North American Transmission Forum

NATF CIP-015 INSM Implementation Guidance

Open Distribution

Copyright © 2025 North American Transmission Forum (“NATF”). All rights reserved. Not for sale or commercial use. The NATF makes no and hereby disclaims all representations or warranties, either express or implied, relating to the content, including as to the accuracy or completeness of the information. No liability is assumed by the NATF for any damages arising directly or indirectly from the content or by the use or application thereof. Use of the content constitutes agreement to defend, indemnify, and hold the NATF harmless from and against all claims arising from such use.

Version 2.0
Document ID: 1797
Approval Date: 09/24/2025

Versioning

Version History

Date	Version	Notes
08/14/2025	1.0	Initial version
09/24/2025	2.0	Approved for Open Distribution

Review and Update Requirements

- Review: every 5 years
- Update: as necessary

Contents

Versioning 2

Contents 3

1. Introduction....4

2. Goal/Problem Statement 4

3. Scope 4

4. Reliability Standard....5

5. Periodic Review 20

6. References.... 21

Appendix 1: Risk Based Considerations.... 22

Appendix 2: Generation Reference Architecture 1 24

Appendix 3: Generation Reference Architecture 2 25

1. Introduction

On January 19, 2023, (FERC) issued Order No. 887 [1] directing NERC to develop requirements within the CIP Reliability Standards for internal network security monitoring (INSM) of all high-impact BES Cyber Systems and medium impact BES Cyber Systems with ERC. Order No. 887 directed NERC to develop Reliability Standard(s) requirement(s) for any new or modified CIP Reliability Standards that address three security issues. The new standard is Reliability Standard CIP-015-1 [2]. The intent of CIP-015-1 is to improve the probability of detecting anomalous or unauthorized network activity to facilitate improved response and recovery from an attack [3].

On September 19, 2024, FERC issued Docket No. RM24-7-000 [4], which proposed approving Reliability Standard CIP-015-1 but directed NERC to modify the standard to include monitoring of EACMS and PACS systems outside of the electronic security perimeter.

This implementation guidance is specific to Electronic Security Perimeters (ESP). This document provides implementation guidance for CIP-015-1 only, as the outcome of the modifications is not known.

2. Goal/Problem Statement

The goal of INSM is to identify adversarial activity in a trusted environment. INSM technologies are most meaningful and effective when they are built to be industrial control system (ICS) protocol aware and provide detection of network activity that might hamper an industrial process. INSM is commonly implemented as a detective (passive) control that assists in finding and responding to adversarial activity rather than a preventative control that blocks suspicious activity. INSM systems may be combined with other detective controls and may also integrate with preventative controls, such as endpoint detection and response. By itself, INSM is not expected to prevent any network or endpoint activity, and many current products are specifically designed as passive monitors to reduce the likelihood of negative impact to operational systems.

While a Responsible Entity may choose to implement active prevention measures in an INSM system or may have a software defined network (SDN) that provides this capability, prevention is not required in Reliability Standard CIP-015-1.

The Implementation Guidance proposes criteria and reference architecture to help inform INSM deployment; this is applicable to the following location types:

- Substations
- Control Centers
- Generation

3. Scope

This NATF Implementation Guidance document describes ways that a Responsible Entity could comply with CIP-015-1 Requirements R1, R2, and R3.

4. Reliability Standard

Requirement R1.

Each Responsible Entity shall implement one or more documented process(es) for INSM of networks protected by the Responsible Entity’s High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with ERC ESP(s) to provide methods for detecting and evaluating anomalous network activity. The documented process(es) shall include each of the following requirement Parts: [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment].

1.1. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

1.2. Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.

1.3. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

Requirement Guidance for R1.

Part 1.1

Architecture diagrams in this guidance, if implemented, use a risk-based rationale, and describe how network data feeds were selected to monitor for network activity, including connections, devices, and network communications.

Part 1.2 and Part 1.3

Reference the Technical Rationale for Reliability Standard CIP-015-1 [5].

Substation INSM Architectures

The network architectures in this section are intended to represent the common network configurations and technologies used in substations. Note that this is not an all-inclusive list and that other network architectures can be made compliant with CIP-015-1.

Substation Reference Architecture 1

The substation network detailed below consists of an Ethernet-connected Remote Terminal Unit (RTU) with managed switches positioned to the north and south of the RTU. Protective relays and other intelligent electronic device (IED)s are connected serially (e.g., using RS-232 / RS-485) to Ethernet-to-serial converters. The managed switches are configured with mirror / SPAN ports to forward traffic to an INSM system located at the substation.

A risk-based analysis will show that collection of INSM traffic at the managed switches would capture enough of the traffic to detect anomalous activity.

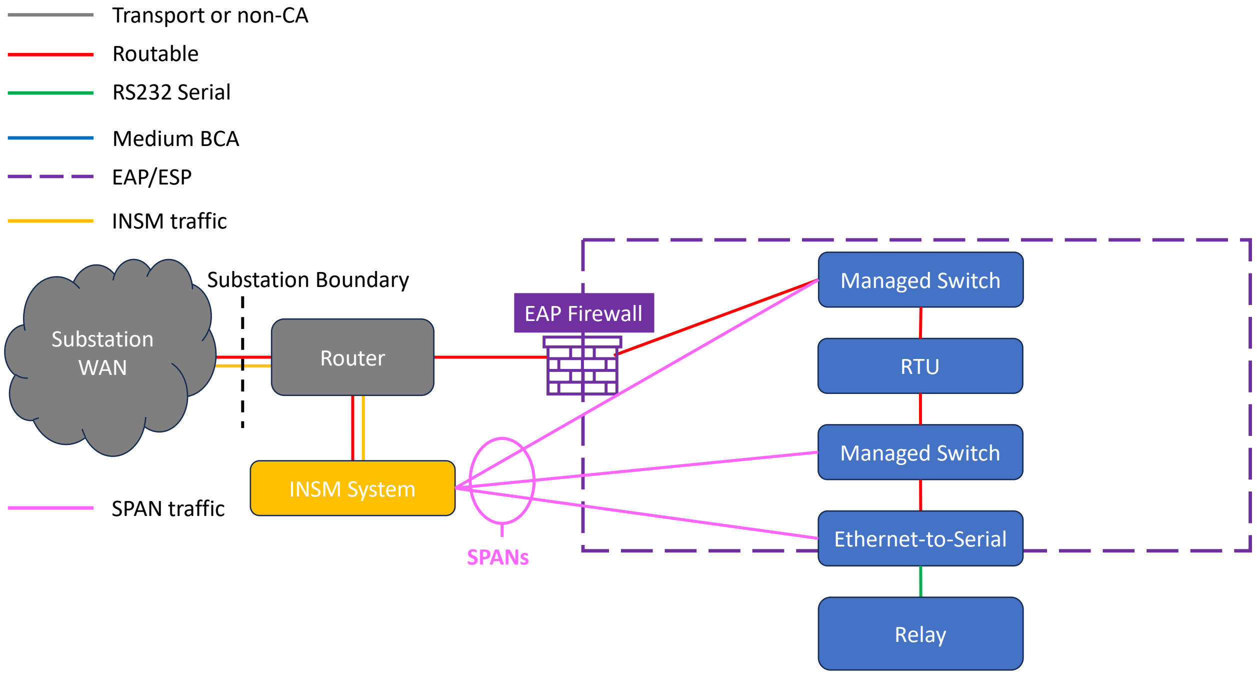


Figure 1: Substation Reference Architecture 1

Substation Reference Architecture 2

The substation network detailed below consists of a star topology with a SDN switch. The SDN can be used to create a baseline of expected network activity and send network activity that doesn't match the baseline to a remote INSM system for evaluation.

