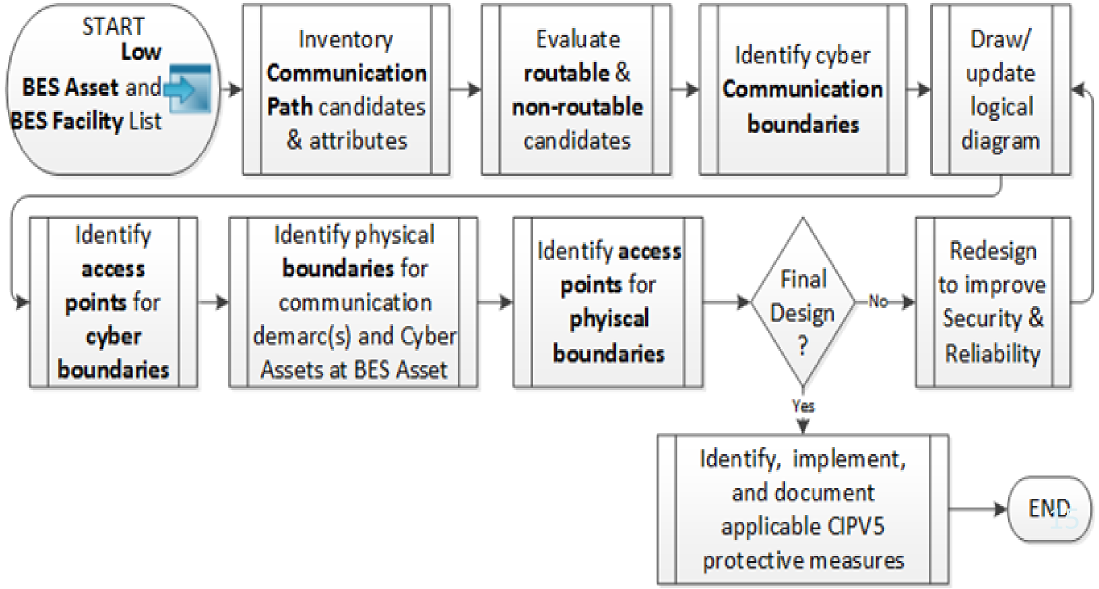
No

Redesign to improve Security & Reliability

Yes

Identify, implement, and document applicable CIPV5 protective measures

END



START Low BES Asset and BES Facility List

Inventory Communication Path candidates & attributes

Evaluate routable & non-routable candidates

Identify cyber Communication boundaries

Draw/ update logical diagram

Identify access points for cyber boundaries

Identify physical boundaries for communication demarc(s) and Cyber Assets at BES Asset

Identify access points for physical boundaries

Final Design ?

No

Redesign to improve Security & Reliability

Yes

Identify, implement, and document applicable CIPV5 protective measures

END

Tools to Identify BES Cyber Assets/Systems

Examples of Inventorying Approaches

- Attribute Tables
- Sample Criterion
- Physical Discovery Mechanisms
- Electronic Discovery Mechanisms

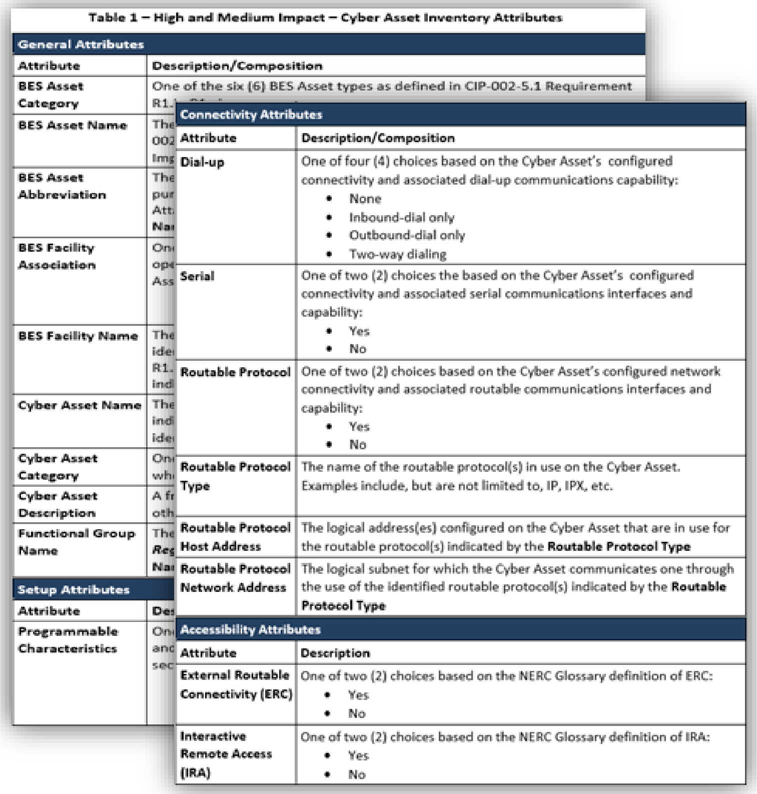


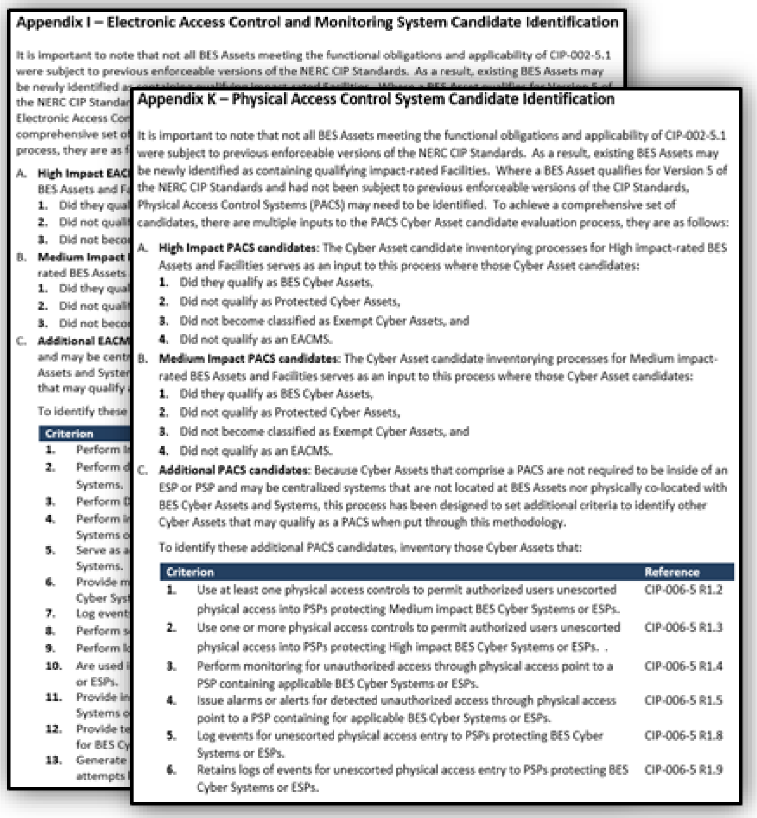
Table 1 – High and Medium Impact – Cyber Asset Inventory Attributes

General Attributes	
Attribute	Description/Composition
BES Asset Category	One of the six (6) BES Asset types as defined in CIP-002-5.1 Requirement R1.
BES Asset Name	The 002 Img
BES Asset Abbreviation	The pur Att Na
BES Facility Association	On ope Ass
BES Facility Name	The ide R1. ind
Cyber Asset Name	The ind ide
Cyber Asset Category	On wh
Cyber Asset Description	A fr oth
Functional Group Name	The *Reg* Na

Setup Attributes	
Attribute	De
Programmable Characteristics	On and sec

Connectivity Attributes	
Attribute	Description/Composition
Dial-up	One of four (4) choices based on the Cyber Asset's configured connectivity and associated dial-up communications capability: • None • Inbound-dial only • Outbound-dial only • Two-way dialing
Serial	One of two (2) choices the based on the Cyber Asset's configured connectivity and associated serial communications interfaces and capability: • Yes • No
Routable Protocol	One of two (2) choices based on the Cyber Asset's configured network connectivity and associated routable communications interfaces and capability: • Yes • No
Routable Protocol Type	The name of the routable protocol(s) in use on the Cyber Asset. Examples include, but are not limited to, IP, IPX, etc.
Routable Protocol Host Address	The logical address(es) configured on the Cyber Asset that are in use for the routable protocol(s) indicated by the **Routable Protocol Type**
Routable Protocol Network Address	The logical subnet for which the Cyber Asset communicates one through the use of the identified routable protocol(s) indicated by the **Routable Protocol Type**

Accessibility Attributes	
Attribute	Description
External Routable Connectivity (ERC)	One of two (2) choices based on the NERC Glossary definition of ERC: • Yes • No
Interactive Remote Access (IRA)	One of two (2) choices based on the NERC Glossary definition of IRA: • Yes • No



