
Reliability & Security
Workshop
WECC
March 17–18, 2026
San Diego, California

Internal Network Security Monitoring (INSM)

Morgan King
CIP Senior Technical Advisor

Electric Reliability & Security for the West

March 18, 2026

Agenda

- Defining INSM (CIP-015-1 Overview)
- The Shift to Internal Security: Why it Matters
- Requirements (R1, R2, R3)
- Implementation Roadmap and Timelines

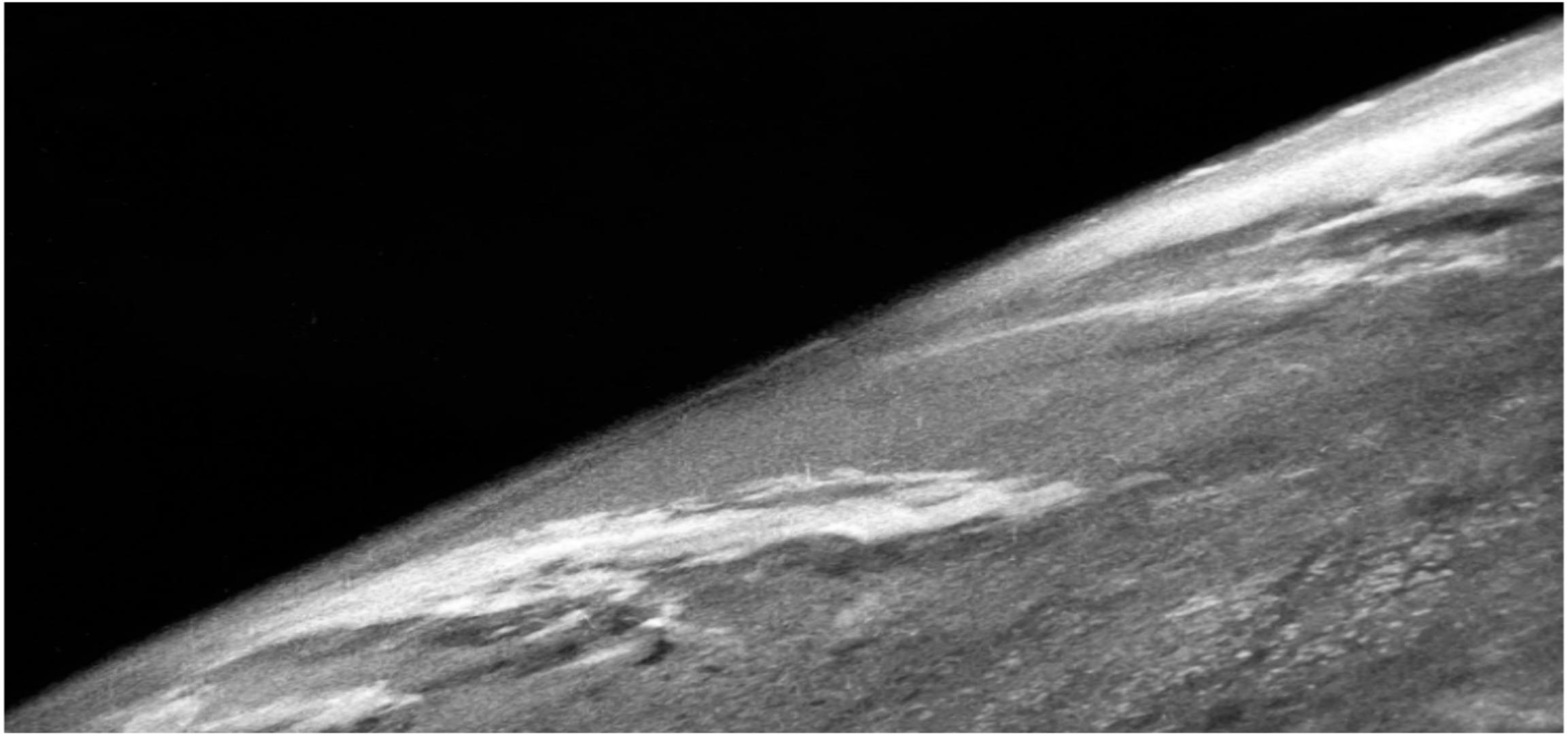
V-2 No.13

V-2 BEING PLACED in POSITION for FIRING 10 May 1946

U.S. Army Ordnance Proving Ground, White Sands, N.M.