A risk-based analysis shows that collection of INSM traffic at the SDN switch captures enough of the traffic to detect anomalous activity.

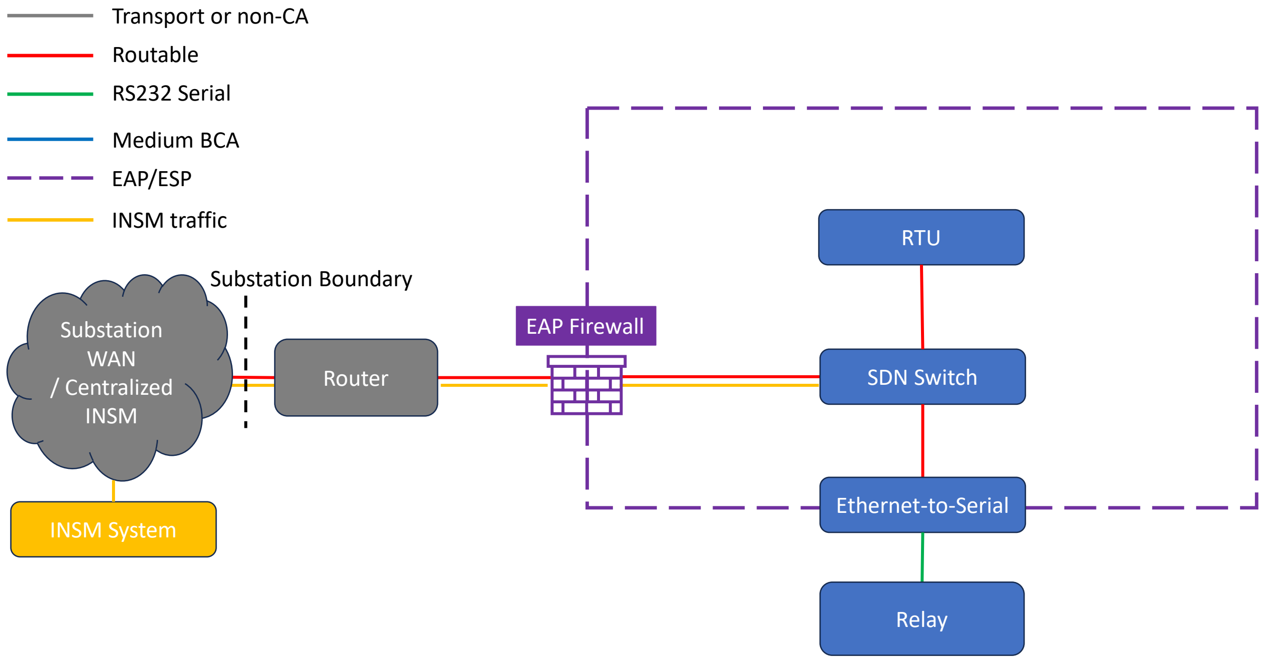


Figure 2: Substation Reference Architecture 2

Substation Reference Architecture 3

The substation network detailed below consists of a fully Ethernet network with two SDN switches capturing network activity on either side of the RTU. In this architecture, the RTU can function as a packet broker, capable of performing tasks such as deduplication, aggregation, traffic filtering, and compression to optimize bandwidth utilization to a remote INSM system.

A risk-based analysis shows that collection of INSM traffic through the SDN switches captures enough of the traffic to detect anomalous activity.

Depending on RTU capabilities and bandwidth limitations, the INSM system may need to be located within the substation with SPAN/mirror ports from each SDN going to the INSM system (see Substation Reference Architecture 8).

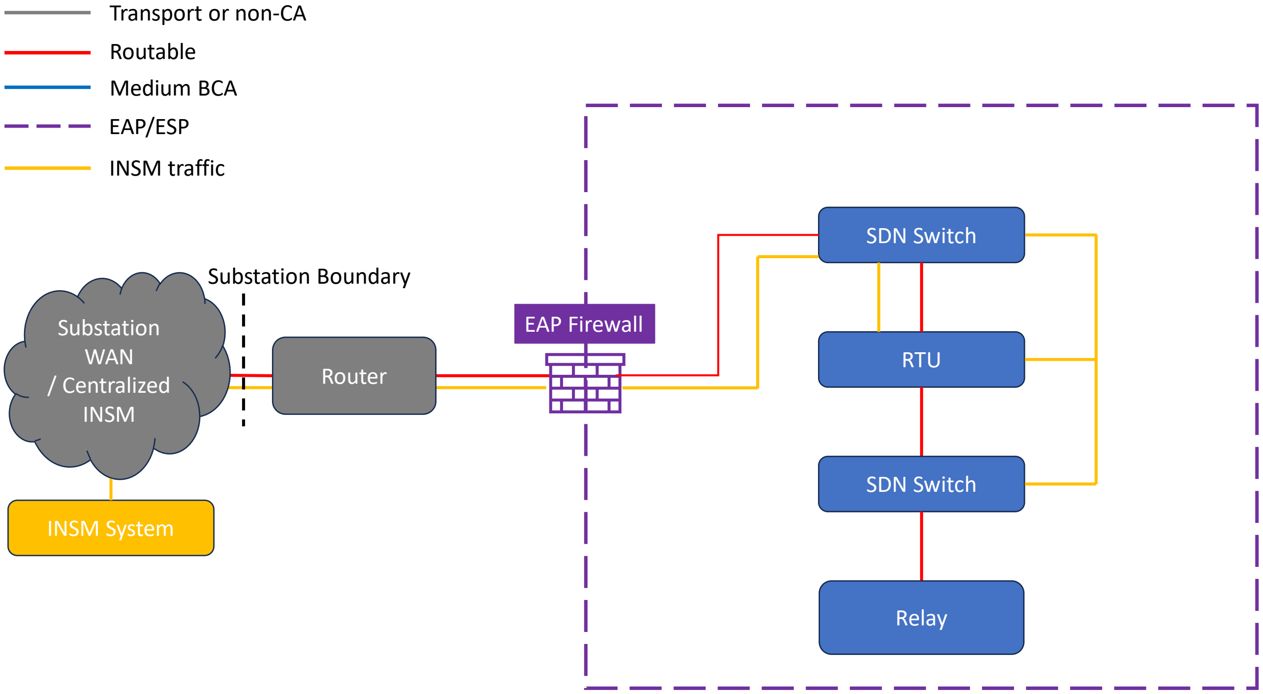


Figure 3: Substation Reference Architecture 3

Substation Reference Architecture 4

The substation network detailed below consists of an Ethernet RTU connected to an unmanaged switch with a mix of Ethernet and serial IEDs. Because the unmanaged switch is unable to SPAN / mirror network activity to the INSM system, taps must be installed on all Ethernet connections to medium impact BES Cyber Assets within the ESP.

