NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

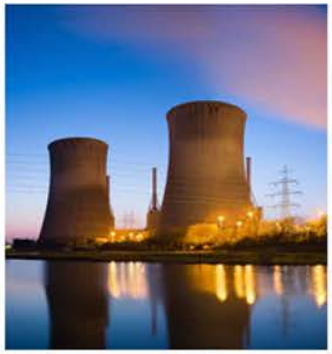
Auditing Low Impact BES Cyber Systems

Scott R. Mix, CISSP, NERC Senior CIP Technical Manager

ReliabilityFirst Spring CIP V5 Workshop

April 14-15, 2016

RELIABILITY | ACCOUNTABILITY

Disclaimer

The information contained in this presentation is preliminary, and represents a possible approach being considered by the ERO as of the fall of 2015.

These approaches are subject to review and modification as the ERO finalizes the audit approaches in response to pre-audit outreach conducted before the effective date of the requirements.

These approaches are also subject to review and modification based on further directives from FERC and subsequent modifications to the requirements by standards development actions.

Agenda

- Lists
- Not all Low Impact Locations are Equal
- Possible Audit Approaches
  - Sampling
  - Connectivity (LERC/LEAP)
  - Generation
  - Transmission
  - Control Centers
  - Physical Security
  - Security Awareness
  - Incident Response
  - Mixed Environments
- WECC Low Impact Case Study Implementation Lessons Learned

Low Impact Lists

- Discrete lists of Low Impact BES Cyber Systems are not required
- HOWEVER:
  - A list containing the name of “each asset that contains a low impact BES Cyber System” is required (CIP-002-5.1 Requirement R1 Part 1.3 “Identify each asset that contains a low impact BES Cyber System …”)
  - This would be a list of generating plants, transmission stations, certain distribution stations, and certain “small” control centers, that contain low impact BES Cyber Systems

Low Impact Lists

- The entity should be prepared to demonstrate that all BES assets (locations) are accounted for on either the list of high impact, medium impact or low impact locations (note: a list of high or medium impact locations is not specifically required, but can be surmised by looking at lists of high impact and medium impact BES Cyber Systems, if they exist)
- The entity should be prepared to demonstrate that all the low impact BES Cyber Systems at the assets on the lists have been afforded electronic and physical protections, and are included in incident response plans

Low Impact Lists

- Similarly, lists of personnel with access to low impact BES Cyber Systems is not required
- HOWEVER:
  - The entity should be prepared to demonstrate how it determines whether personnel have a “need” to access the low impact BES Cyber Systems
  - The entity should be prepared to demonstrate how the electronic security protections and physical protections are implemented to ensure that only personnel that have a “need” have access
  - The entity should be prepared to demonstrate that all those personnel have had access to the security awareness materials