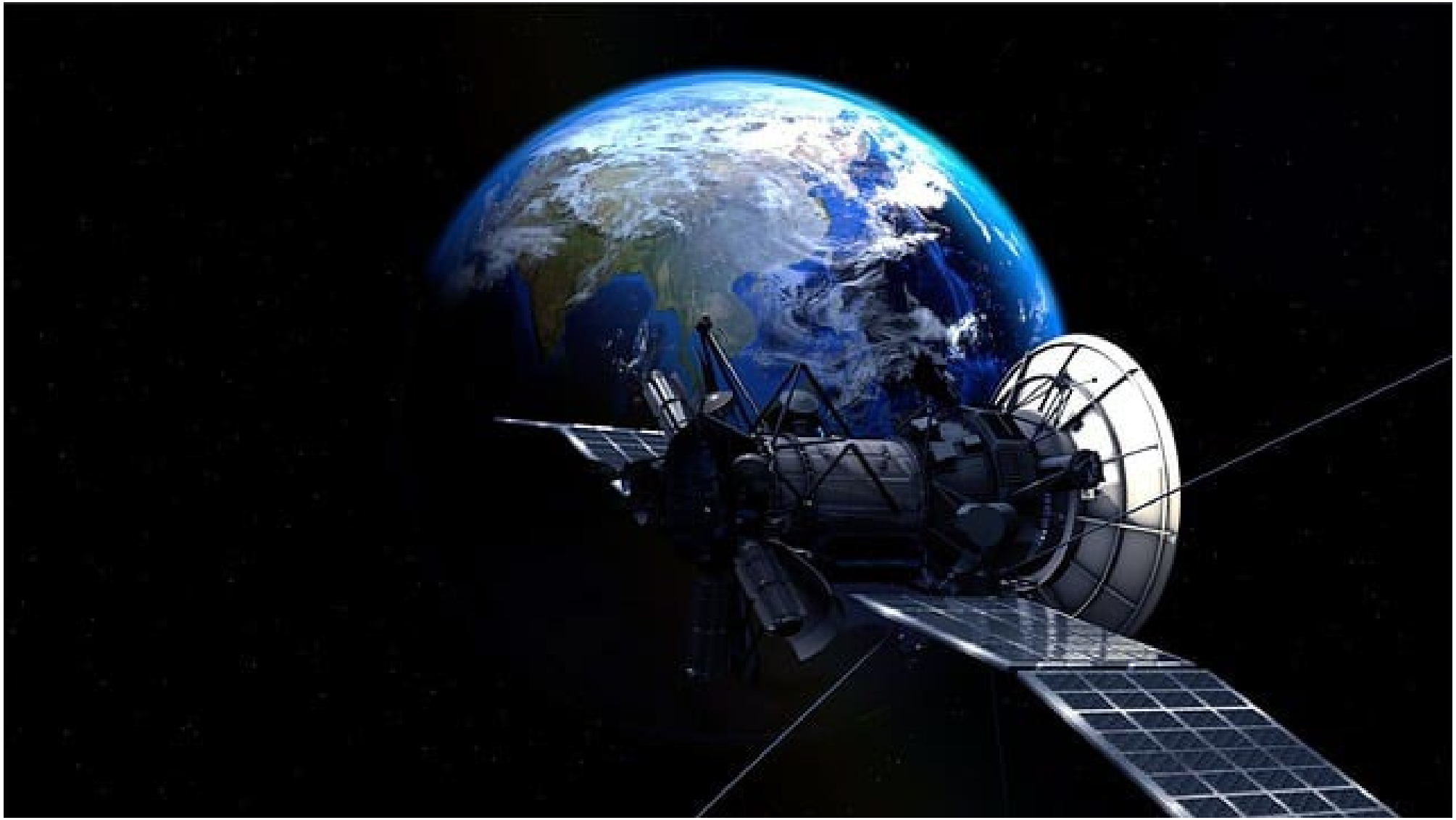
https://www.historyofinformation.com/image.php?id=8067