A risk-based analysis shows that collection of INSM traffic at the tap points as shown captures enough of the traffic to detect anomalous activity.

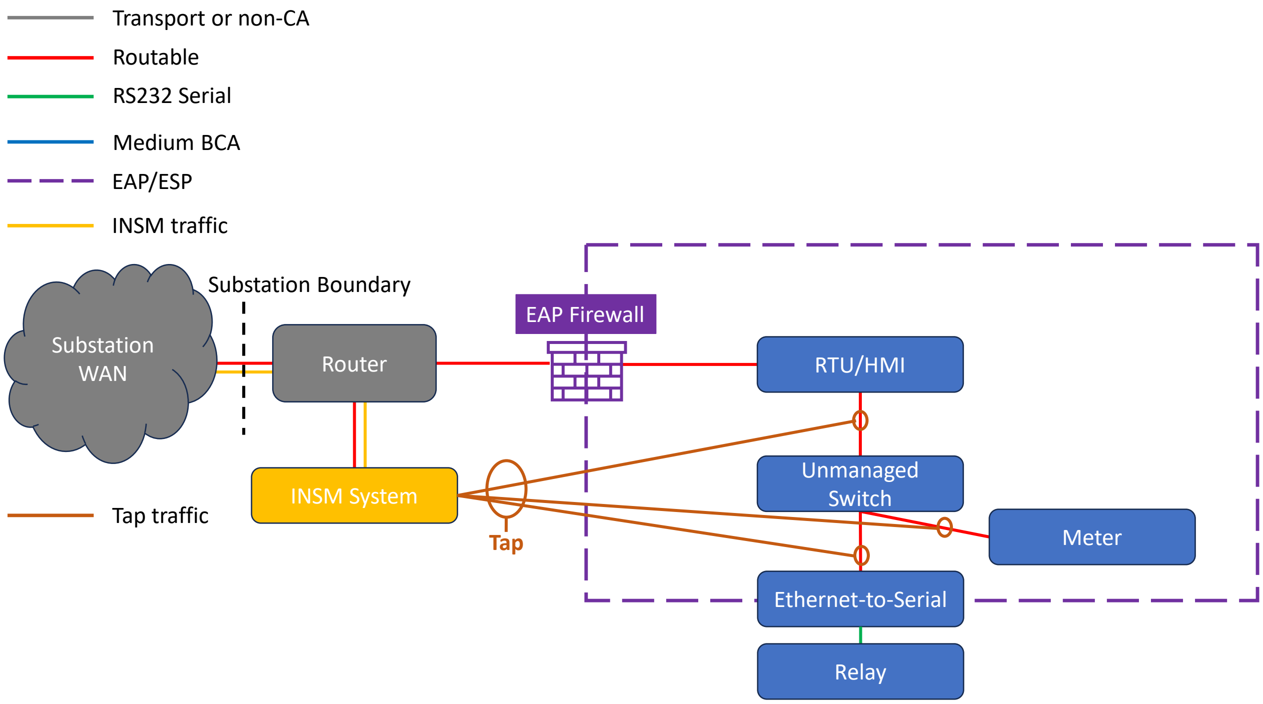


Figure 4: Substation Reference Architecture 4

Substation Reference Architecture 5

The substation network detailed below consists of a star topology with an unmanaged switch and a mix of Ethernet and serial relays and IEDs. Because the unmanaged switch is unable to SPAN / mirror network activity to the INSM system, TAPs must be installed on all Ethernet connections to medium impact BES Cyber Assets within the ESP.

A risk-based analysis shows that collection of INSM traffic at the tap points as shown captures enough of the traffic to detect anomalous activity.

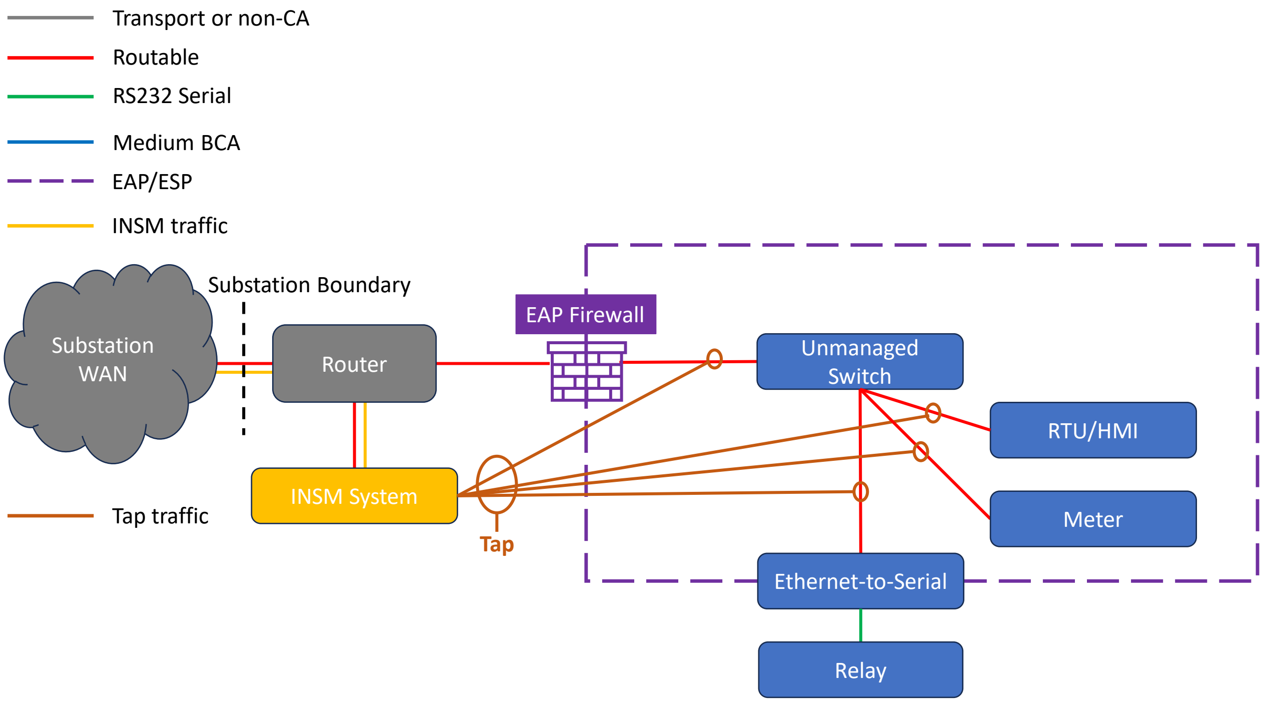


Figure 5: Substation Reference Architecture 5

Substation Reference Architecture 6

The substation network detailed below consists of an Ethernet RTU with direct serial communications to all the other medium impact BCAs.