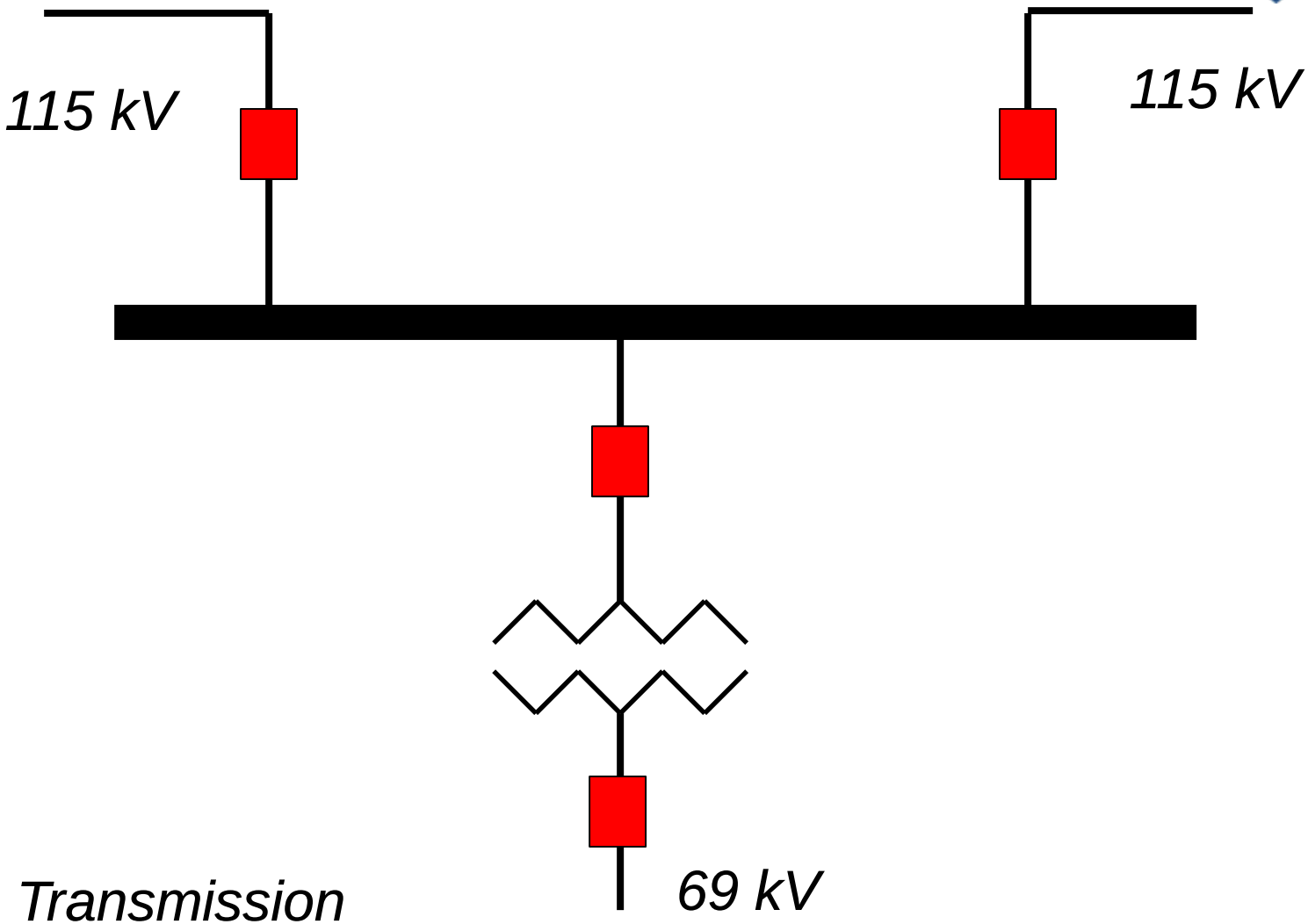
Low Impact Lists

- Even though BES Cyber Asset / BES Cyber System lists are not required for compliance, it is in the entity's best interest to maintain lists to ensure that all low impact BES Cyber Systems are properly secured with both physical and electronic controls
  - Station, plant, or Control Center drawings showing all Cyber Assets at the location, drawings showing computer network paths through identified LEAPS, and drawings of physical locations to demonstrate required physical access control may be beneficial in demonstrating compliance
  - These lists will not be assessed for completeness – only to help the entity "tell its story"

Not All Low Impact Locations are Equal

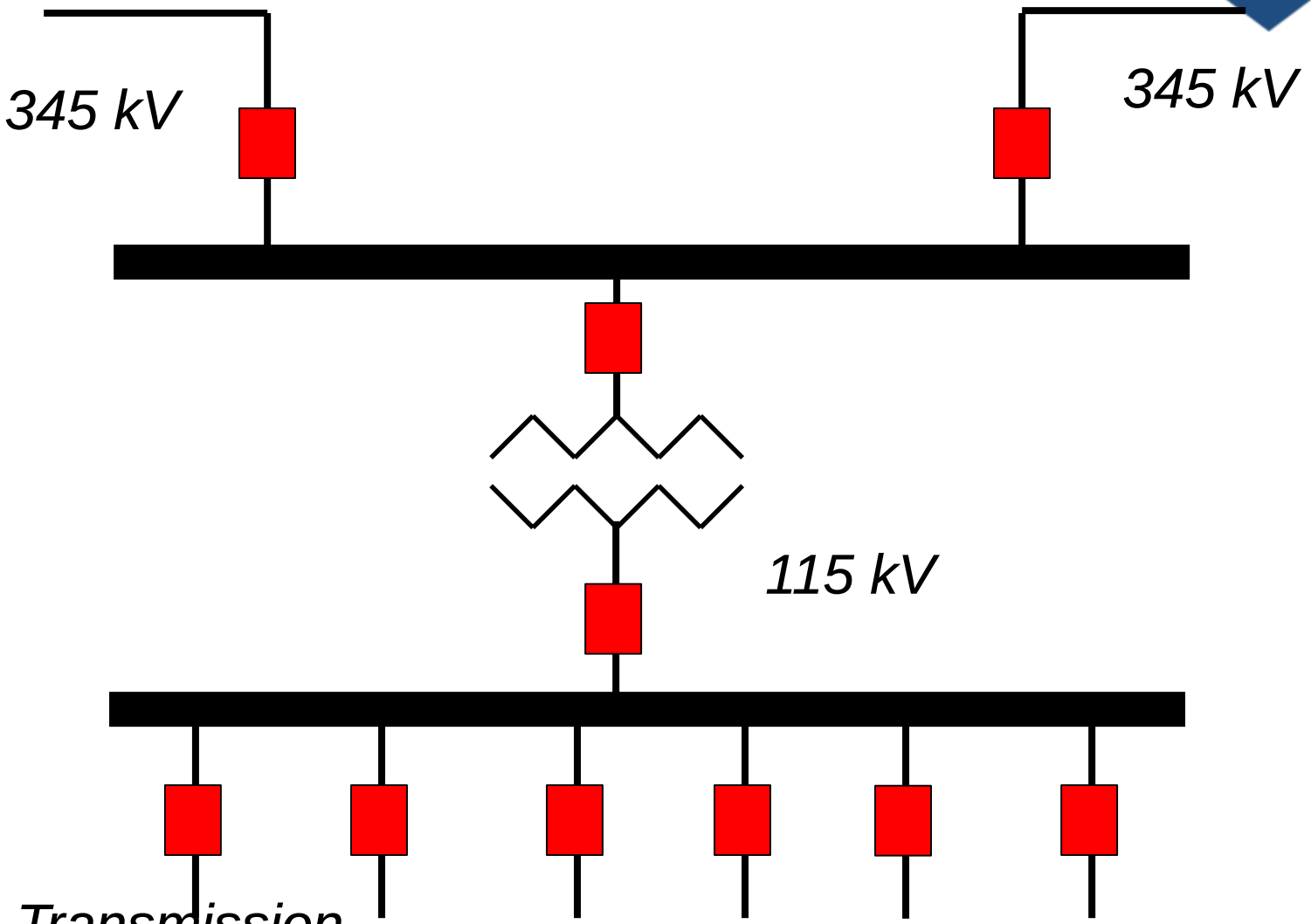
- "Low impact" covers a wide range of BES locations and Facilities
- Within "low impact" there are potentially vastly different BES impacts
  - The CIP Standards don't make a distinction between a "big" (i.e., more impactful) low impact site and a "small" (i.e., less impactful) low impact site
- Consider the following field examples:

Not All Low Impact Locations are Equal

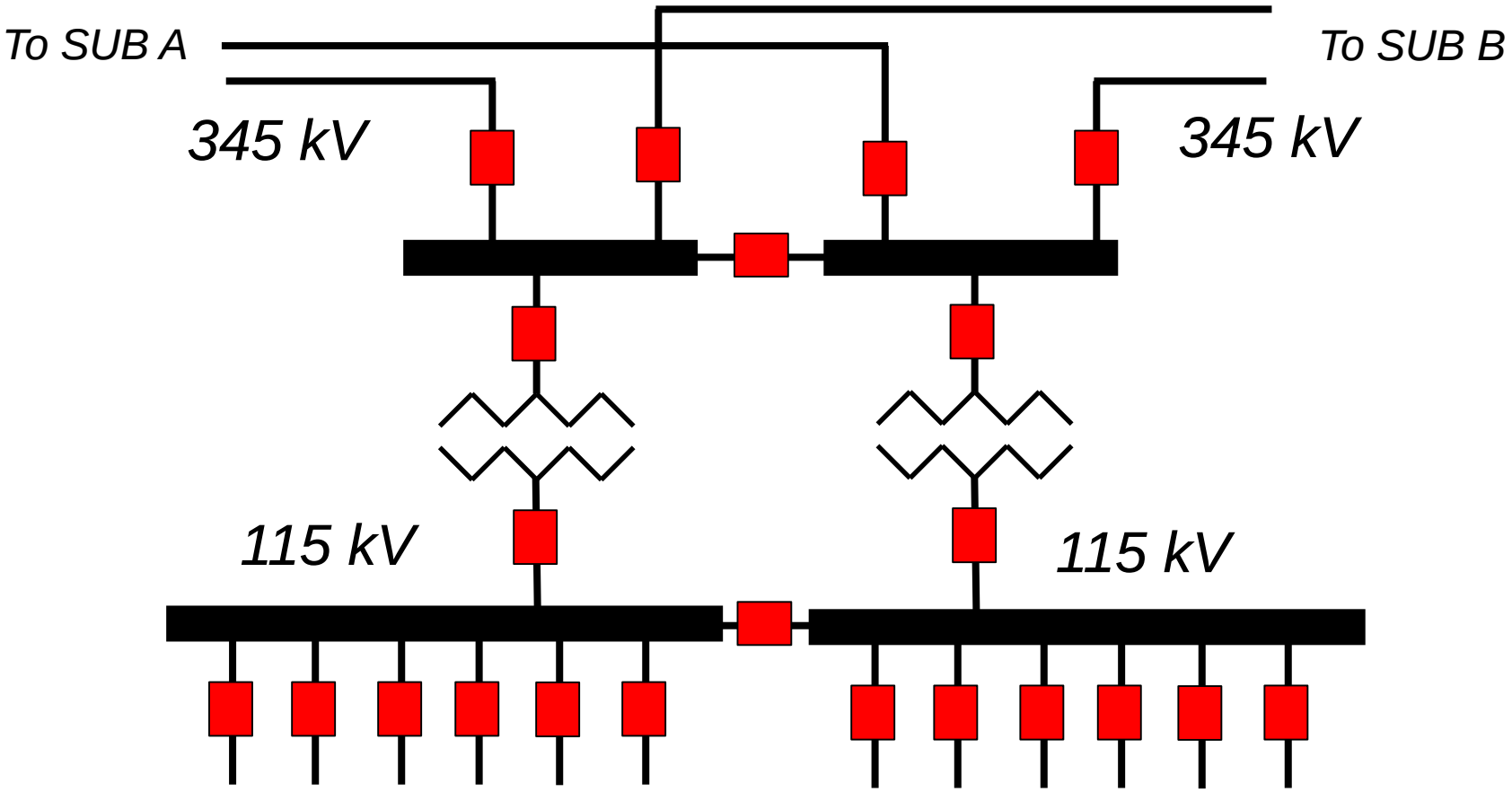


Transmission Considerations

Not All Low Impact Locations are Equal

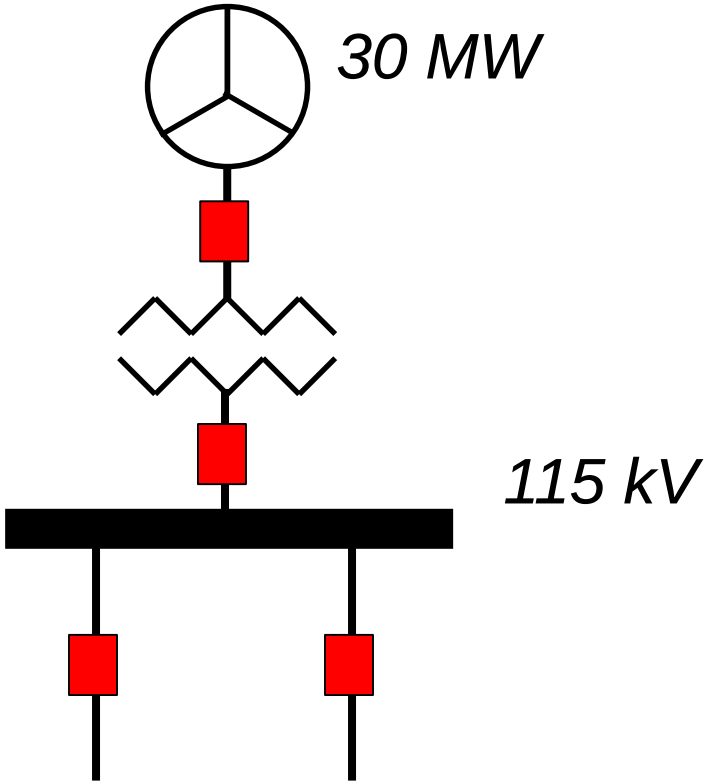


Not All Low Impact Locations are Equal



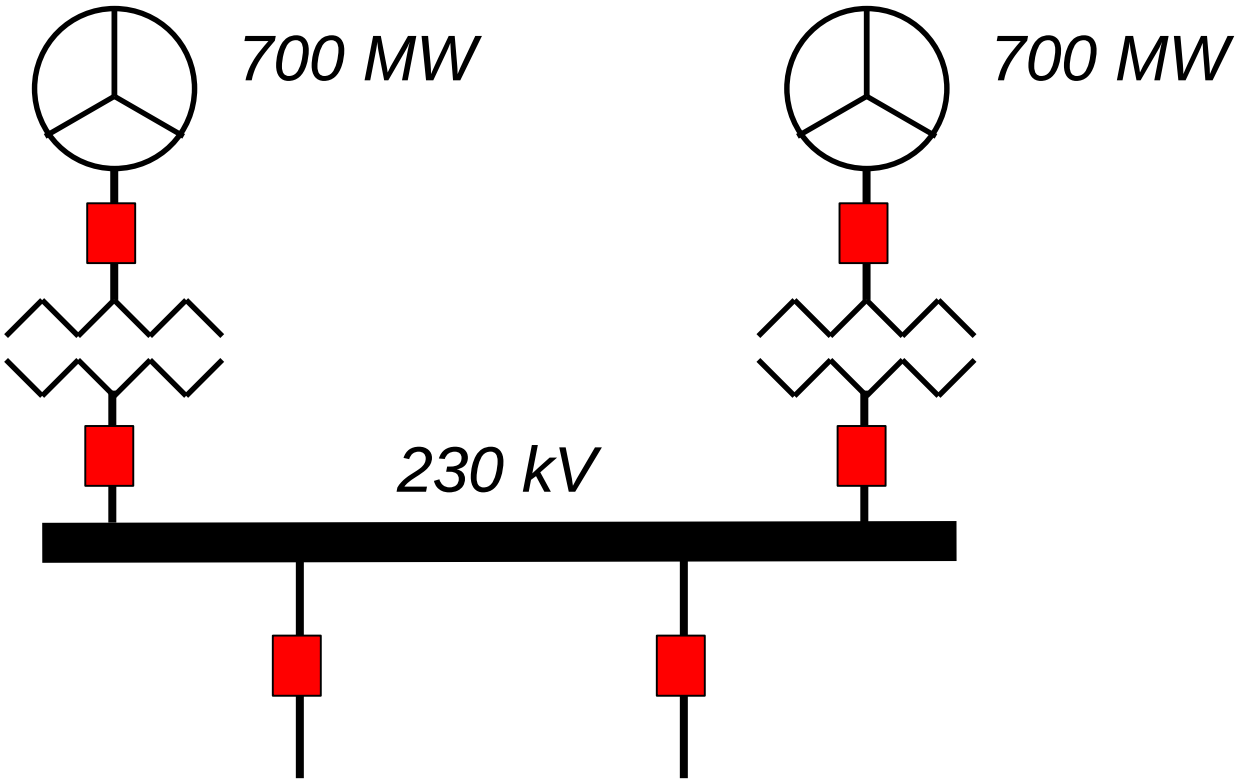
Transmission Considerations

Not All Low Impact Locations are Equal



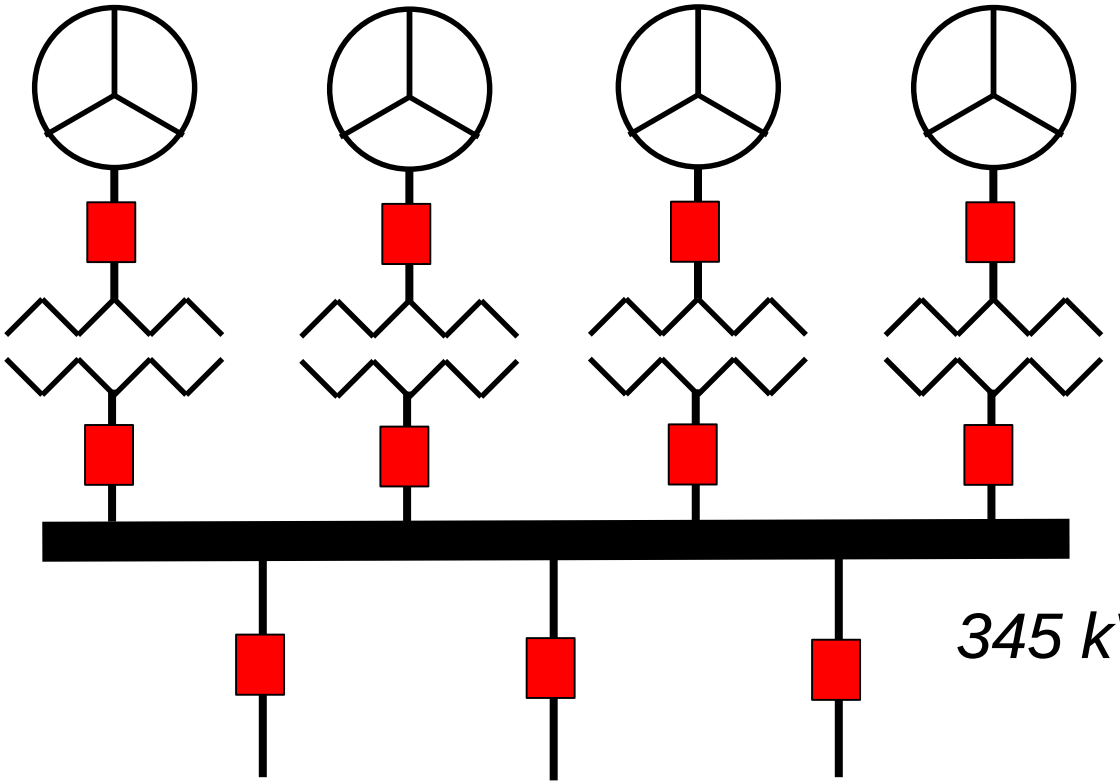
Generation Considerations

Not All Low Impact Locations are Equal



Generation Considerations

Not All Low Impact Locations are Equal



4 x 700 MW
(with segmented control systems)

345 kV

Generation Considerations

Compliance Implications

- Pure random sampling of low impact assets for audit purposes is not appropriate
  - Random sampling within *specific subsets* of low impact assets may be appropriate
- Expect risk and impact based judgmental sampling
- Expect more audit attention at low impact locations with larger impact
- Expect more audit attention to larger generation plants than at smaller plants

Auditing Connectivity