Appendix I – Electronic Access Control and Monitoring System Candidate Identification

It is important to note that not all BES Assets meeting the functional obligations and applicability of CIP-002-5.1
were subject to previous enforceable versions of the NERC CIP Standards. As a result, existing BES Assets may
be newly identified as
the NERC CIP Standar
Electronic Access Con
comprehensive set of
process, they are as f

A. **High Impact EAC**
BES Assets and Fa
1. Did they qual
2. Did not quali
3. Did not becor

B. **Medium Impact**
rated BES Assets
1. Did they qual
2. Did not quali
3. Did not becor

C. **Additional EACM**
and may be centr
Assets and Syster
that may qualify

To identify these

Criterion
1. Perform In
2. Perform d Systems.
3. Perform D
4. Perform in Systems o
5. Serve as a Systems.
6. Provide m Cyber Syst
7. Log event
8. Perform s
9. Perform lo
10. Are used i or ESPs.
11. Provide in Systems o
12. Provide te for BES Cy
13. Generate attempts

Appendix K – Physical Access Control System Candidate Identification

It is important to note that not all BES Assets meeting the functional obligations and applicability of CIP-002-5.1 were subject to previous enforceable versions of the NERC CIP Standards. As a result, existing BES Assets may be newly identified as containing qualifying impact-rated Facilities. Where a BES Asset qualifies for Version 5 of the NERC CIP Standards and had not been subject to previous enforceable versions of the CIP Standards, Physical Access Control Systems (PACS) may need to be identified. To achieve a comprehensive set of candidates, there are multiple inputs to the PACS Cyber Asset candidate evaluation process, they are as follows:

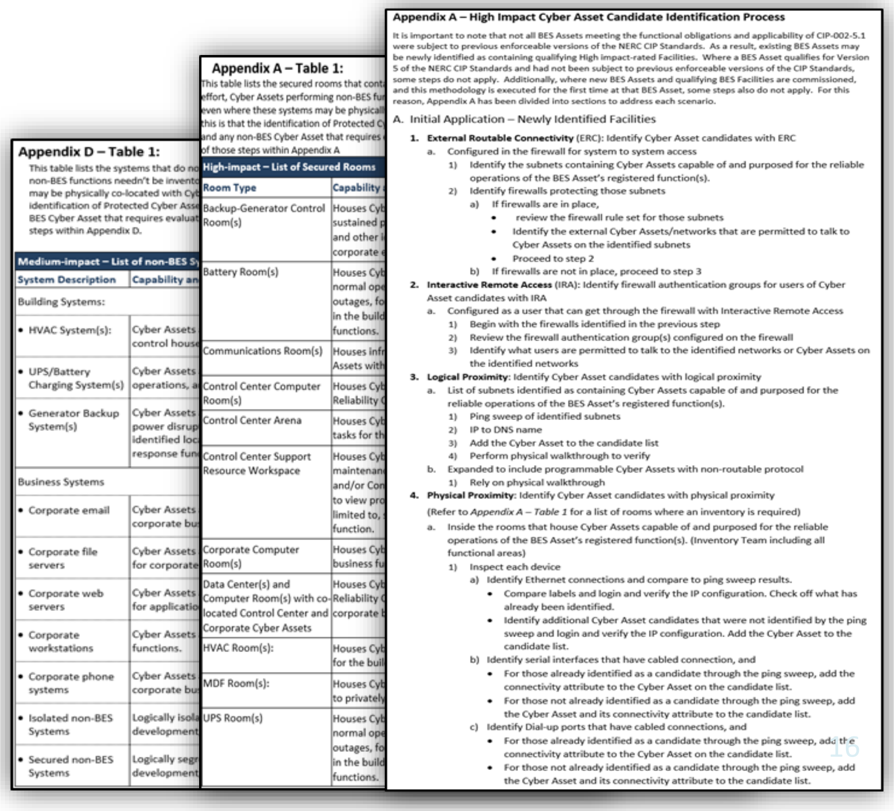
A. **High Impact PACS candidates:** The Cyber Asset candidate inventorying processes for High impact-rated BES Assets and Facilities serves as an input to this process where those Cyber Asset candidates:
1. Did they qualify as BES Cyber Assets,
2. Did not qualify as Protected Cyber Assets,
3. Did not become classified as Exempt Cyber Assets, and
4. Did not qualify as an EACMS.

B. **Medium Impact PACS candidates:** The Cyber Asset candidate inventorying processes for Medium impact-rated BES Assets and Facilities serves as an input to this process where those Cyber Asset candidates:
1. Did they qualify as BES Cyber Assets,
2. Did not qualify as Protected Cyber Assets,
3. Did not become classified as Exempt Cyber Assets, and
4. Did not qualify as an EACMS.

C. **Additional PACS candidates:** Because Cyber Assets that comprise a PACS are not required to be inside of an ESP or PSP and may be centralized systems that are not located at BES Assets nor physically co-located with BES Cyber Assets and Systems, this process has been designed to set additional criteria to identify other Cyber Assets that may qualify as a PACS when put through this methodology.

To identify these additional PACS candidates, inventory those Cyber Assets that:

Criterion	Reference
1. Use at least one physical access controls to permit authorized users unescorted physical access into PSPs protecting Medium impact BES Cyber Systems or ESPs.	CIP-006-5 R1.2
2. Use one or more physical access controls to permit authorized users unescorted physical access into PSPs protecting High impact BES Cyber Systems or ESPs. .	CIP-006-5 R1.3
3. Perform monitoring for unauthorized access through physical access point to a PSP containing applicable BES Cyber Systems or ESPs.	CIP-006-5 R1.4
4. Issue alarms or alerts for detected unauthorized access through physical access point to a PSP containing for applicable BES Cyber Systems or ESPs.	CIP-006-5 R1.5
5. Log events for unescorted physical access entry to PSPs protecting BES Cyber Systems or ESPs.	CIP-006-5 R1.8
6. Retains logs of events for unescorted physical access entry to PSPs protecting BES Cyber Systems or ESPs.	CIP-006-5 R1.9



Appendix D – Table 1:

This table lists the systems that do no
non-BES functions needn't be invento
may be physically co-located with Cyb
identification of Protected Cyber Asse
BES Cyber Asset that requires evaluat
steps within Appendix D.

Medium-impact – List of non-BES Sy	
System Description	Capability an
Building Systems:	
• HVAC System(s):	Cyber Assets control house
• UPS/Battery Charging System(s)	Cyber Assets operations, a
• Generator Backup System(s)	Cyber Assets power disrup identified loc response fun
Business Systems	
• Corporate email	Cyber Assets corporate bu
• Corporate file servers	Cyber Assets for corporate
• Corporate web servers	Cyber Assets for applicatio
• Corporate workstations	Cyber Assets functions.
• Corporate phone systems	Cyber Assets corporate bu
• Isolated non-BES Systems	Logically isola development
• Secured non-BES Systems	Logically segr development

Appendix A – Table 1:

This table lists the secured rooms that conta
effort, Cyber Assets performing non-BES fun
even where these systems may be physicall
this is that the identification of Protected Cy
and any non-BES Cyber Asset that requires
of those steps within Appendix A

High-impact – List of Secured Rooms	
Room Type	Capability
Backup-Generator Control Room(s)	Houses Cyb sustained p and other i corporate e
Battery Room(s)	Houses Cyb normal ope outages, fo in the build functions.
Communications Room(s)	Houses Infr Assets with
Control Center Computer Room(s)	Houses Cyb Reliability C
Control Center Arena	Houses Cyb tasks for th
Control Center Support Resource Workspace	Houses Cyb maintenanc and/or Con to view pro limited to, function.
Corporate Computer Room(s)	Houses Cyb business fu
Data Center(s) and Computer Room(s) with co-located Control Center and Corporate Cyber Assets	Houses Cyb Reliability C corporate b
HVAC Room(s):	Houses Cyb for the buil
MDF Room(s):	Houses Cyb to privately
UPS Room(s)	Houses Cyb normal ope outages, fo in the build functions.