A risk-based analysis would determine whether network activity within the ESP would allow for collection of east/west communication, making this architecture not applicable for INSM. In this scenario, anomalous network activity can be forwarded from the firewall up to a central INSM system. For scenarios where the EAP is not capable of monitoring network activity (the EAP is not a firewall), a network tap may be necessary to capture required traffic.

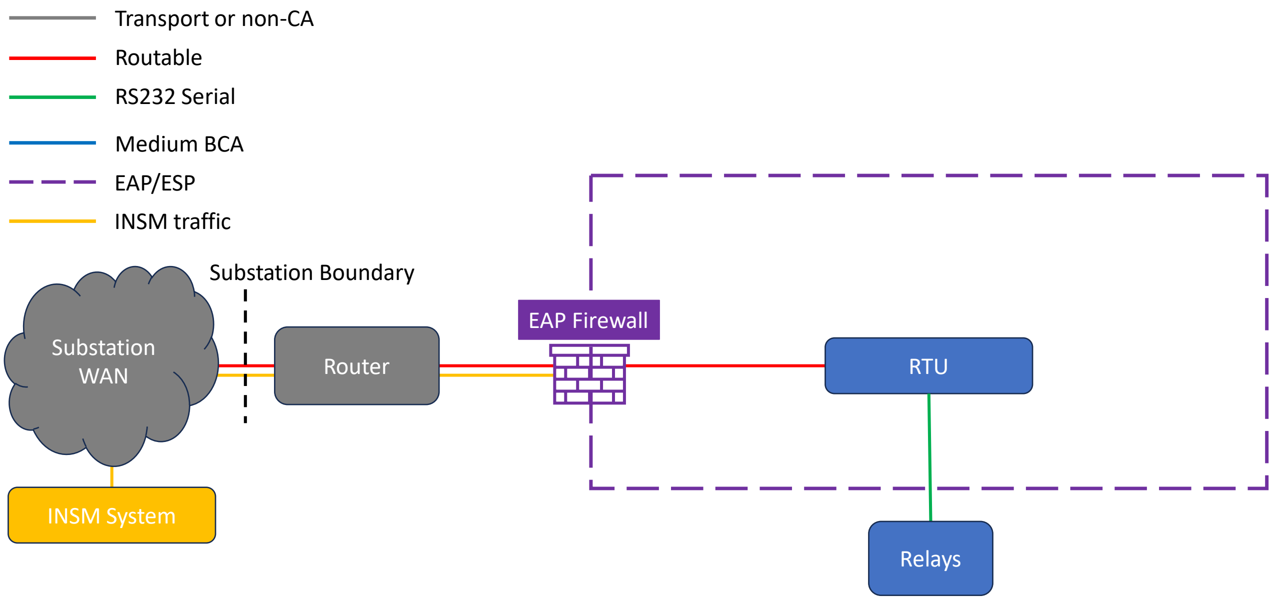


Figure 6: Substation Reference Architecture 6

Substation Reference Architecture 7

The substation network detailed below consists of a star topology using a managed switch. In this scenario, all Ethernet connected medium impact BCAs are connected directly to the managed switch, with the switch configured to SPAN/mirror traffic to a local INSM system.

A risk-based analysis shows that collection of INSM traffic at the managed switch captures enough of the traffic to detect anomalous network activity.

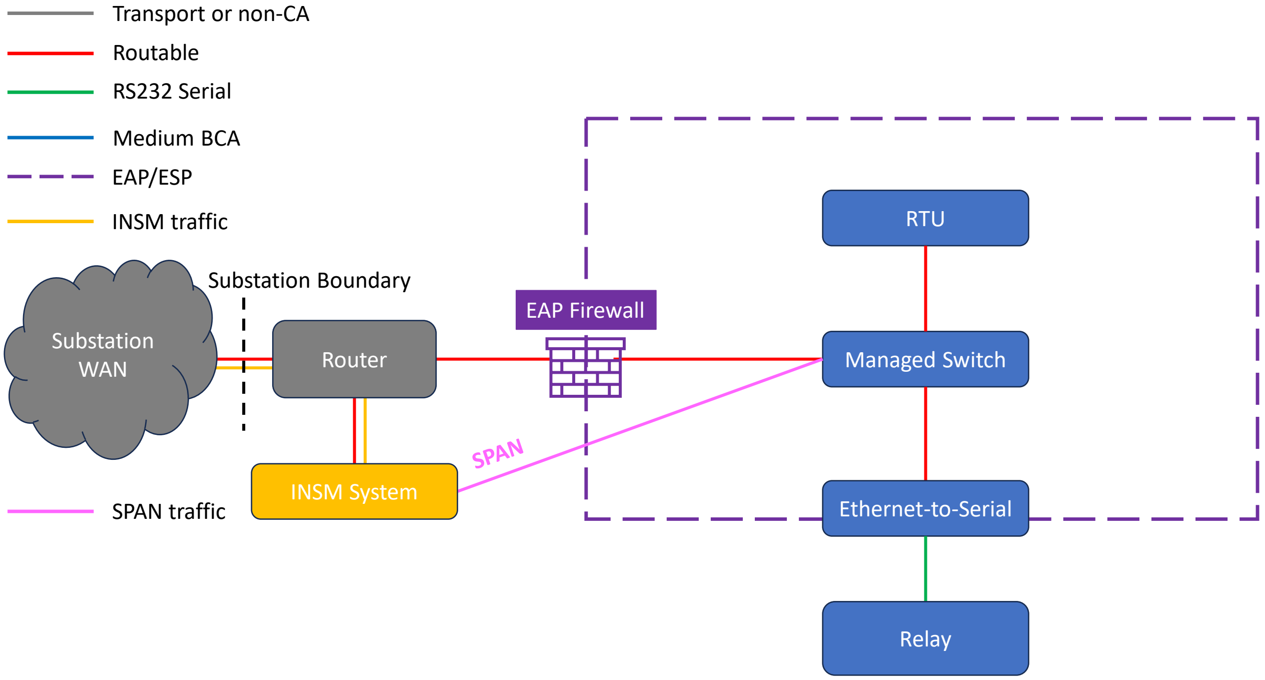


Figure 7: Substation Reference Architecture 7

Substation Reference Architecture 8

The substation network detailed below consists of a star topology using a managed switch. In this scenario, all medium impact BCAs are connected directly to the managed switch, with the switch configured to SPAN/mirror traffic to a local INSM system.