- In order to determine if LERC/LEAP is present, expect a number of questions:
  1. Is there *any* routable protocol communications in the wide area network used to communication with assets containing low impact BES Cyber Systems?
     - If no, then there is no LERC, and no requirement for LEAP
     - If yes, then further questions are needed
     - Expect to be asked for network drawings, configurations, etc. to support your answer

Auditing Connectivity

2. For each low impact “location” (asset), is there routable protocol communications in the wide area network connecting to that location?
   - If no, there is no LERC at that location
   - If yes, further questions will be asked
   - Expect to be asked for network drawings, configurations, etc. to support your answer

Auditing Connectivity

3. Does the routable communications connect to the low impact BES Cyber Systems (including reference model 4 considerations)?
   - If no, there is no LERC at that location
     - Example: stand-alone computer in transmission station used for time entry and work orders
     - Note there may be modifications to this concept in response to FERC Order No. 822
   - If yes, then there may be LERC at the location
   - Note that *any* routable protocol communications to the BES Cyber Assets may trigger LERC
     - LERC is *not* restricted to only telemetry and control communications
   - Expect to be asked for network drawings, configurations, etc. to support your answer

Auditing Connectivity

4. Are there "protocol breaks" of any kind (see reference model 5 or 6) in the local area portion of the communications path?
   - If yes, expect to be asked to provide details of the protocol break
     - Note there may be modifications to this concept in response to FERC Order No. 822
   - If no, then there is LERC at the location, and a LEAP should be identified
     - The Cyber Asset containing the LEAP may be located at the asset, or may be located remote to the asset
   - Expect to be asked for network drawings, configurations, etc. to support your answer