Appendix A – High Impact Cyber Asset Candidate Identification Process

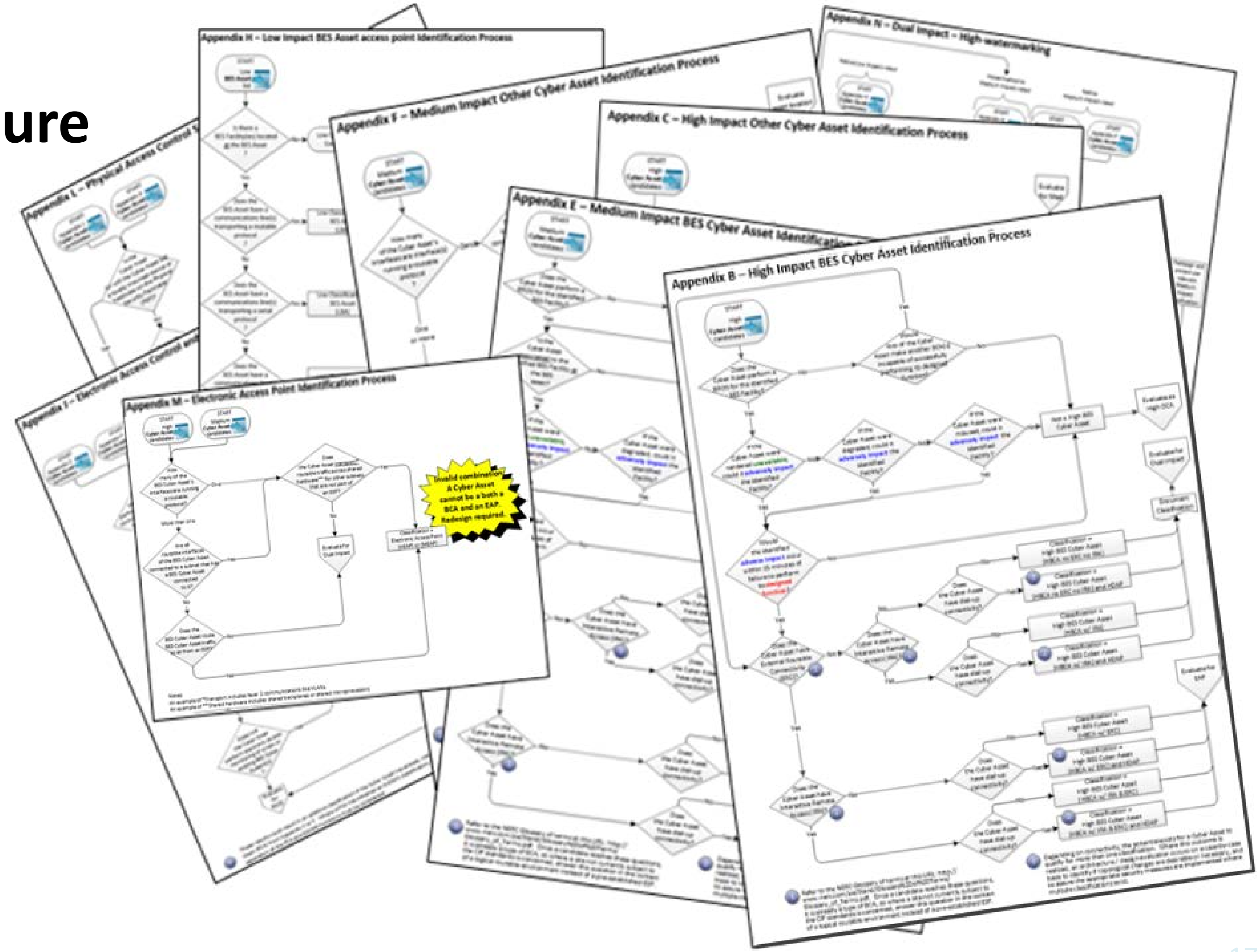
It is important to note that not all BES Assets meeting the functional obligations and applicability of CIP-002-5.1 were subject to previous enforceable versions of the NERC CIP Standards. As a result, existing BES Assets may be newly identified as containing qualifying High impact-rated Facilities. Where a BES Asset qualifies for Version 5 of the NERC CIP Standards and had not been subject to previous enforceable versions of the CIP Standards, some steps do not apply. Additionally, where new BES Assets and qualifying BES Facilities are commissioned, and this methodology is executed for the first time at that BES Asset, some steps also do not apply. For this reason, Appendix A has been divided into sections to address each scenario.

A. Initial Application – Newly Identified Facilities

1. **External Routable Connectivity** (ERC): Identify Cyber Asset candidates with ERC
   a. Configured in the firewall for system to system access
      1) Identify the subnets containing Cyber Assets capable of and purposed for the reliable operations of the BES Asset's registered function(s).
      2) Identify firewalls protecting those subnets
         a) If firewalls are in place,
            - review the firewall rule set for those subnets
            - Identify the external Cyber Assets/networks that are permitted to talk to Cyber Assets on the identified subnets
            - Proceed to step 2
         b) If firewalls are not in place, proceed to step 3
2. **Interactive Remote Access** (IRA): Identify firewall authentication groups for users of Cyber Asset candidates with IRA
   a. Configured as a user that can get through the firewall with Interactive Remote Access
      1) Begin with the firewalls identified in the previous step
      2) Review the firewall authentication group(s) configured on the firewall
      3) Identify what users are permitted to talk to the identified networks or Cyber Assets on the identified networks
3. **Logical Proximity**: Identify Cyber Asset candidates with logical proximity
   a. List of subnets identified as containing Cyber Assets capable of and purposed for the reliable operations of the BES Asset's registered function(s).
      1) Ping sweep of identified subnets
      2) IP to DNS name
      3) Add the Cyber Asset to the candidate list
      4) Perform physical walkthrough to verify
   b. Expanded to include programmable Cyber Assets with non-routable protocol
      1) Rely on physical walkthrough
4. **Physical Proximity**: Identify Cyber Asset candidates with physical proximity
   (Refer to *Appendix A – Table 1* for a list of rooms where an inventory is required)
   a. Inside the rooms that house Cyber Assets capable of and purposed for the reliable operations of the BES Asset's registered function(s). (Inventory Team including all functional areas)
      1) Inspect each device
         a) Identify Ethernet connections and compare to ping sweep results.
            - Compare labels and login and verify the IP configuration. Check off what has already been identified.
            - Identify additional Cyber Asset candidates that were not identified by the ping sweep and login and verify the IP configuration. Add the Cyber Asset to the candidate list.
         b) Identify serial interfaces that have cabled connection, and
            - For those already identified as a candidate through the ping sweep, add the connectivity attribute to the Cyber Asset on the candidate list.
            - For those not already identified as a candidate through the ping sweep, add the Cyber Asset and its connectivity attribute to the candidate list.
         c) Identify Dial-up ports that have cabled connections, and
            - For those already identified as a candidate through the ping sweep, add the connectivity attribute to the Cyber Asset on the candidate list.
            - For those not already identified as a candidate through the ping sweep, add the Cyber Asset and its connectivity attribute to the candidate list.

Tools to Identifying BES Cyber Assets/Systems

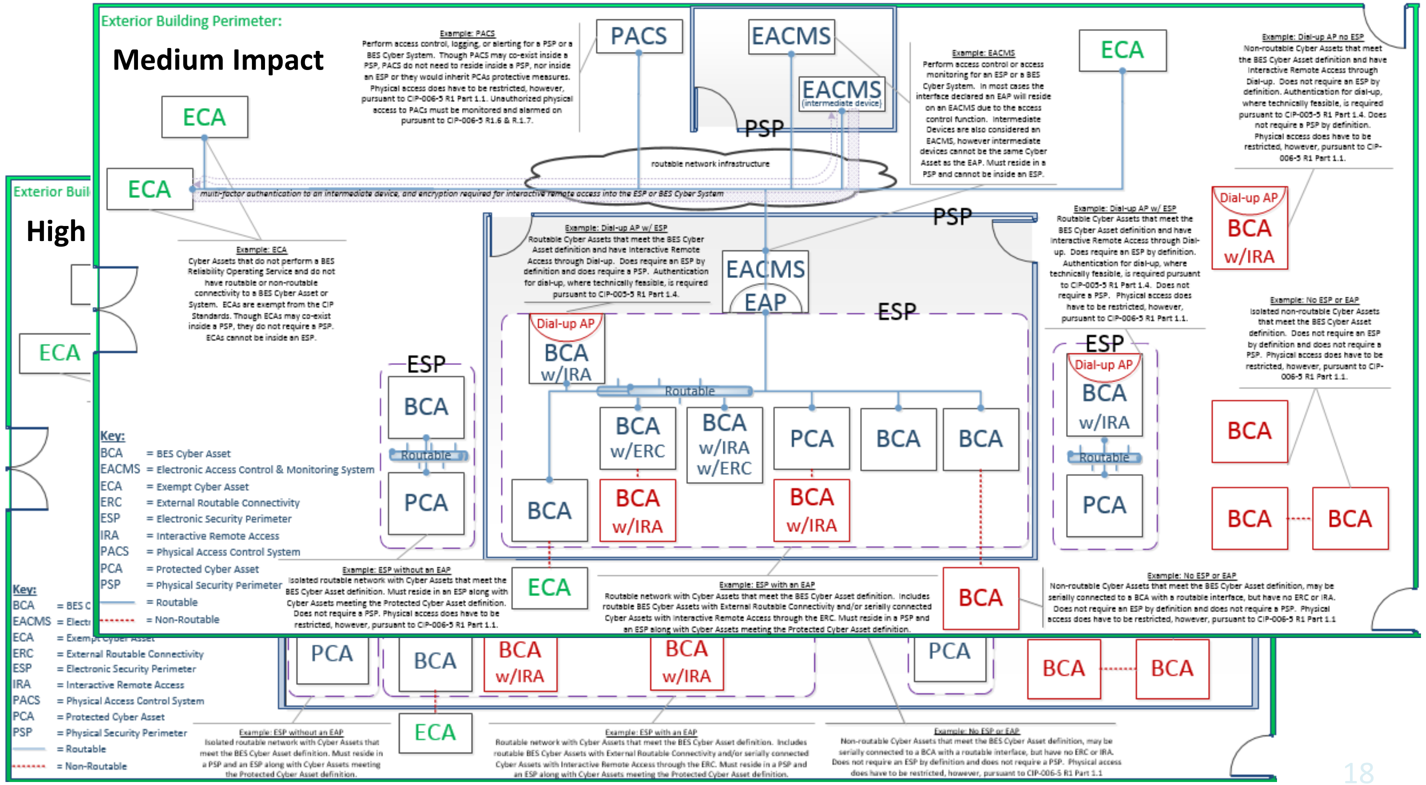
- **Sample Standard Operating Procedure**
  - Step-by-Step Instruction to:
    - ✓ Identify Cyber Asset Candidates
    - ✓ Evaluate Cyber Asset Candidates
    - ✓ Classify BES Cyber Assets
    - ✓ Determine BES Cyber Systems
  - Detailed process flow diagrams
    - ✓ Objective criteria
    - ✓ Includes other protected Cyber Assets