Dawn of System-Wide Visibility



https://www.historyofinformation.com/image.php?id=8063

Beyond the Perimeter



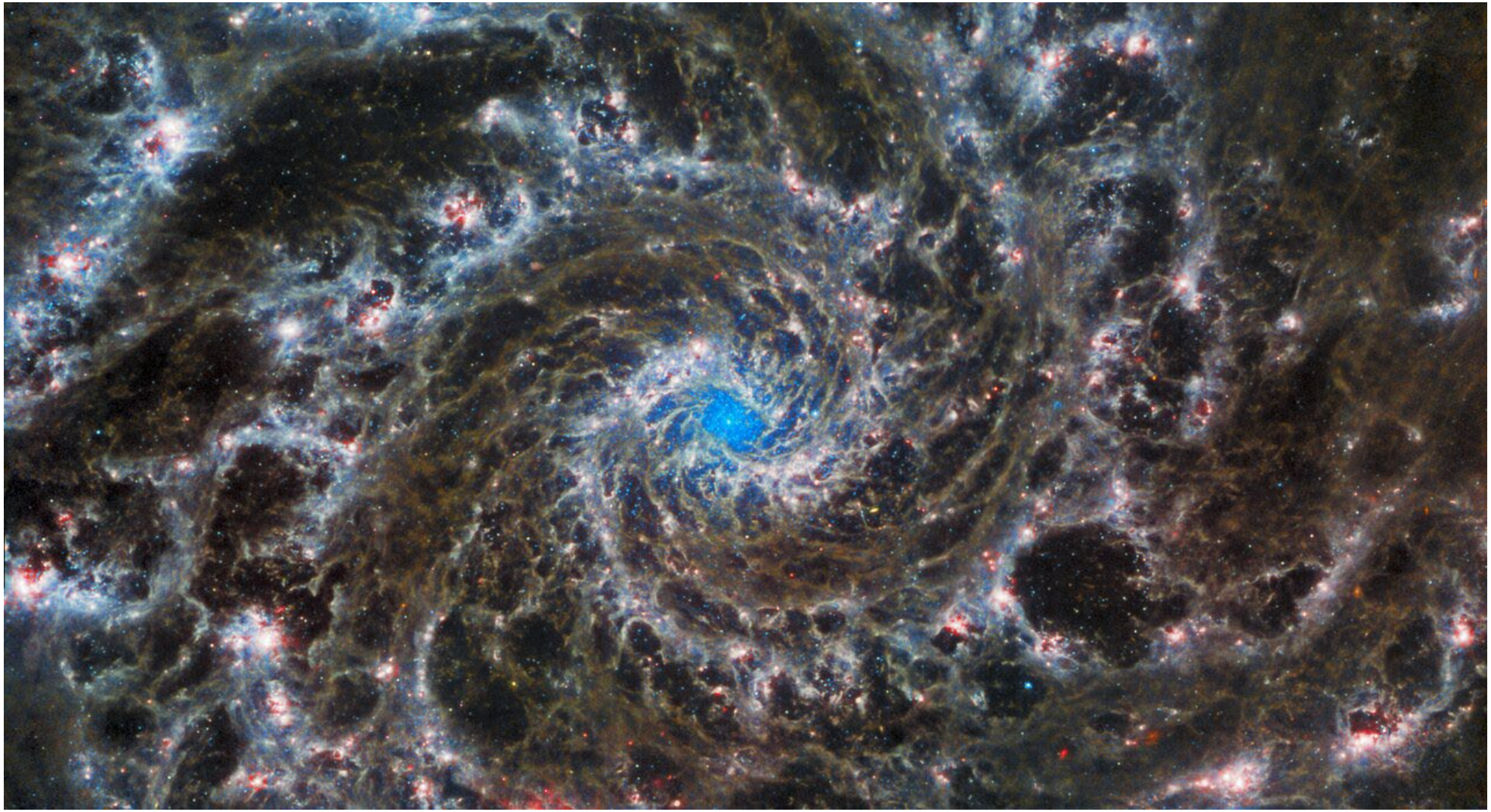
https://www.iot-now.com/2024/06/14/144921-the-evolution-of-satellite-technology-from-sputnik-to-starlink/

“Walled Garden"

"Snapshots" to Sentinel

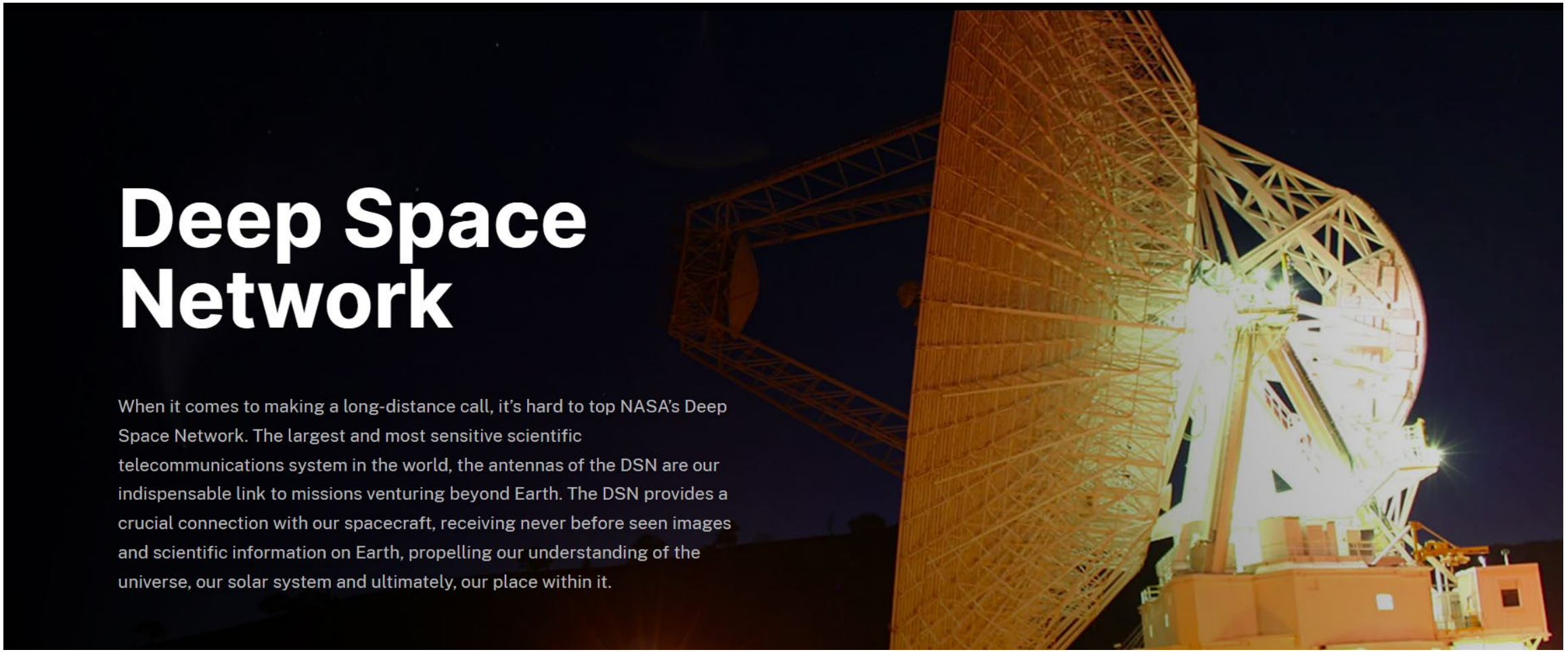
- Space Imagery
  - Blurry, static glimpses of Earth.
    - See the "outline," but not the activity.
  - Corona Missions
    - The Cold War era introduced photo spy satellites.
    - Specialized sensors for nuclear detonation detection.
  - Landsat 1
    - Monitor Earth's natural resources, land use, and environmental changes.
    - No visibility until the next scheduled orbit.
- Network Monitoring
  - Traditional monitoring was a digital Snapshot
    - Static dashboards and predefined thresholds (e.g., "Is the server up?").
    - Tools used SNMP and basic logs to check system "pulse" at set intervals.
    - Point-in-time, perimeter logs (firewall block/allow).
    - Single device logs
    - Isolated views