Auditing Connectivity

- Once LERC has been determined to exist at an asset, the low impact BES Cyber Systems must all be protected logically
- Expect to be asked for network drawings showing that all low impact BES Cyber Systems are appropriately protected
  - Detailed inventory lists are not required, but high-level network drawings may be beneficial for describing what needs to be protected
  - Detailed inventory lists may be provided (at the entity's option) to help support decisions, but the detailed lists will not themselves be subject to audit

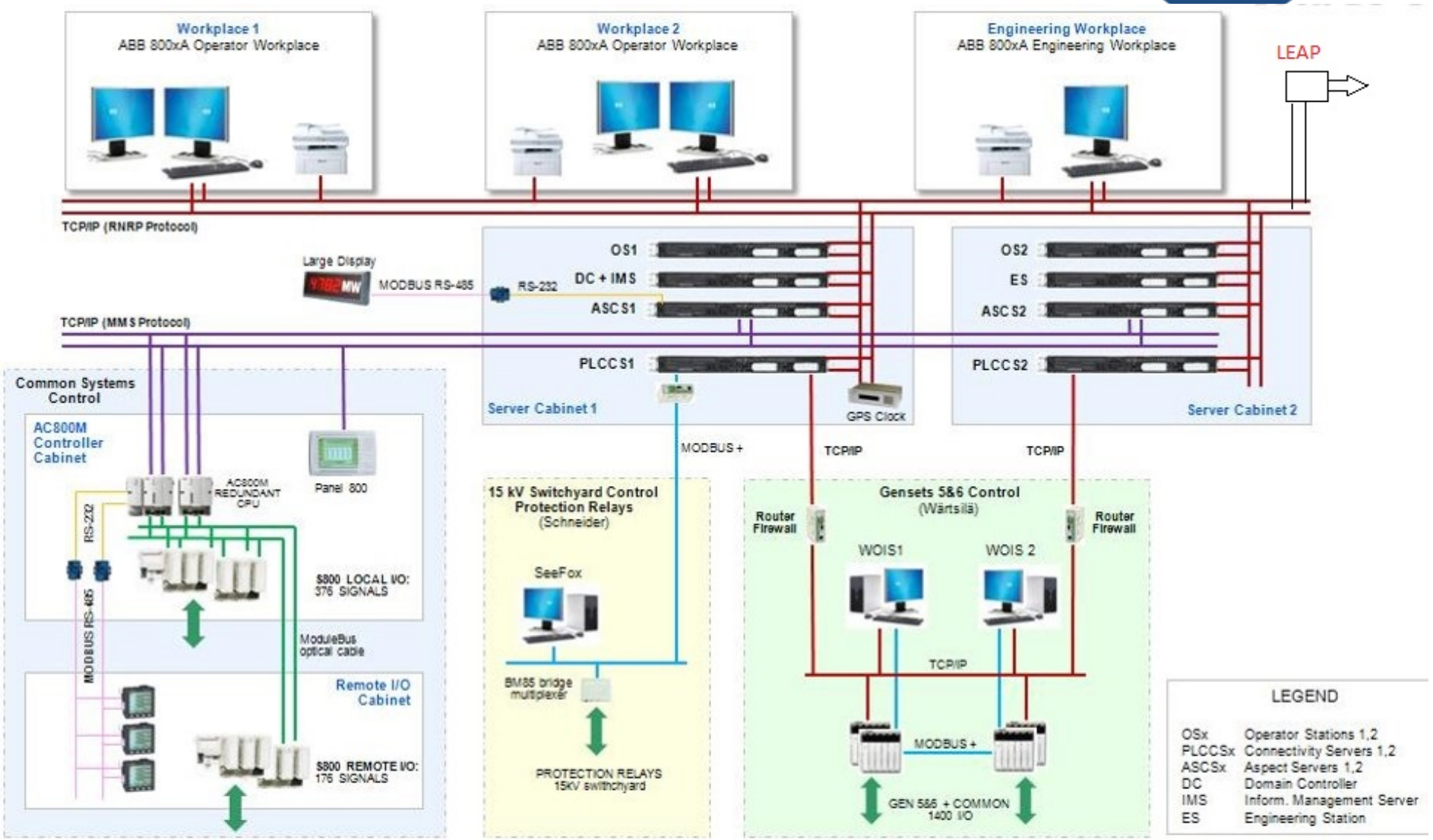
Low Impact Audit Evidence

- Since lists of BES Cyber Assets / Systems are not required, what kinds of evidence are appropriate?
- Since there are no device-specific requirements, lists aren't needed
- Requirements are for border protection or system-level recovery

Low Impact Audit Evidence

- Existing "as-built" documentation and drawings should provide sufficient detail to allow the ERO to determine whether protections are put into place
  - Drawings show connectivity
  - Drawings show high-level component detail
  - Drawings allow auditors to determine whether all required logical protections (e.g., LERC/LEAP) are put into place
  - Drawings can indicate physical locations that need to be protected (or at least identify what needs physical protection)
  - Drawings can show what systems need incident response plans