Appendix H – Low Impact BES Asset access point Identification Process
Appendix F – Medium Impact Other Cyber Asset Identification Process
Appendix N – Dual Impact – High-watermarking
Appendix C – High Impact Other Cyber Asset Identification Process
Appendix L – Physical Access Control
Appendix E – Medium Impact BES Cyber Asset Identification
Appendix B – High Impact BES Cyber Asset Identification Process
Appendix J – Electronic Access Control
Appendix M – Electronic Access Point Identification Process
Invalid combination. A Cyber Asset cannot be a both a BCA and an EAP. Redesign required.

Tools for CIP-005-5 & CIP-006-5 Considerations

- **Sample Connectivity Scenarios**
  - Various topologies, cyber configurations or redesign options
  - Other types of Protected Cyber Assets
  - Impact of connectivity on:
    - ✓ Applicability of Requirements
    - ✓ BES Cyber System determination
  - Electronic Security requirements
  - Physical Security requirements

How its all related…



Example: PACS
Perform access control, logging, or alerting for a PSP or a BES Cyber System. Though PACS may co-exist inside a PSP, PACS do not need to reside inside a PSP, nor inside an ESP or they would inherit PCAs protective measures. Physical access does have to be restricted, however, pursuant to CIP-006-5 R1 Part 1.1. Unauthorized physical access to PACs must be monitored and alarmed on pursuant to CIP-006-5 R1.6 & R.1.7.

Example: EACMS
Perform access control or access monitoring for an ESP or a BES Cyber System. In most cases the interface declared an EAP will reside on an EACMS due to the access control function. Intermediate Devices are also considered an EACMS, however intermediate devices cannot be the same Cyber Asset as the EAP. Must reside in a PSP and cannot be inside an ESP.

Example: Dial-up AP no ESP
Non-routable Cyber Assets that meet the BES Cyber Asset definition and have Interactive Remote Access through Dial-up. Does not require an ESP by definition. Authentication for dial-up, where technically feasible, is required pursuant to CIP-005-5 R1 Part 1.4. Does not require a PSP by definition. Physical access does have to be restricted, however, pursuant to CIP-006-5 R1 Part 1.1.

Example: ECA
Cyber Assets that do not perform a BES Reliability Operating Service and do not have routable or non-routable connectivity to a BES Cyber Asset or System. ECAs are exempt from the CIP Standards. Though ECAs may co-exist inside a PSP, they do not require a PSP. ECAs cannot be inside an ESP.

Example: Dial-up AP w/ ESP
Routable Cyber Assets that meet the BES Cyber Asset definition and have Interactive Remote Access through Dial-up. Does require an ESP by definition and does require a PSP. Authentication for dial-up, where technically feasible, is required pursuant to CIP-005-5 R1 Part 1.4.

Example: Dial-up AP w/ ESP
Routable Cyber Assets that meet the BES Cyber Asset definition and have Interactive Remote Access through Dial-up. Does require an ESP by definition. Authentication for dial-up, where technically feasible, is required pursuant to CIP-005-5 R1 Part 1.4. Does not require a PSP. Physical access does have to be restricted, however, pursuant to CIP-006-5 R1 Part 1.1.

Example: No ESP or EAP
Isolated non-routable Cyber Assets that meet the BES Cyber Asset definition. Does not require an ESP by definition and does not require a PSP. Physical access does have to be restricted, however, pursuant to CIP-006-5 R1 Part 1.1.

Key:

BCA	= BES Cyber Asset
EACMS	= Electronic Access Control & Monitoring System
ECA	= Exempt Cyber Asset
ERC	= External Routable Connectivity
ESP	= Electronic Security Perimeter
IRA	= Interactive Remote Access
PACS	= Physical Access Control System
PCA	= Protected Cyber Asset
PSP	= Physical Security Perimeter
───	= Routable
-------	= Non-Routable

Example: ESP without an EAP
Isolated routable network with Cyber Assets that meet the BES Cyber Asset definition. Must reside in an ESP along with Cyber Assets meeting the Protected Cyber Asset definition. Does not require a PSP. Physical access does have to be restricted, however, pursuant to CIP-006-5 R1 Part 1.1.

Example: ESP with an EAP
Routable network with Cyber Assets that meet the BES Cyber Asset definition. Includes routable BES Cyber Assets with External Routable Connectivity and/or serially connected Cyber Assets with Interactive Remote Access through the ERC. Must reside in a PSP and an ESP along with Cyber Assets meeting the Protected Cyber Asset definition.

Example: No ESP or EAP
Non-routable Cyber Assets that meet the BES Cyber Asset definition, may be serially connected to a BCA with a routable interface, but have no ERC or IRA. Does not require an ESP by definition and does not require a PSP. Physical access does have to be restricted, however, pursuant to CIP-006-5 R1 Part 1.1

Key:

BCA	= BES C
EACMS	= Electr
ECA	= Exempt Cyber Asset
ERC	= External Routable Connectivity
ESP	= Electronic Security Perimeter
IRA	= Interactive Remote Access
PACS	= Physical Access Control System
PCA	= Protected Cyber Asset
PSP	= Physical Security Perimeter
───	= Routable
-------	= Non-Routable

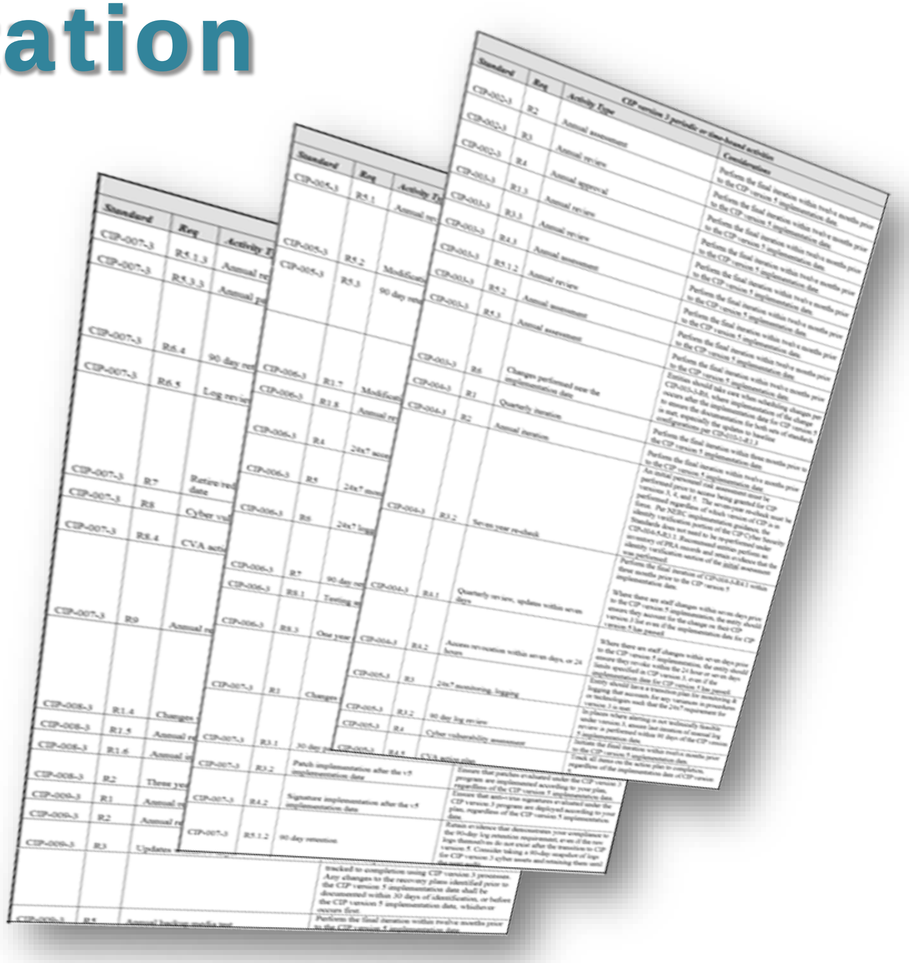
Example: ESP without an EAP
Isolated routable network with Cyber Assets that meet the BES Cyber Asset definition. Must reside in a PSP and an ESP along with Cyber Assets meeting the Protected Cyber Asset definition.