Persistent High-Definition



https://esawebb.org/images/potm2208a/

Deep Observability



https://www.nasa.gov/communicating-with-missions/dsn/

Looking to Observing

- **Space Monitoring**
  - Seeing an object and understanding its behavior
  - “Living map" that tracks change over time rather than just single moments
  - Deep space probes detection of subtle gravitational shifts
  - Deep Space Network (DSN)
    - The NASA Deep Space Network doesn't just "see" spacecraft; it maintains a persistent, complex communication link that tracks health, trajectory, and intent across billions of miles
  - Move from seeing the surface to understanding the core
- **Network Monitoring**
  - Beyond standard telemetry (logs/metrics, and traces) to network intelligence (packet flows and correlation)
  - Continuous line-of-sight into all east-west traffic, allowing for real-time anomaly detection

U.S. Effective Date

October 1, 2028

High and Medium Impact BES Cyber Systems at Control Centers w/ERC

U.S. Effective Date

October 1, 2030

All other Medium Impact BES Cyber System w/ERC

Cyberattack on Poland's DER

- Coordinated destructive campaign against critical energy infrastructure occurred on December 29, 2025, during a period of severe winter weather in Poland
- Affecting over 30 renewable energy facilities and a major combined heat and power (CHP) plant
- A custom wiper malware dubbed DYNOWIPER was used to irreversibly destroy data across compromised networks
- CERT Polska attributed the attack infrastructure to the threat cluster Static Tundra, which is also tracked as Berserk Bear, Blue Kraken, Crouching Yeti, Dragonfly, Energetic Bear, Ghost Blizzard (formerly Bromine), and Havex.
  - Static Tundra is assessed to be linked to Russia's Federal Security Service's (FSB) Center 16 unit.
  - Recent reports attributed the activity with moderate confidence to a different Russian state-sponsored hacking group known as Sandworm.

Cyberattack on Poland's DER

- The attack caused a "loss of view and control" for operators, who were unable to remotely monitor or manage the affected facilities.
- Some operational technology (OT) equipment, including RTU controllers from Hitachi, Mikronika, and Moxa, was damaged beyond repair, requiring physical replacement.
- The threat actor reportedly gained initial access through Fortinet FortiGate devices prior to December 29, exploiting.
  - VPN interfaces allowing authentication without multi-factor authentication
  - Reused credentials across multiple facilities
  - Historical vulnerabilities in unpatched devices