A risk-based analysis shows that collection of INSM traffic at the managed switch captures enough of the traffic to detect anomalous network activity.

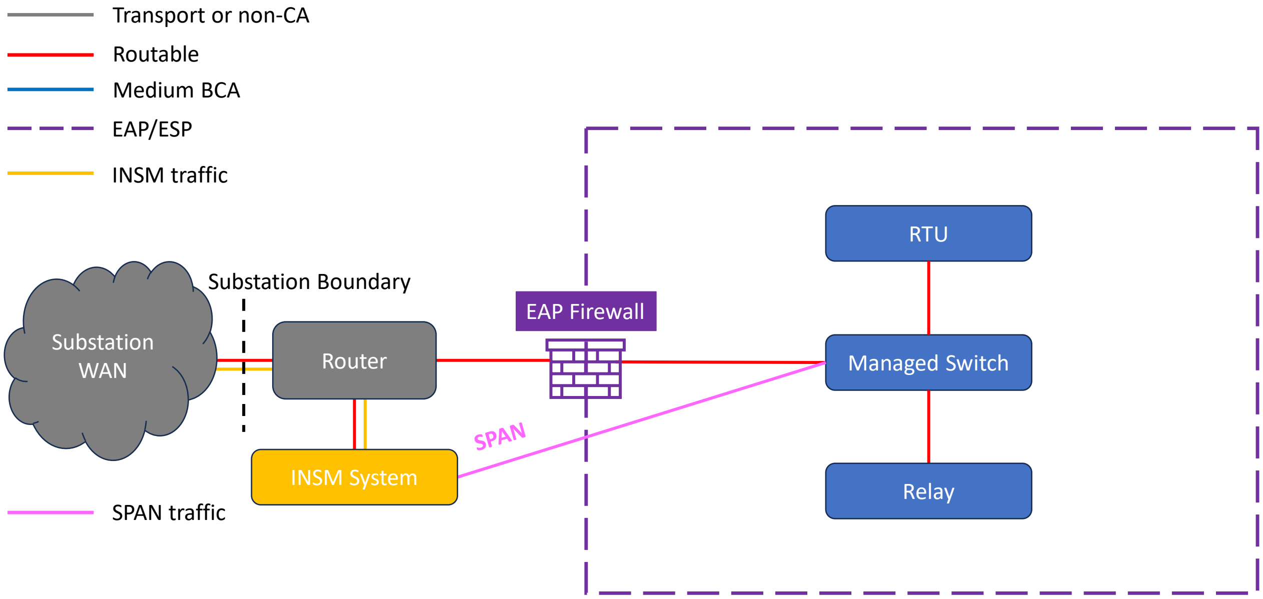


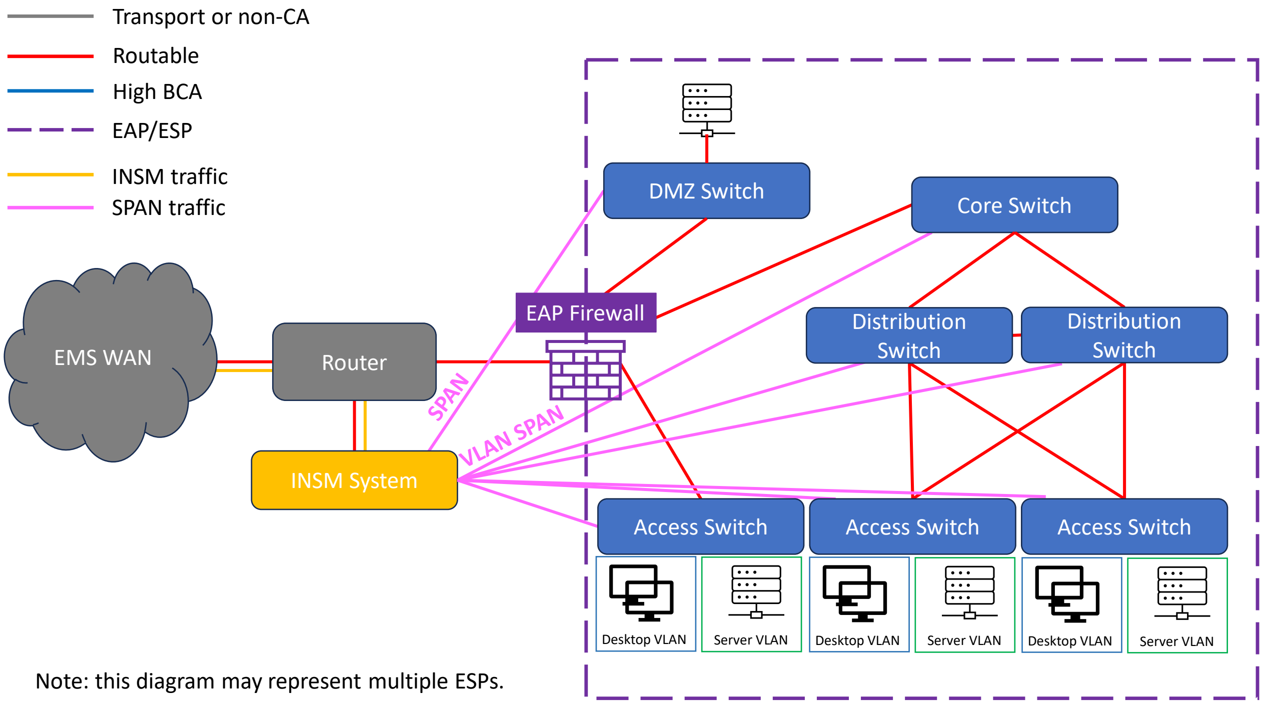
Figure 8: Substation Reference Architecture 8

Control Center INSM Architectures

The control center reference architectures below depict generalized views of a supervisory control and data acquisition system (SCADA) and could represent transmission management (usually energy management systems) or distribution management systems (DMS). The managed switches are configured with mirror / SPAN ports to forward traffic to an INSM system located at or near the control center.

Control Center Reference Architecture 1

A risk-based analysis shows that collection of INSM traffic would occur at all switches and captures all the traffic necessary to detect anomalous activity. See Appendix 1 for supplemental information regarding which VLANs to include or exclude.



Note: this diagram may represent multiple ESPs.

Figure 9: Control Center Reference Architecture 1

Control Center Reference Architecture 2

A risk-based analysis shows that a collection of INSM traffic would occur at all switches and captures all the traffic necessary to detect anomalous network activity. See Appendix 1 for supplemental information regarding which VLANs to include or exclude.