Example: ESP with an EAP
Routable network with Cyber Assets that meet the BES Cyber Asset definition. Includes routable BES Cyber Assets with External Routable Connectivity and/or serially connected Cyber Assets with Interactive Remote Access through the ERC. Must reside in a PSP and an ESP along with Cyber Assets meeting the Protected Cyber Asset definition.

Example: No ESP or EAP
Non-routable Cyber Assets that meet the BES Cyber Asset definition, may be serially connected to a BCA with a routable interface, but have no ERC or IRA. Does not require an ESP by definition and does not require a PSP. Physical access does have to be restricted, however, pursuant to CIP-006-5 R1 Part 1.1

Tools for V3 to V5 Implementation

- **Companion Guide:**
  - V5 effective dates
  - Entity specific considerations
    - ✓What each entity needs to ask themselves
    - ✓Next steps depending on the answer
  - Audit cycles
  - Evidence retention
  - Periodic or time-bound activities
    - ✓V3 Requirement by Requirement



Does it work? SMET tested it, three ways.

Why we tested our recommended approach:

- **Confidence in the product**
- **Measure the usability**
- **Reasonable assurance it will work for others**

How we tested our recommended approach:

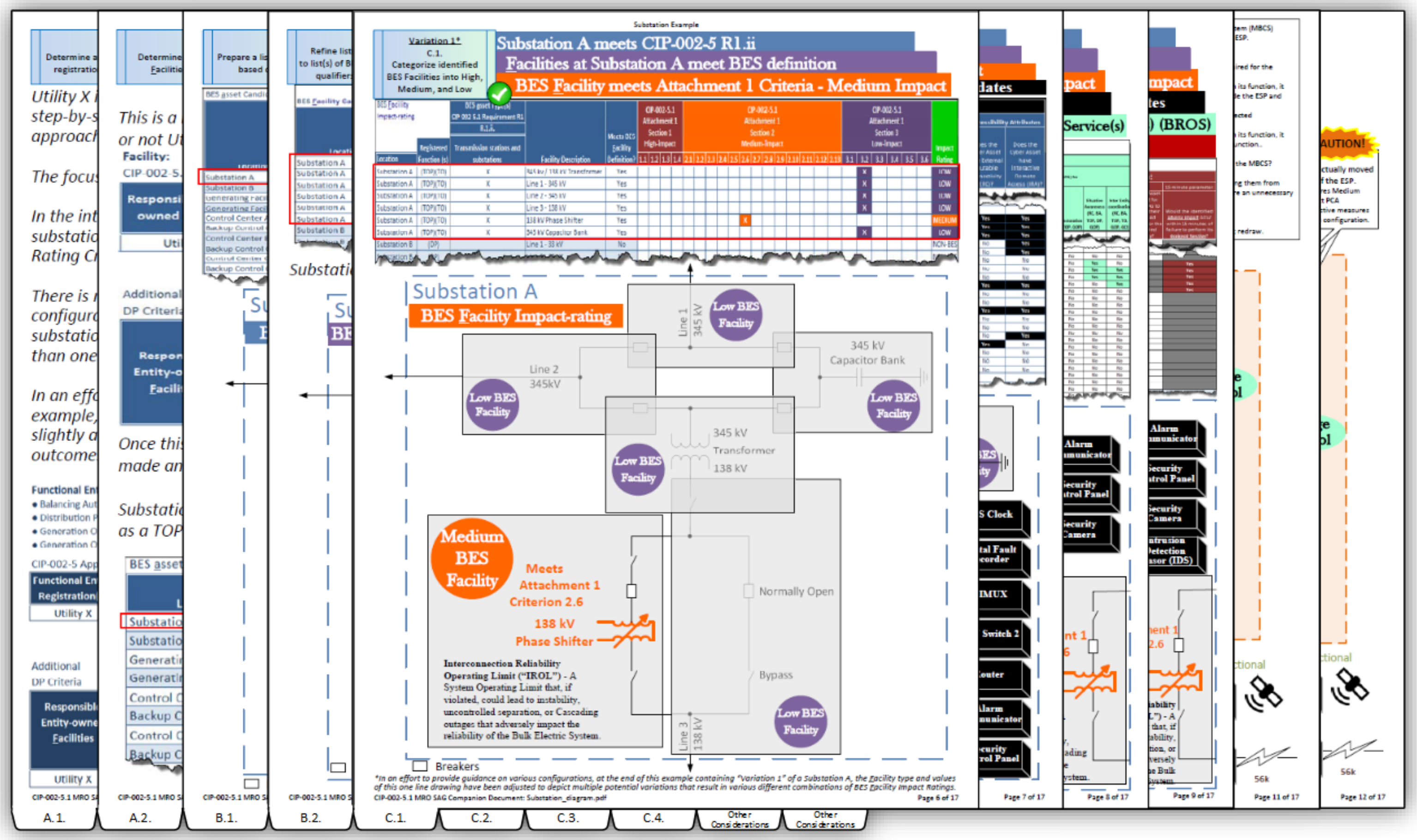
- **Applied the Step-by-Step Instruction**
  - Transmission Substation
  - Generating Station
  - Control Center

What we learned from testing/proving it out:

- **The methodology is**
  - Usable
  - Flexible
  - Straight forward
  - Repeatable
  - Adaptive
  - Comprehensive
  - Reaps results and evidence
- **Bonus – Companion Diagrams**
  - We have these various scenarios and examples to provide to the industry to accompany the CIP-002-5.1 SAG

Transmission Substation – Proof of Concept

- Approach 1.a
- Cyber Asset-based
- Electrical Focus
  - 1-line diagrams
- Five similar, yet different scenarios



Substation Example

Variation 1*
C.1.
Categorize identified BES Facilities into High, Medium, and Low

Substation A meets CIP-002-5 R1.ii

Facilities at Substation A meet BES definition

BES Facility meets Attachment 1 Criteria - Medium Impact

BES Facility Impact-rating

BES asset Type(s) CIP 002 5.1 Requirement R1 R.1.ii.

Location	Registered Function(s)	Transmission stations and substations	Facility Description	Meets BES Facility Definition?	CIP-002-5.1 Attachment 1 Section 1 High-Impact				CIP-002-5.1 Attachment 1 Section 2 Medium-Impact													CIP-002-5.1 Attachment 1 Section 3 Low-Impact						Impact Rating
					1.1	1.2	1.3	1.4	2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	2.11	2.12	2.13	3.1	3.2	3.3	3.4	3.5	3.6	
Substation A	(TOP)(TO)	X	345 kV / 138 kV Transformer	Yes																			X					LOW
Substation A	(TOP)(TO)	X	Line 1 - 345 kV	Yes																			X					LOW
Substation A	(TOP)(TO)	X	Line 2 - 345 kV	Yes																			X					LOW
Substation A	(TOP)(TO)	X	Line 3 - 138 kV	Yes																			X					LOW
Substation A	(TOP)(TO)	X	138 kV Phase Shifter	Yes										X														MEDIUM
Substation A	(TOP)(TO)	X	345 kV Capacitor Bank	Yes																			X					LOW
Substation B	(DP)		Line 1 - 33 kV	No																								NON-BES

Substation A

BES Facility Impact-rating

Interconnection Reliability Operating Limit ("IROL") - A System Operating Limit that, if violated, could lead to instability, uncontrolled separation, or Cascading outages that adversely impact the reliability of the Bulk Electric System.