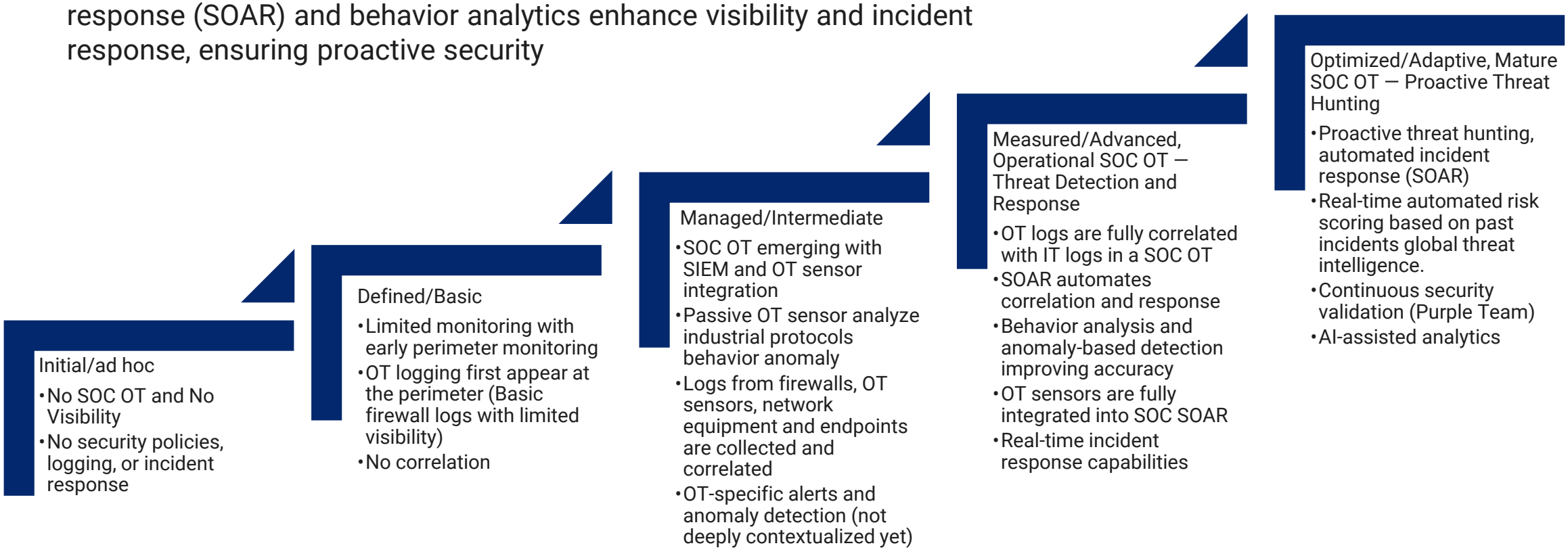
Defining INSM

- Assume breach, detect movement, and reduce dwell time
  - Bypass perimeters using valid credentials
  - Exploit trusted third-party connections
  - Traverse internal routing paths undetected
  - Weaponize normal operational protocols
- Post-compromise detection
  - IOC & IOA
  - Verification of suspicious activity
  - Forensic visibility
  - Timeline reconstruction
  - Evidence to validate

ICS Monitoring Maturity Lifecycle

Ability to detect and respond to OT threats evolves with maturity

1. At early stages, perimeter logs and sensors provide isolated insights
2. True detection begins with correlation and SIEM integration
3. As SOC OT capabilities mature, advanced correlation, automated response (SOAR) and behavior analytics enhance visibility and incident response, ensuring proactive security



https://www.cs2ai.org/

People, Process, Technology

- Collaboration, Coordination, Cooperation
  - What stakeholders configure and manage of ESP environment?
  - Who will be performing monitoring for CIP-015?
    - INSM tools deployed may be new to some SMEs
- Installation of new hardware
  - Procurement, installation, configuration and change management, etc.
- What does compliance evidence need to include?

Scope

- CIP-015-1, R1
  - Each Responsible Entity shall implement one or more documented process(es) for internal network security **monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable** Connectivity to provide methods for detecting and evaluating anomalous network activity.
- CIP-015-1 FAQ
  - EACMS and PACS **not protected by an entity's defined ESP** are outside the scope of Project 2023-03 INSM.
  - Entities **that choose** to protect EACMS, PACS, and PCAs with a defined ESP should consider network traffic from those systems to be in scope for proposed Reliability Standard CIP-015-1, Requirement R1.

Scope

- FERC order 907 states
  - " … the scope of CIP-networked environment includes the systems within the electronic security perimeter *and* one or more of the following: (1) network segments that are connected to EACMS and PACS outside of the electronic security perimeter; (2) network segments between EACMS and PACS outside of the electronic security perimeter; or (3) network segments that are internal to EACMS and PACS outside of the electronic security perimeter."
- CIP-015-2 SAR
  - FERC Order No. 9071 directs NERC to develop modifications to Reliability Standard CIP-015-1 to extend internal network security monitoring (INSM) to include Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) **outside of the Electronic Security Perimeter (ESP).**

Risk-based Rationale

- Monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s)
  - "Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications."
- What, Where, Why, and How
  - The risk-based rationale should include why an entity chose to monitor specific ESP networks as well as rationale to support not monitor other networks protected by an ESP.
- Establish asset inventory where collection is available
  - Types of assets/data available
  - Physical, passive, active, configuration analysis
- Risk analysis / Impact analysis
  - Analysis of common adversarial techniques
    - Annual risk report
    - Top 10 threats and trends