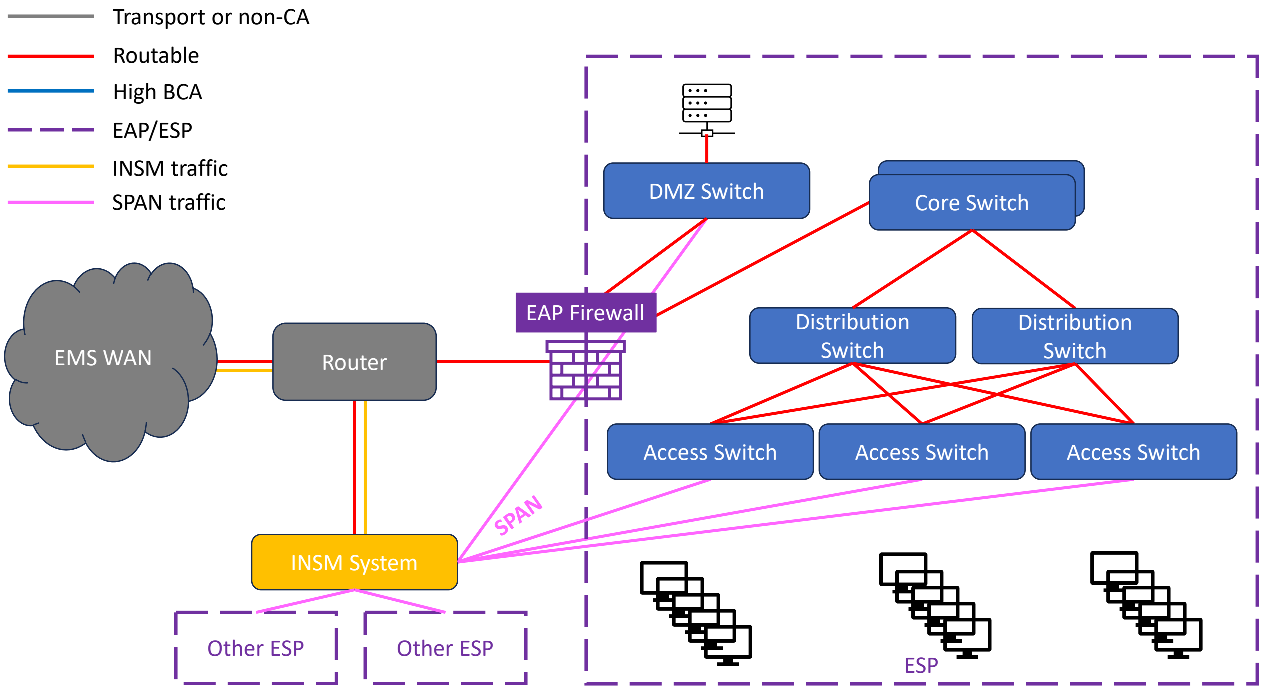


Figure 10: Control Center Reference Architecture 2

Generation INSM Architectures

The generation reference architectures below depict generalized views of distributed control systems (DCS) and associated balance of plant networks. The managed switches are configured with mirror / SPAN ports to forward traffic to an INSM system located at or connected to the generation plant.

Generation Reference Architecture 1

DCS traffic in this reference architecture is primarily multicast. Therefore, adding SPAN ports to access switching in the power blocks would create significant duplication of collected data. Plant operational procedures should also be considered. If operators regularly use remote HMIs for plant operations, then a risk-based analysis might conclude that collection of HMI traffic at an access switch is necessary; however if plant operations generally use only control room HMIs, then a risk-based analysis would likely conclude that collection at the core switches would capture enough traffic to detect anomalous activity.

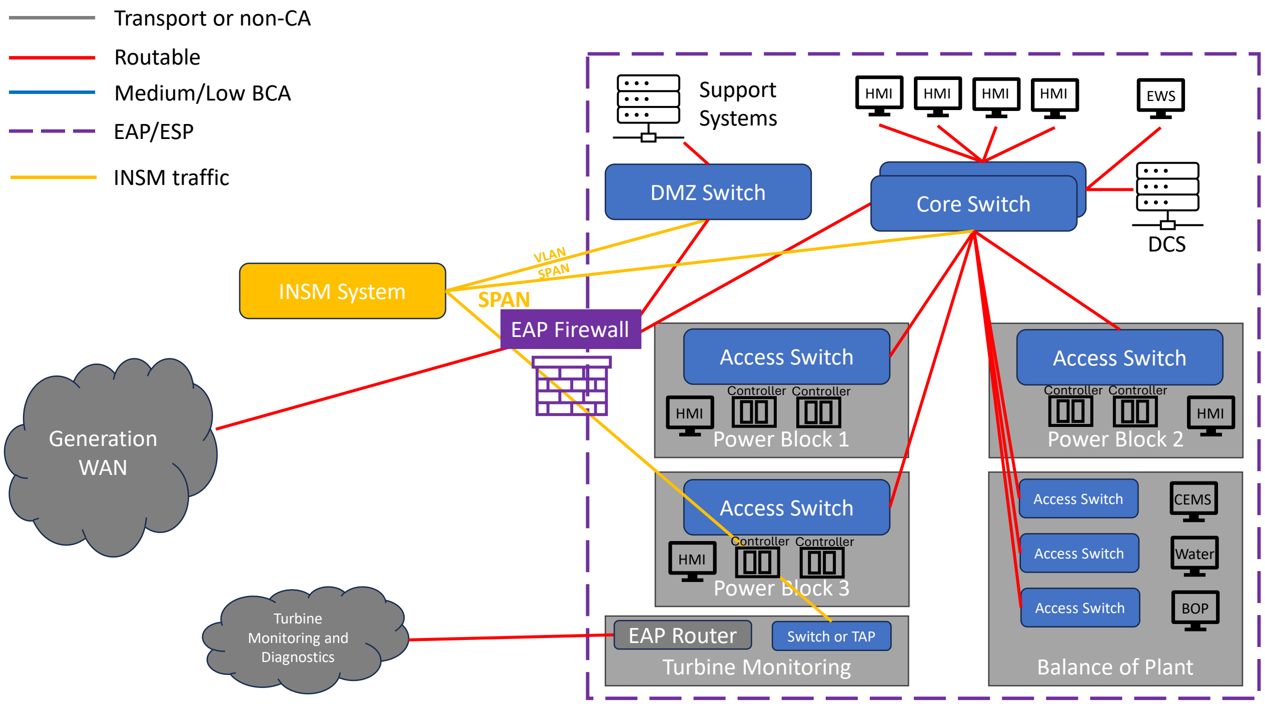


Figure 11: Generation Reference Architecture 1

Generation Reference Architecture 2

A risk-based analysis of generation reference architecture 2 would likely prioritize traffic collection from the plant network, DMZ switch, and turbine monitoring system. A risk-based analysis of the monitoring network which connects each unit network might show communication between various power blocks and balance of plant systems and might also be included in the data collection. Risk based analysis of each unit network, where traffic primarily consists of local broadcasts and multicasts, would likely result in a lower priority for collection.