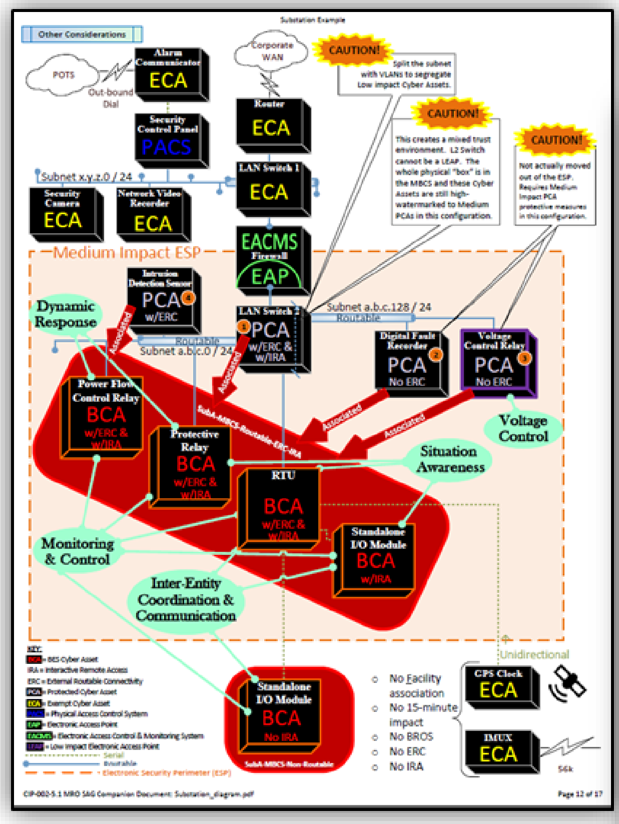
In an effort to provide guidance on various configurations, at the end of this example containing "Variation 1" of a Substation A, the Facility type and values of this one line drawing have been adjusted to depict multiple potential variations that result in various different combinations of BES Facility Impact Ratings.

CIP-002-5.1 MRO SAG Companion Document: Substation_diagram.pdf Page 6 of 17

Other Considerations

Mixed Trust vs. Segregated Trust Zones

- **High Watermarking**
  - Virtualization
    - ✓ Hypervisors
    - ✓ VLANs
    - ✓ Chassis/Shared Backplanes
  - Medium inside High ESP → High
  - Low inside High ESP → High
  - Low inside Medium ESP → Medium



CAUTION! Split the subnet with VLANs to segregate Low impact Cyber Assets.

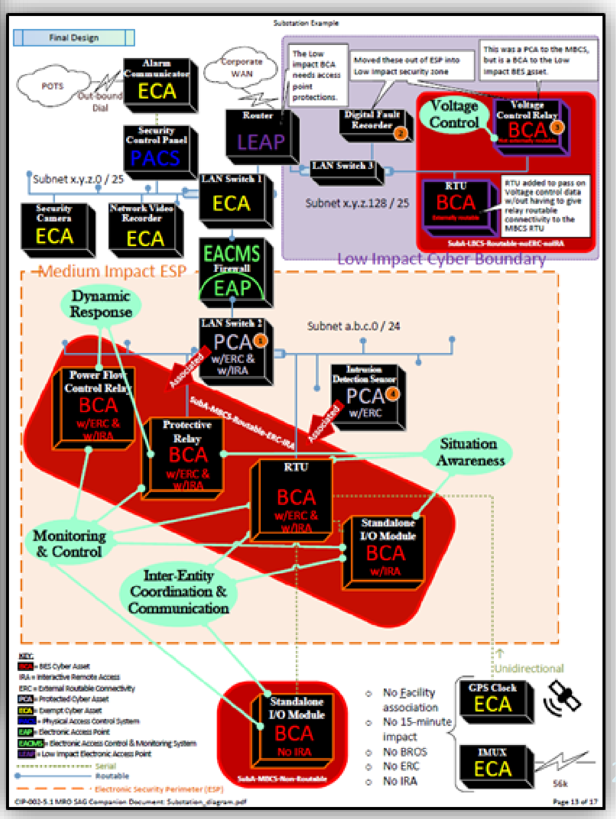
CAUTION! This creates a mixed trust environment. L2 Switch cannot be a LEAP. The whole physical "box" is in the MBCS and these Cyber Assets are still high-watermarked to Medium PCAs in this configuration.

CAUTION! Not actually moved out of the ESP. Requires Medium Impact PCA protective measures in this configuration.

- No Facility association
- No 15-minute impact
- No BROS
- No ERC
- No IRA

KEY:
BCA = BES Cyber Asset
IRA = Interactive Remote Access
ERC = External Routable Connectivity
PCA = Protected Cyber Asset
ECA = Exempt Cyber Asset
PACS = Physical Access Control System
EAP = Electronic Access Point
EACMS = Electronic Access Control & Monitoring System
LEAP = Low Impact Electronic Access Point
Serial
Routable
Electronic Security Perimeter (ESP)

CIP-002-5.1 MRO SAG Companion Document: Substation_diagram.pdf Page 12 of 17



The Low impact BCA needs access point protections.

Moved these out of ESP into Low impact security zone

This was a PCA to the MBCS, but is a BCA to the Low impact BES asset.

RTU added to pass on Voltage control data w/out having to give relay routable connectivity to the MBCS RTU

- No Facility association
- No 15-minute impact
- No BROS
- No ERC
- No IRA

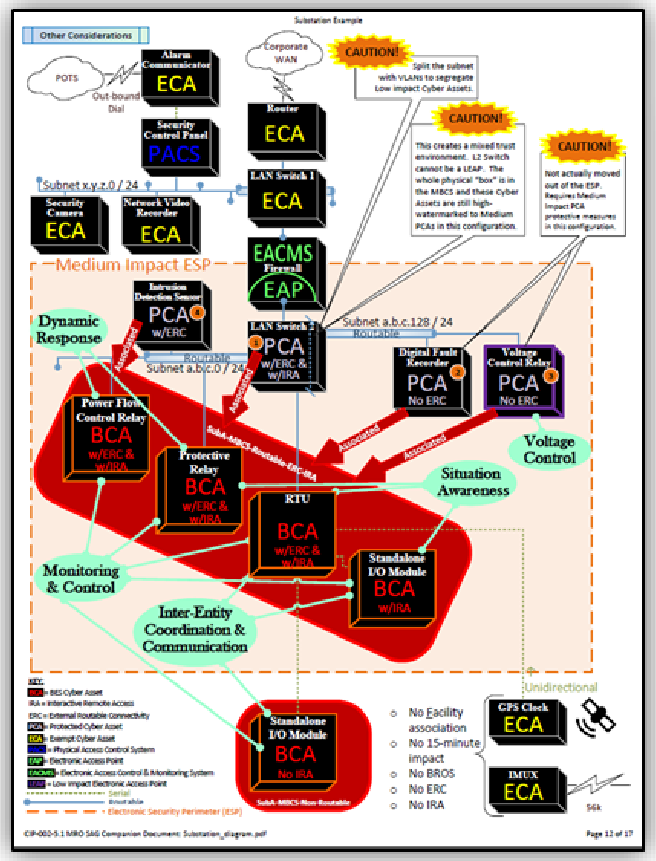
KEY:
BCA = BES Cyber Asset
IRA = Interactive Remote Access
ERC = External Routable Connectivity
PCA = Protected Cyber Asset
ECA = Exempt Cyber Asset
PACS = Physical Access Control System
EAP = Electronic Access Point
EACMS = Electronic Access Control & Monitoring System
LEAP = Low Impact Electronic Access Point
Serial
Routable
Electronic Security Perimeter (ESP)

CIP-002-5.1 MRO SAG Companion Document: Substation_diagram.pdf Page 13 of 17

Other Considerations (continued)

Mixed Trust vs. Segregated Trust Zones

- **Co-existing Impact-rated BCS**
  - High, Medium, and Low
  - High and Medium
  - High and Low
  - Medium and Low



CAUTION! Split the subnet with VLANs to segregate Low impact Cyber Assets.

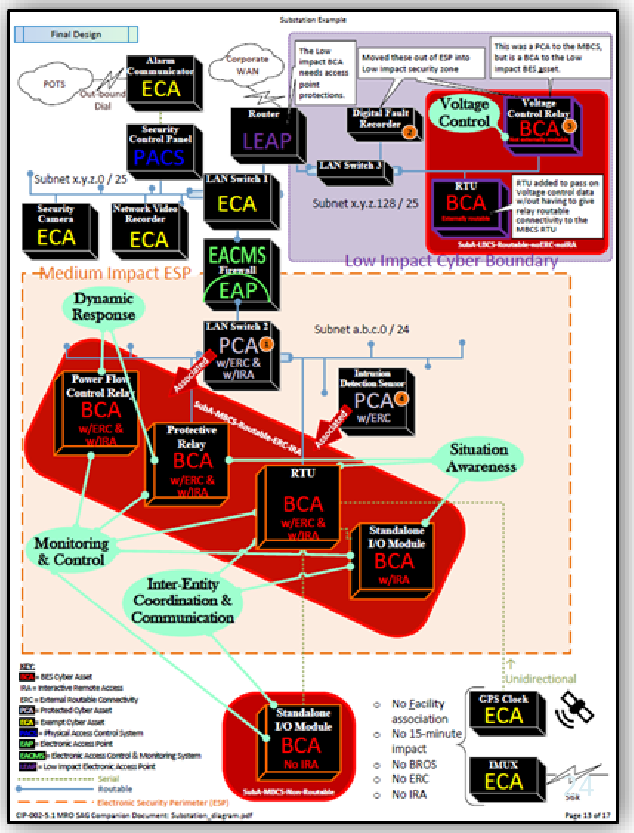
CAUTION! This creates a mixed trust environment. L2 Switch cannot be a LEAP. The whole physical "box" is in the MBCS and these Cyber Assets are still high-watermarked to Medium PCAs in this configuration.