Anomaly-based Detection Methods

Detection Type	Category	Primary Logic	Strengths	Limitations	Example Use Cases
Modeling Detections	Anomaly-based (Baseline-driven)	Establish a "single source of truth" for normal network behavior.	Detecting obvious anomalies, volumetric attacks (DDoS), or unauthorized changes in baseline traffic patterns.	Requires accurate baseline; tuning period	- Unusual DNP3 function codes - New periodic communication between devices that never talk - Sudden increase in traffic pattern - Controller begins sending commands at abnormal timestamps
Configuration Detections	Anomaly-based (Environment-driven)	Detect unauthorized or unexpected device, addressing, or topology changes	Catching rogue or misconfigured assets	Alerts require validation after legitimate configuration changes	- New MAC address appears in a substation switch CAM table - Change in routing path to a relay - New VLAN tag seen entering the ESP - A device changes its IP address

Threat-based Detection Methods

Detection Type	Category	Primary Logic	Strengths	Limitations	Example Use Cases
Threat Behavior Detections	Intelligence-driven (TTP-based)	Detect actions consistent with adversary techniques (OT reconnaissance, lateral movement, manipulation-of-control)	Detects campaigns, not just signatures; resilient to obfuscation	Requires continuous threat research; context needed to reduce FP	- Ladder logic download outside maintenance window - Unauthorized read/modify commands to PLC - Enumeration of IEDs or relays using ICS scanning tools - Multi-stage ICS kill chain activity (recon → manipulation)
IoC Detections	Intelligence-driven (Signature-based)	Match known malicious IPs, domains, file hashes, or payloads	High-confidence alerts with strong clarity	Blind to novel attacks; requires frequent updates	- Known ICS-targeting malware signature (e.g., packet-level pattern match) - Traffic beaconing to a known malicious IP/domain - OT host contacting known adversary infrastructure - Packet payload match indicating known exploit