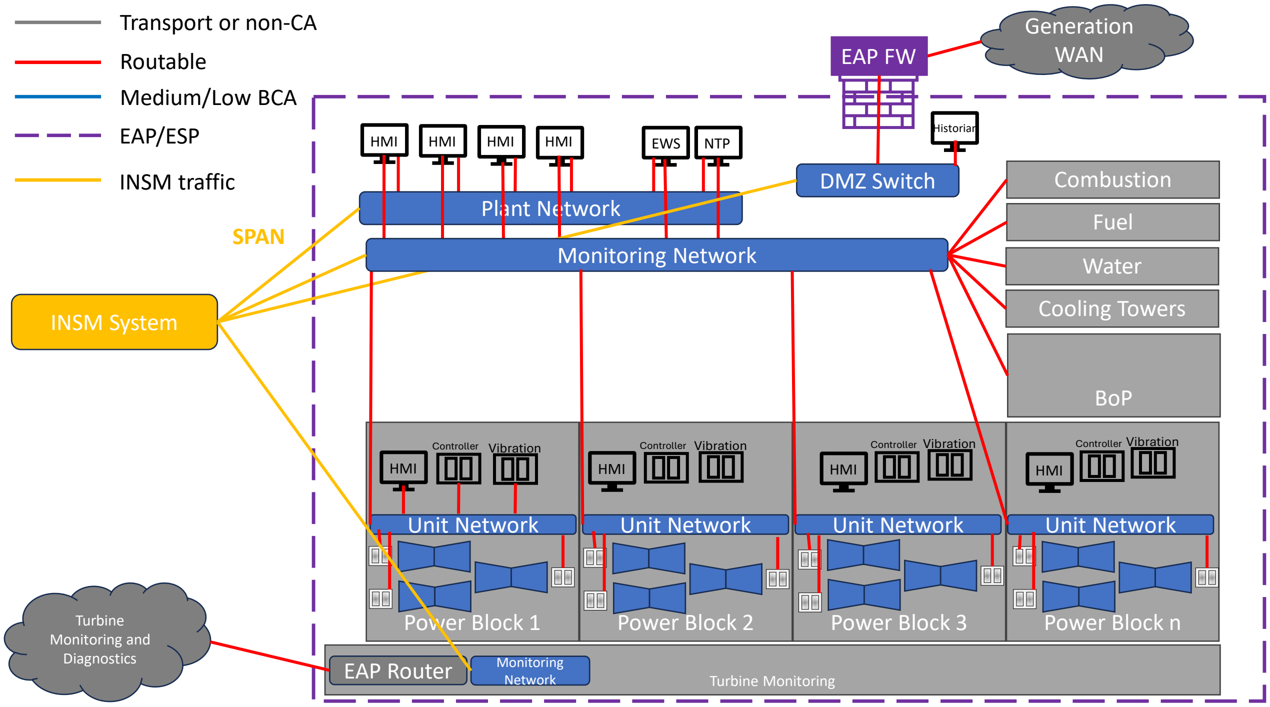


Figure 12: Generation Reference Architecture 2

Requirement R2.

Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain INSM data associated with network activity determined to be anomalous by the Responsible Entity at a minimum until the action is complete in support of Requirement R1, Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment].

Note: The Responsible Entity is not required to retain INSM data that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Requirement Guidance for R2.

It is recommended that the responsible entity determine which data and data types to store for short time frames, and which data types to store for longer periods of time, aligning to the entity's corporate incident response plan and records retention requirements. Table 1, adapted from [5], outlines retention considerations.

Table 1

Network Communication Data Type	Cyber Security Value Over Time	Retention Cost	Retention Timeframes or Number of Events to Retain
Network traffic: Full PCAP (payloads) (Recording all or most data on the network.)	Value diminishes quickly with time Encrypted payloads have little retention value	High	To be determined by Responsible Entity. This data, if retained at all, is expected to be retained for a short time.
Targeted PCAP (payloads) generated as part of an analysis or investigation. Targeted PCAP (payloads) related to or generated from an alert, notification, or event of interest. Network traffic records saved as part of an analysis or investigation.	Value diminishes slowly with time	Low	To be determined by Responsible Entity
Network metadata: Network connection data generated from PCAP Network flow data Network connection and session information	Value diminishes slowly with time	Low	To be determined by Responsible Entity

Network Communication Data Type	Cyber Security Value Over Time	Retention Cost	Retention Timeframes or Number of Events to Retain
Carved Files retrieved from PCAP	Malicious files have high value – other files have almost no value	Medium	To be determined by Responsible Entity
Hashes of carved files retrieved from PCAP	Maintains high value over time	Low	To be determined by Responsible Entity

Entities should also follow the Compliance Monitoring Process Section 1.2 Evidence Retention in CIP-015-1.

Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority (CEA) may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved, or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

Requirement R3.

Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect INSM data collected in support of Requirement R1 and data retained in support of Requirement R2 to mitigate the risks of unauthorized deletion or modification. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment].

Requirement Guidance for R3.

The entity must evaluate the INSM system against their CIP-002 and CIP-011 processes to determine if the system could be considered an EACMS or a BCSI repository.

The entity can implement PoLP (principle of least privilege) ensuring users, applications, and systems only have access to the resources and privileges necessary to perform their tasks.

Compliance with this requirement includes implementation of protective and detective controls. Examples of controls that could be considered to safeguard INSM data include:

- Granting only authorized personnel electronic and physical access to the INSM system
- Installing an INSM system with built-in methods that safeguard the integrity of stored data
- Segmentation of the INSM system into an isolated network separate from the BES Cyber System being monitored
- Authentication and authorization systems used by the INSM system could be maintained at a higher assurance level than corporate authentication systems or separated from corporate authentication systems
- Implement two-factor authentication for access to the INSM system
- Other commonly accepted methods used to protect log data

5. Periodic Review

The *NATF Document Procedure* provides instructions and requirements for developing, revising, marking, distributing, sharing, tracking, and retiring NATF documents consistent with NATF confidentiality policies and obligations.

The overarching purpose is to ensure strict control of NATF confidential information while allowing sharing of select, non-sensitive information outside the membership in a deliberate fashion, as approved and as needed, to advance the NATF's mission and vision. NATF Implementation Guidance documents and subsequent revisions are approved by the NATF board for Open Distribution to facilitate public posting of the guidance documents on the NERC public site.

The periodicity of review and revision history is set forth in the Version History section of this document.

6. References

[1] Federal Energy Regulatory Commission, "FERC Order 887," 19 January 2023. [Online]. Available: https://www.ferc.gov/media/e-1-rm22-3-000. [Accessed 11 June 2025].

[2] North American Electric Reliability Corporation, "CIP-015-1 - Cyber Security - Internal Network Security Monitoring," 9 May 2024. [Online]. Available: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-015-1.pdf. [Accessed 24 September 2025].