CAUTION! Not actually moved out of the ESP. Requires Medium Impact PCA protective measures in this configuration.

- No Facility association
- No 15-minute impact
- No BROS
- No ERC
- No IRA

KEY:
BCA = BES Cyber Asset
IRA = Interactive Remote Access
ERC = External Routable Connectivity
PCA = Protected Cyber Asset
ECA = Exempt Cyber Asset
PACS = Physical Access Control System
EAP = Electronic Access Point
EACMS = Electronic Access Control & Monitoring System
LEAP = Low impact Electronic Access Point
Serial
Routable
Electronic Security Perimeter (ESP)

CIP-002-5.1 MRO SAG Companion Document: Substation_diagram.pdf
Page 12 of 17



The Low impact BCA needs access point protections.

Moved these out of ESP into Low impact security zone

This was a PCA to the MBCS, but is a BCA to the Low impact BES asset.

RTU added to pass on voltage control data w/out having to give relay routable connectivity to the MBCS RTU

- No Facility association
- No 15-minute impact
- No BROS
- No ERC
- No IRA

KEY:
BCA = BES Cyber Asset
IRA = Interactive Remote Access
ERC = External Routable Connectivity
PCA = Protected Cyber Asset
ECA = Exempt Cyber Asset
PACS = Physical Access Control System
EAP = Electronic Access Point
EACMS = Electronic Access Control & Monitoring System
LEAP = Low impact Electronic Access Point
Serial
Routable
Electronic Security Perimeter (ESP)

CIP-002-5.1 MRO SAG Companion Document: Substation_diagram.pdf
Page 13 of 17

Let's dive in to the details

First Example:

Transmission Substation

- Reference Companion Document: Substation_diagram.pdf

Medium Criteria for Generation

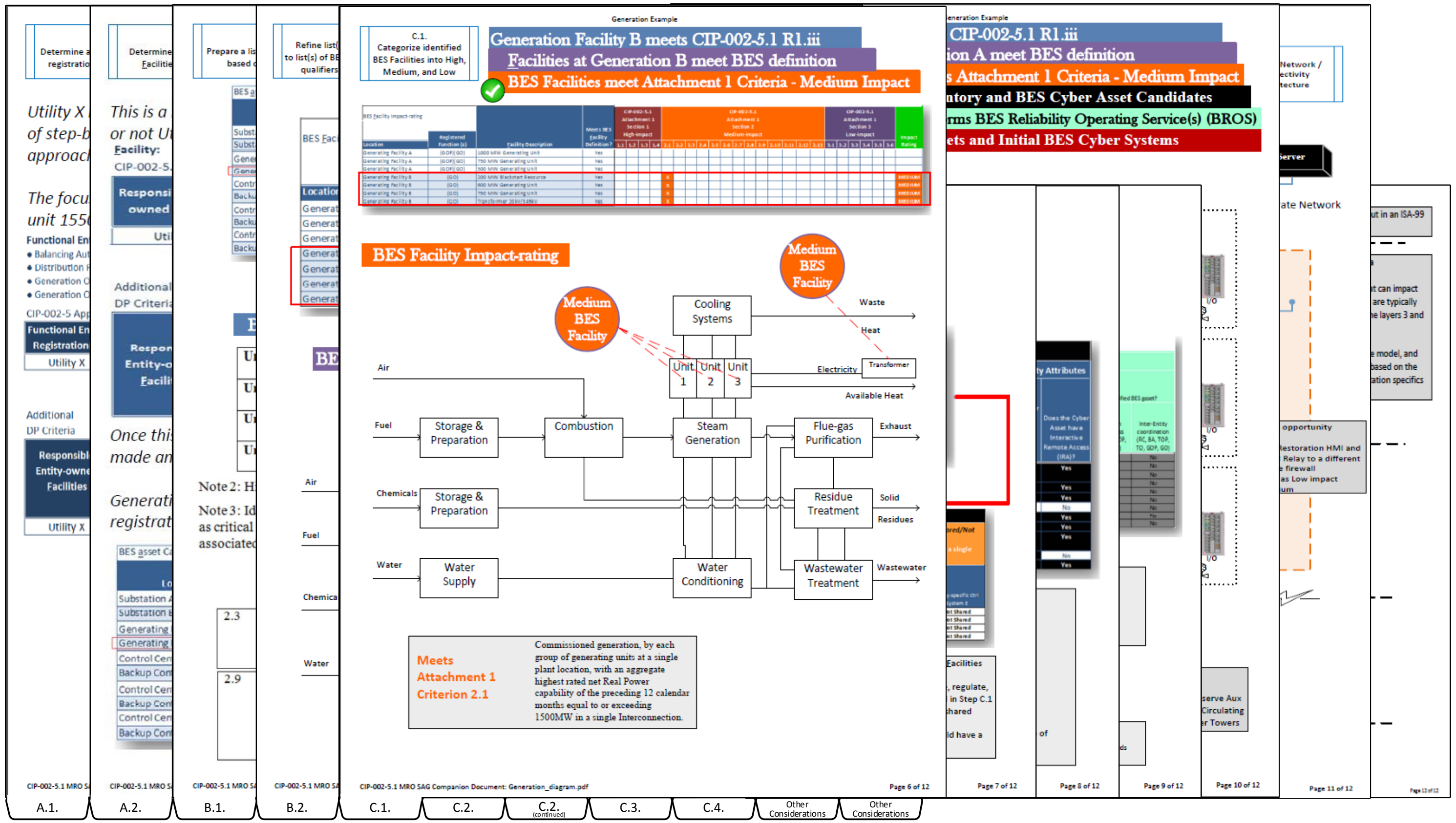
2.1	Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. ***For each group of generating units, the only BES Cyber 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.***
2.3	Each generation ***Facility*** that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.
2.6	Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

Also criteria:

2.9 SPS
2.11 Control Center for >1500MW

Generating Station – Proof of Concept

- **Approach 1.a**
- **Cyber Asset-based**
- **Mechanical Focus**
  - Units
  - Water
  - Chemicals
  - Fuel
  - Air
  - Cooling, etc.



Generation Example

C.1. Categorize identified BES Facilities into High, Medium, and Low

Generation Facility B meets CIP-002-5.1 R1.iii

Facilities at Generation B meet BES definition

BES Facilities meet Attachment 1 Criteria - Medium Impact

BES Facility Impact-rating				CIP-002-5.1 Attachment 1 Section 1 High-impact				CIP-002-5.1 Attachment 1 Section 2 Medium-impact													CIP-002-5.1 Attachment 1 Section 3 Low-impact						
Location	Registered Function (s)	Facility Description	Meets BES Facility Definition?	1.1	1.2	1.3	1.4	2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	2.11	2.12	2.13	3.1	3.2	3.3	3.4	3.5	3.6	Impact Rating
Generating Facility A	(GOP)(GO)	1000 MW Generating Unit	Yes																								
Generating Facility A	(GOP)(GO)	750 MW Generating Unit	Yes																								
Generating Facility A	(GOP)(GO)	500 MW Generating Unit	Yes																								
Generating Facility B	(GO)	200 MW Blackstart Resource	Yes					x																			MEDIUM
Generating Facility B	(GO)	600 MW Generating Unit	Yes					x																			MEDIUM
Generating Facility B	(GO)	750 MW Generating Unit	Yes					x																			MEDIUM
Generating Facility B	(GO)	Transformer 20kV/345kV	Yes					x																			MEDIUM