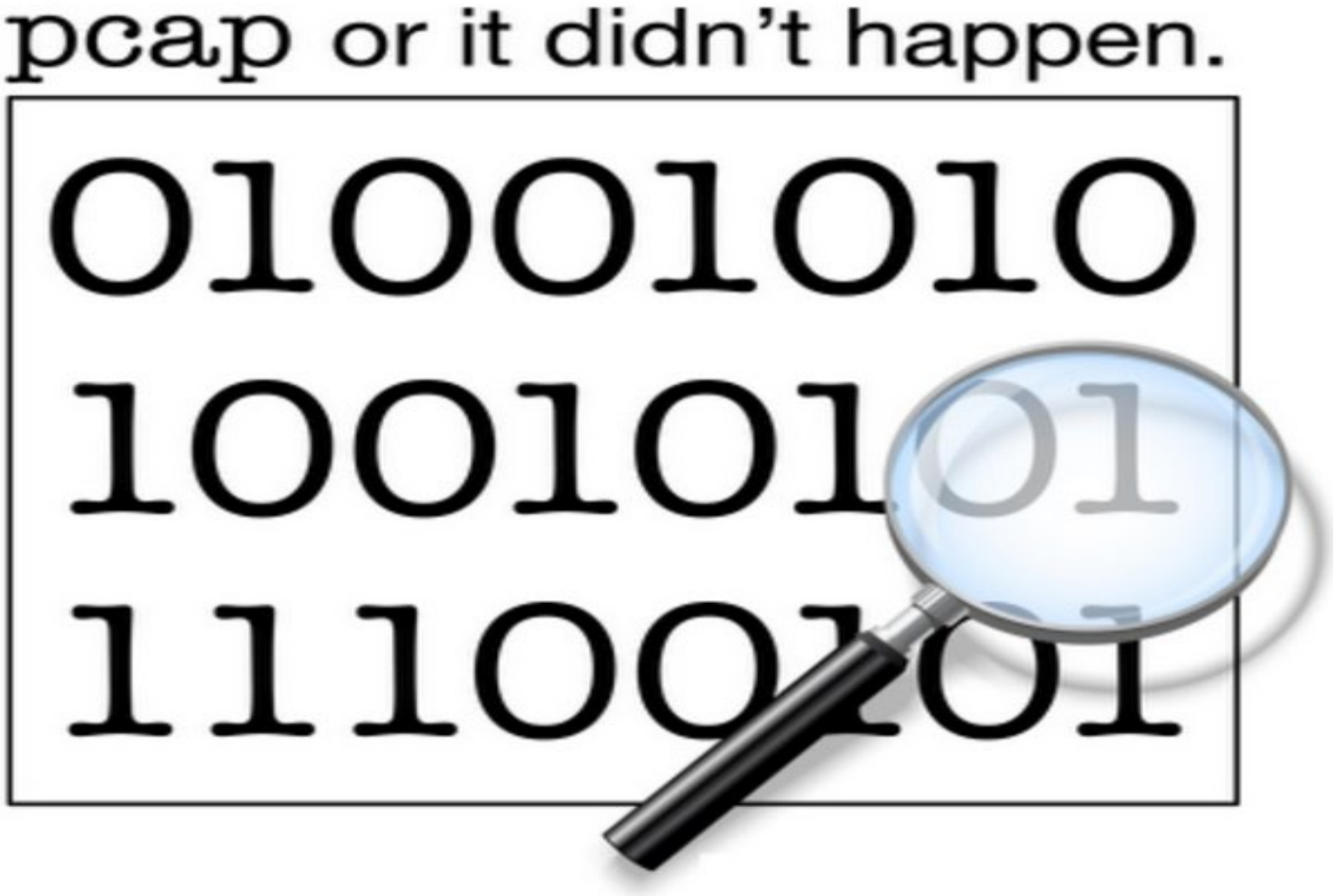
Monitor Network Activity

- Define and Map ESP Network Segments and Data Collection Points
  - Identify and Select High-value Data Sources
  - Implement a Risk-based Data Selection Strategy
    - Energy management system (EMS) or distributed control system (DCS) server(s) and workstations, third-party connections, traffic associated with authentication servers
    - Active Directory or two-actor authentication systems, and programmable logic controller (PLC)/remote terminal units (RTU) communication paths
  - Contextual Filtering
    - Backup traffic
    - Encrypted connections

Data Collection Methods

Monitoring Method	Strengths	Limitations	Use Case
SPAN Port	Flexible, low-cost, simple to deploy; mirrors specific ports/VLANs; no physical changes required	May drop packets under load; can be disabled via config; depends on switch CPU	Access/distribution layers with moderate traffic; environments needing rapid deployment
Network TAP	Packet-accurate visibility; tamper-resistant; does not drop packets; ideal for OT protocol inspection	Requires physical installation; cost; potential outage to insert	High-assurance monitoring of core or high-value ESP links; substations; high-speed links
Aggregation Device / Packet Broker	Centralizes multiple feeds; filters, deduplicates, load balances; scalable	Added complexity and cost; becomes a critical asset to secure	Large ESP environments with multiple sensing points requiring consolidation
Endpoint Telemetry	Provides host-level visibility; detects process, auth, and local anomalies; complements network monitoring	Requires agents; does not replace network-layer requirements	Validating network anomalies; encrypted east–west traffic visibility
Passive Network Sensor	No interference with traffic; perform deep packet inspection on mirrored/TAP feeds; detect OT protocol anomalies, timing irregularities, unauthorized command sequences; easy to scale by adding sensors at each segment	Dependent on input quality — SPAN drops affect fidelity; require proper placement (visibility gaps possible); may struggle with encrypted payloads; require compute/storage for analysis; Cost of managing	Monitoring OT/ICS protocols at substation LANs, distribution networks, or critical ESP segments; works best when fed by reliable TAPs or high-quality SPANs

Network Communication Data Type



Network Communication Data Type

Data Type	Strengths	Limitations	Use Case
PCAP	Full packet capture enables forensic reconstruction, payload inspection, replay analysis, and deep protocol validation; high-fidelity data for unknown threat detection' essential for post-incident investigation, including Misoperation	High storage requirements; may require filtering to manage volume; encrypted traffic reduces analytical value' ongoing management and retention needed	Forensic-quality INSM monitoring on critical OT segments' short-term rolling capture on high-value control networks' detailed analysis of protocol misuse, ICS command manipulation, or zero-day behavior
Flow Data (NetFlow/IPFIX/sFlow)	Lightweight; low bandwidth; excellent for behavioral/connection monitoring; scalable; effective for asset inventory	No payload; limited OT protocol insight; cannot detect malformed packets; lacks deep packet inspection (DPI) for payload analysis, offering limited forensic detail for OT-specific protocols	Broad network visibility; low-bandwidth sites; supplement to packet inspection;
Network Metadata	Offers a balance between the context of full packets and the efficiency of flow data; ideal for identifying behavioral anomalies.	Can miss subtle, obfuscated attacks that are hidden deep within payload content.	Monitoring DNS abuse, identifying invalid SSL/TLS certificates, and identifying user-agent strings indicative of attacks.
Log Data	Provides detailed, contextual information from the perspective of the application or security device itself.	Often scattered across many systems, requiring central management (SIEM) to be effective.	Investigating brute-force attacks (authentication logs), firewall policy violations, and auditing user behavior.

Monitoring Data Sources

- A variety of sources from strategic network locations
- Identify broad data feeds and then narrow the focus to collect the data
- Context surrounding a notification/detection to help with analysis and incident response
- Layered anomaly detection methodologies to drive resilient security posture rather than focusing on just baselines

Human-in-the-loop (HITL)

- Automated
  - Using automation to analyze traffic over a specific period
  - Build baseline rules based on that traffic
  - Faster and generally includes more granular rules
  - Learning window matters
    - May depends on the objective, storage, and size of the control environment
  - May accidentally learn unwanted behavior if the automation looks back over too long
  - Understanding change cycle for the site/zone a baseline is created to ensure baseline period
- Manual
  - Human analysis and expertise
  - Tune more specific over time
  - Knowledgeable about the assets in environment, typical change cycles, and have a dedicated focus on tuning