[3] North American Electric Reliability Corporation, "Implementation Plan Project 2023-03 Internal Network Security Monitoring (INSM) Reliability Standard CIP-015-1," April 2024. [Online]. Available: https://www.nerc.com/pa/Stand/Project_202303_INSM_DL/2023-03%20Implementation%20Plan%20FB%20clean.pdf. [Accessed 11 June 2025].

[4] Federal Energy Regulatory Commission, "E-2 RM24-7-000," 19 September 2024. [Online]. Available: https://www.ferc.gov/media/e-2-rm24-7-000. [Accessed 11 June 2025].

[5] North American Electric Reliability Corporation, "Technical Rationale for Reliability Standard CIP-015-1," 24 April 2024. [Online]. Available: https://www.nerc.com/pa/Stand/Project_202303_INSM_DL/2023-03%20Technical%20Rationale%20FB%20clean.pdf. [Accessed 11 June 2025].

Appendix 1: Risk Based Considerations

Appendix 1 lists several considerations that are applicable to R1.1 risk-based analysis. This table can be used to assess each potential data collection location (listed as “System Under Consideration”) to determine if that location has a high, medium, or low value of collection.

Collection locations could be a switch with no VLANs, a switch with VLANs, a tap, a subnet, a software defined networking channel, SPAN/mirror port, RSPAN, flow, or any similar data source.

System Under Consideration (SUC) **(Switch, tap location, subnet, VLAN, etc.)**	**Data Collection Value for Cyber Security**
SUC includes an EAP, remote access gateway, or Jump host	Very High
SUC includes an Engineering Workstations (EWS)	High
SUC includes traffic related to programming, loading, updating logic and control functions that is not collected from another SUC (e.g., an HMI used as an EWS)	High
SUC includes HMI(s) used regularly by Operations to control the process	High
SUC includes industrial protocols that are direct and unencrypted (e.g., DNP3, ICCP, NTP, telnet, ftp)	High
SUC includes non-critical protocols that are unencrypted and provide significant context for defenders (e.g., ARP, DNS)	High
SUC includes systems for which the entity needs to collect detailed asset information passively	High
SUC includes user interactive communications (e.g., RDP, SSH) that are not monitored using more detailed sources such as endpoint logs	High
Traffic, protocols, or endpoints that have been exploited by adversaries in publicized cyber-attacks at similar industries	High
SUC data primarily consists of broadcast/multicast protocols common in generation environments such as Foxboro, EGD, Ovation, and similar	First SUC: High Additional SUC: Low
SUC includes only HMIs used infrequently. (e.g., HMI in a PEECC used primarily for local view with control functions used during abnormal situations)	Medium
SUC includes two or fewer devices that regularly communicate using direct traffic (e.g., a switch with a single HMI and a PLC and the protocol in use requires a tcp handshake protocol)	Medium
Two or more devices that have user-interactive logon capability (e.g., keyboard and screen). Note: if the entity is monitoring endpoint logs of connected devices, INSM collection value may be lower	Medium
INSM system does not recognize the protocols or does not have alerts to detect common attacks that would occur in the SUC. Alternate controls (such as SIEM) are available that can detect anomalous activity	Medium
SUC includes two or fewer devices that do not communicate using direct traffic (e.g., a switch with a single HMI and a PLC and the protocol in use is a multicast/broadcast protocol)	Low

System Under Consideration (SUC) **(Switch, tap location, subnet, VLAN, etc.)**	**Data Collection Value for Cyber Security**
SUC includes two or fewer devices that do not communicate using direct traffic (e.g., a switch with a single HMI and a PLC and the protocol in use is a multicast/broadcast protocol)	Low
Traffic is collected (duplicated) in other systems such as firewalls or related INSM collection	Low
SUC includes user interactive communications (e.g., RDP, SSH) that are monitored using more detailed sources such as endpoint logs	Low
SUC consists of large packets with low security value (e.g., backups, vSAN, vMotion, SAN, video)	Flow data: Low Payload data: Very Low
SUC traffic that is encrypted or wrapped in encrypted protocols; note there is no CIP-015 requirement to decrypt encrypted traffic	Flow data: Low Payload data: Very Low

Appendix 2: Generation Reference Architecture 1

The DMZ switch(es) will probably contain some traffic that could be filtered from analysis. Appendix 1 includes considerations related to filtering traffic. These risk decisions could be informed by threat intelligence, detection capabilities of the INSM system, and other related factors.

This architecture depicts a remote turbine monitoring system. If such a system is in place, the traffic from the remote diagnostics center is likely high value for monitoring, especially if the monitoring service includes interactive remote access for turbine tuning.

Risk-based decisions related to collection from the access switches in each power block and balance of plant systems should include factors such as:

- How frequently the systems are used for plant operations
- Protocol characteristics (e.g., multicast communications)
- Number of devices connected to each access switch (in situations where a switch has only two devices such as an HMI and a controller, collection from that switch may not add appreciable detection capability. However, if multiple devices with interactive logon capabilities are connected to the switch, then traffic collection may improve the situational awareness and may increase detection capability.)
- INSM system capability to deduplicate traffic. In DCS systems that rely on multicast and broadcast protocols, collection of traffic from multiple switches may require that the INSM system has deduplication capabilities

Appendix 3: Generation Reference Architecture 2

DCS traffic in this reference architecture is primarily multicast. Therefore, adding SPAN ports to Unit networks in each power block would not collect much additional data over and above collection from the monitoring network and would create significant duplication of collected data. Plant operational procedures should also be considered. If operators regularly use remote HMIs for plant operations, then a risk-based analysis might conclude that collection of HMI traffic is necessary. However, if plant operations generally use only control room HMIs, then a risk-based analysis would likely conclude that collection at the plant network and monitoring network switches would capture enough traffic to detect anomalous activity.

The DMZ switch(es) will probably contain some traffic that could be filtered from analysis. Common VLANs that would be excluded from collection would be backup traffic. A risk-based analysis could identify other traffic to be excluded from collection such as repeated pings from a monitoring system, virtualization, or storage area network traffic. These risk decisions could be informed by threat intelligence, detection capabilities of the INSM system, and other related factors.

This architecture depicts a remote turbine monitoring system. If such a system is in place, the traffic from the remote diagnostics center is likely high value for monitoring, especially if the monitoring service includes interactive remote access for turbine tuning.

Risk-based decisions related to collection from the switches in each power block and balance of plant systems should include factors such as:

- How frequently the systems are used for plant operations
- Protocol characteristics (e.g., multicast communications)
- Number of devices connected to each access switch (in situations where a switch has only two devices such as an HMI and a controller, collection from that switch may not add appreciable detection capability. However, if multiple devices with interactive logon capabilities are connected to the switch, then traffic collection may improve the situational awareness and may increase detection capability.)
- INSM system capability to deduplicate traffic. In DCS systems that rely on multicast and broadcast protocols, collection of traffic from multiple switches may require that the INSM system has deduplication capabilities