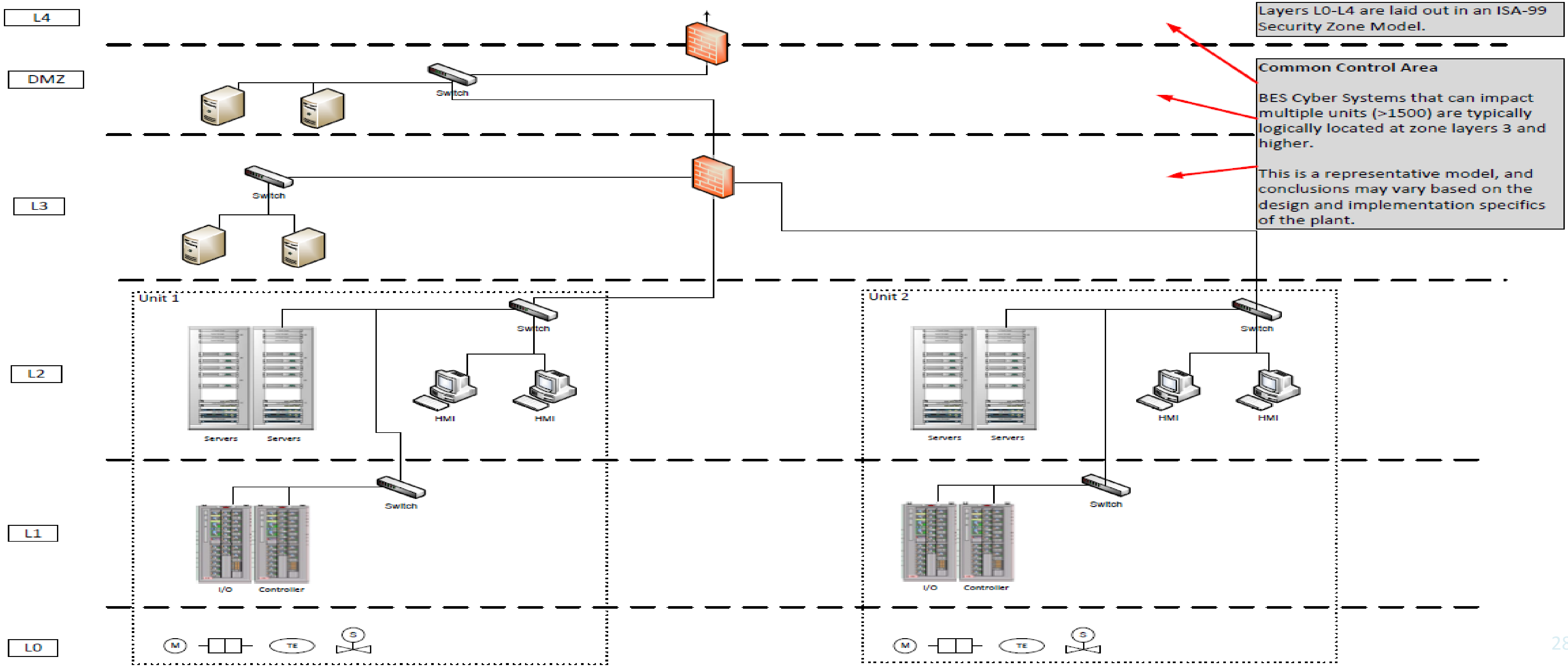
BES Facility Impact-rating

Meets Attachment 1 Criterion 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 1500MW in a single Interconnection.

CIP-002-5.1 MRO SAG Companion Document: Generation_diagram.pdf Page 6 of 12

Other Considerations - Segregated Trust Zones



Layers L0-L4 are laid out in an ISA-99 Security Zone Model.

Common Control Area

BES Cyber Systems that can impact multiple units (>1500) are typically logically located at zone layers 3 and higher.

This is a representative model, and conclusions may vary based on the design and implementation specifics of the plant.

Let’s dive in to the details

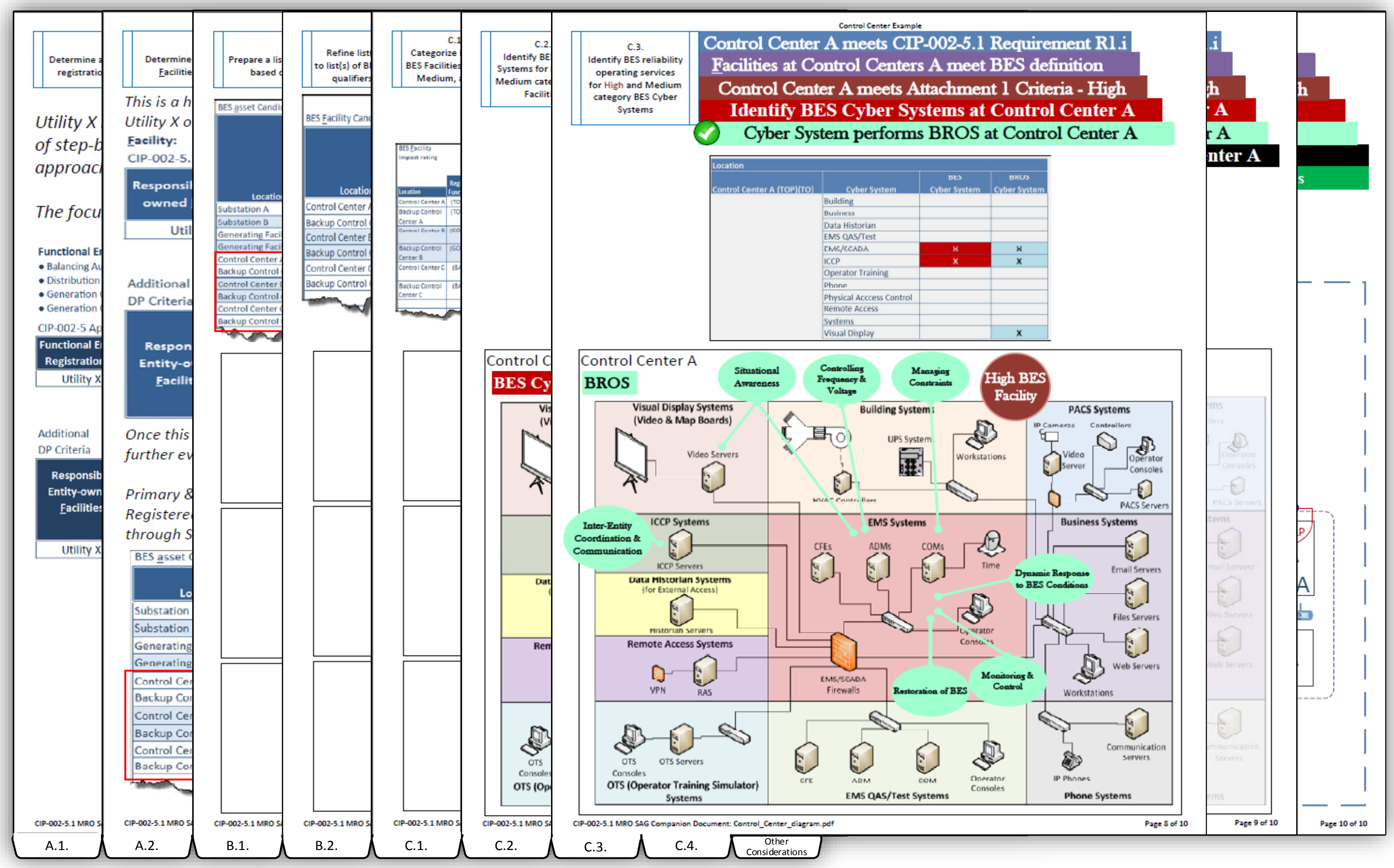
Second Example:

Generating Station

- Reference Companion Document: Generation_diagram.pdf

Control Center – Proof of Concept

- **Approach 1.b**
- **Cyber System-based**
  - Business Systems
    - ✓Corporate Apps
    - ✓Building, etc.
  - BES Systems
    - ✓EMS
    - ✓ICCP, etc.
- **BROS**


Control Center Example
C.3. Identify BES reliability operating services for High and Medium category BES Cyber Systems
Control Center A meets CIP-002-5.1 Requirement R1.i
Facilities at Control Centers A meet BES definition
Control Center A meets Attachment 1 Criteria - High
Identify BES Cyber Systems at Control Center A
Cyber System performs BROS at Control Center A
Control Center A
BROS
Situational Awareness
Controlling Frequency & Voltage
Managing Constraints
High BES Facility
Inter-Entity Coordination & Communication
Dynamic Response to BES Conditions
Monitoring & Control
Restoration of BES
Visual Display Systems (Video & Map Boards)
Building Systems
PACS Systems
ICCP Systems
EMS Systems
Business Systems
Data Historian Systems (for External Access)
Remote Access Systems
OTS (Operator Training Simulator) Systems
EMS QAS/Test Systems
Phone Systems
CIP-002-5.1 MRO SAG Companion Document: Control_Center_diagram.pdf
Page 8 of 10
Page 9 of 10
Page 10 of 10
A.1.
A.2.
B.1.
B.2.
C.1.
C.2.
C.3.
C.4.
Other Considerations

Let's dive in to the details

Third Example:

Control Center

- Reference Companion Document: ControlCenter_diagram.pdf

Control Center Summary

- **Assemble a cross functional assessment team**
- **Assessment team needs to:**
  - Have representation from of each system identified
  - Understand system functionality and interconnectivity
  - Be able to answer questions about the BROS
- **Start at the System level**

Control Center Summary (continued)

- Eliminate systems that do not meet the criteria for applicable systems
- Assess Cyber Assets in applicable BES Cyber Systems
- DOCUMENT ALL ASSESSMENTS!!!
- Get ready to apply the rest of the CIP Standards to the applicable Cyber Assets
- To assist with classifications of Cyber Asset refer to the NERC Glossary of Terms

Testing Results

- **Three different Registered Entities**
- **Three different BES asset types**
- **Three different ways to apply**
  - Electrical
  - Mechanical
  - Cyber System
- **One Methodology**
- **Three successful outcomes**

Summary

- SAG is over a year in the making
- CIP SMET is proud to present this to the region and the industry

**Thank you for your time,
and this opportunity!**

Questions?