Possible Low Impact Evidence



Source: http://www.intea.hr/uploads/control_system.jpg (modified)

Possible Low Impact Evidence

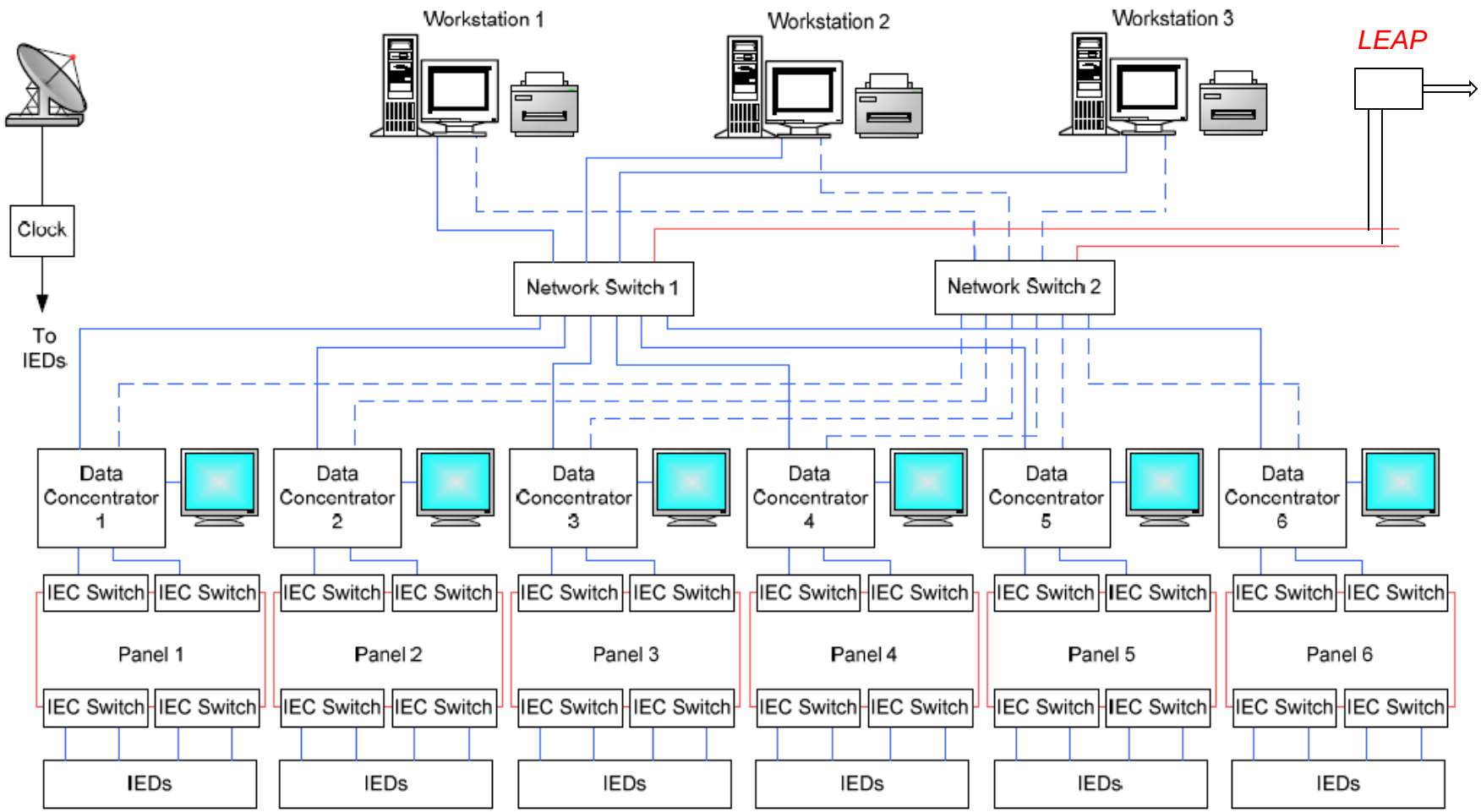


Fig. 9. Ethernet network architecture implemented in the IGSTPP

Source: http://www.ucaiug.org/Meetings/CIGRE_2014/USB%20Promo%20Content/SEL/Technical%20Papers/Integration%20Considerations%20For%20Large%20Scale%20IEC%2061850%20Systems.pdf *(modified)*

LERC / LEAP

- The entity should be prepared to provide a list of LEAP devices, and indicate which (assets containing) low impact BES Cyber Systems are associated with each LEAP
- The entity should be prepared to demonstrate rationale for what constitutes “necessary inbound and outbound bi-directional routable protocol access”
- The entity should be prepared to demonstrate the access control lists that ensure that only “necessary inbound and outbound” connections are allowed

LERC / LEAP

- Expect that large or complicated LEAP devices may receive additional inspection to ensure that all traffic between different low impact BES Cyber Systems is correctly filtered
- Expect that LEAP devices at Control Centers will be audited concurrently with the Control Centers

Dial-up

- The entity should be prepared to demonstrate Dial-up Connectivity protections at low impact BES Cyber System locations, the authentication methods in place, and any “per Cyber Asset” capabilities documented

Large Generation

- Based on inherent risk and impact, expect more attention at any generation plant > 1500 MW
  - The entity should be prepared to demonstrate how the unit controls are segregated, including computer network diagrams, firewall configurations, data flow analysis, etc.
  - The entity should be prepared to demonstrate the analysis of any common systems at the plant
    - Expect the analysis to include both a time-based component as well as an impact-based component
  - The entity should be prepared to allow inspection of any common control rooms that have control of >1500 MW of generation

Larger Low Impact Transmission

- Based on inherent risk and impact, expect more attention at large networked transmission stations
  - For example, transmission stations that have multiple lines, but with some excluded from the IRC 2.5 calculation because of being generator interconnection lines
  - The requirements are the same, but they may be more likely to be reviewed as part of the audit

Control Center

- Based on inherent risk and impact, expect more attention at Balancing Authority and multi-function Control Centers
- Based on inherent risk and impact, expect more attention if the control center is close to a medium impact threshold

Physical Security

- Low Impact physical security is significantly different than that required for CIP-014
  - CIP-014 uses medium impact transmission as an input
- Much of existing physical protections (e.g., for copper theft protection) should be leveraged:
  - Fencing, locked gates, lighting, cameras, motion sensing, etc.
- Physical security is required for all low impact BES Cyber System locations regardless of electronic connectivity

Physical Security

- Physical Security applies to both the BES asset locations (i.e., generation plants, transmission stations, control centers) as well as to locations containing Low Impact BES Cyber System Electronic Access Points (LEAPs)
  - These might be at BES locations containing low impact BES Cyber Systems, BES locations containing medium impact BES Cyber Systems, at telecommunication hub locations, or at Control Centers

Physical Security

- The entity should be prepared to demonstrate how it controls access to the BES asset or LEAP device
- The entity should be prepared to demonstrate how it assesses the “based on need” clause of the requirement
- Since LEAPs can be located at “field locations,” Control Centers, or at other locations (e.g., communications hubs), the entity should be prepared to produce a list of locations containing LEAPs, especially if they are located outside of BES assets

Physical Security

- The entity should be prepared to demonstrate that all Low Impact BES Cyber Systems and LEAP devices have been afforded the appropriate protections.
- Drawings, floor plans, etc. are acceptable, so long as they provide sufficient detail to indicate that all required BES Cyber Systems and LEAP devices are included
  - Detailed inventory lists are not required, and reviews will be conducted at a high level

Cyber Security Awareness

- The entity should be prepared to demonstrate that cyber security awareness materials have been made available
  - Materials and audit approaches are the same as for high and medium
  - Examples include emails, posters, meeting presentations, etc.
- Specific actions are similar to CIP-004-6 Requirement R1 Part 1.1, but a “change interval” of 15 months rather than 3 months.

Incident Response

- The entity should be prepared to demonstrate it has the required procedure documentation and evidence that the procedure has been followed
- Specific actions are similar to CIP-008-5, but relaxed testing timeframes (36 months rather than 15 months) and plan update timeframes (180 days rather than 90 days).

Mixed High / Med and Low

- The low impact requirements are not expected to be implemented in a vacuum
- Entities with low impact BES Cyber Systems as well as high or medium impact BES Cyber Systems may take advantage of existing programs or procedures, for example:
  - Cyber Security Awareness materials and delivery may be the same for all impact levels
  - Physical Security plan documentation developed for CIP-006-6 Requirement R1, Part 1.1 may include sections on how physical security controls are applied to locations containing low impact BES Cyber Systems

Mixed High / Med and Low

- Examples continued:
  - Configuration and management of electronic access controls may be similar for LEAPs and EACMS containing EAPs (e.g., common vendor, common equipment, common configuration tools, common procedures for requesting and granting access, common administrative staff)
  - Cyber Security Incident Response procedures may share procedural documentation for all impact levels
- The entity should be prepared to demonstrate procedures for applicability and note differences between high/medium impact and low impact, if any

Implementation Lessons Learned

Observations from WECC Low Impact Study:

- Don't make it more difficult or bigger than it is. Lean on existing policies already in place.
- Plug in early, something will always pop-up and potently impact the project. Build some extra time into your project timeline for testing & feedback, budget cycles, and unplanned contingencies
- Review the standards/requirements and clarify all of the documentation requirements for each standard early on
- Research, Research, Research - Tap unlikely resources such as your commercial insurance carrier/broker – One participant used a great template from their insurance carrier for their cyber incident response plan

Implementation Lessons Learned

- Don’t be fooled by the generic and oversimplified requirements for policies and requirements - They are simplistic by design to allow you the flexibility for workable policies and plans
- Engage SMEs and plant/field personnel who are going to have to live with the results of your creations early on
- Have weekly team meetings – even if there’s not much to discuss, it keeps the project on everyone’s radar
- Make sure all documents, at minimum, undergo a basic technical and legal review and then a final formatting review – cut & paste is a blessing and a curse!
- If you are coming from the IT side of the house, go shake hands with and learn about the OT environment, as it will allow you to better understand the assets you’re trying to protect

Questions and Answers