Detect Anomalous

- Point Anomalies
  - A single data point that stands out significantly from the rest
- Contextual Anomalies
  - A data point that is unusual within a specific context but may be normal elsewhere
- Collective Anomalies
  - A group of data points that, when viewed together, indicate an anomaly
- Anomalous based on a comparison with the INSM system’s patterns of expected network behavior
  - Unauthorized activity, connections, devices, and software.
  - Detected events
  - Configuration settings
  - Network communication baseline used
  - Other methods

Evaluate Anomalous

- Document method(s)
  - Establish approach and procedure(s) for collection, detection, and evaluation
- Documented classification of anomalies
  - Define what constitutes an anomaly and categorize different types of deviations
- Triage workflow
  - Outline the specific steps for the initial sorting and prioritization of detected anomalies
- Threat intelligence analysis
  - Apply external data and context to understand the nature of the detected activity
- Classification Metrics
  - True Positive: Confirmed anomalous activity that is malicious or relevant
  - False Positive: Activity incorrectly flagged as an anomaly
  - True Negative: Normal activity correctly ignored (often used for baseline validation)
  - False Negative: Malicious activity that was missed by the system

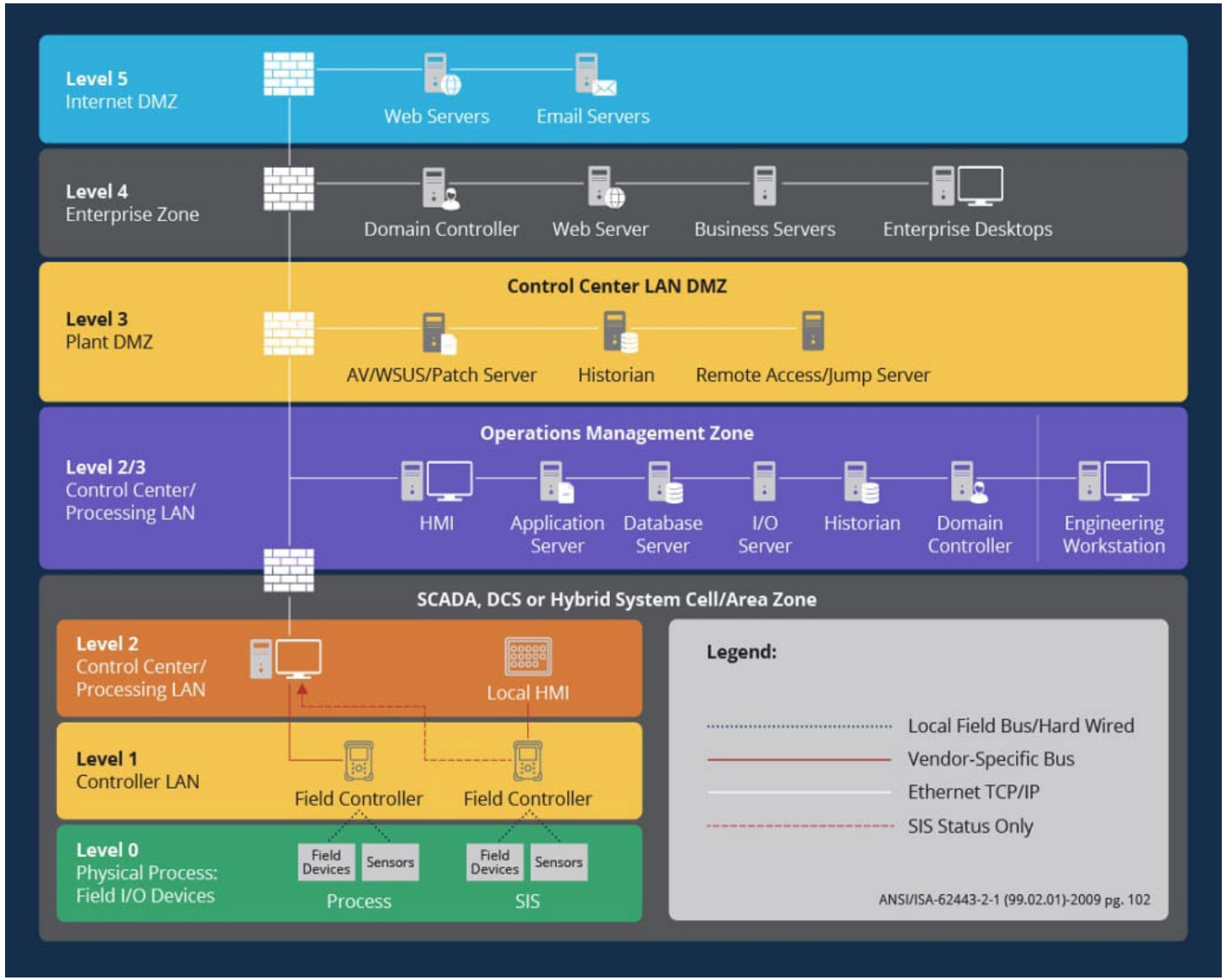
Evaluate Anomalous

- Severity level of scanning tool
  - Evaluate whether the detection settings are tuned correctly based on the classification results (e.g., if there are too many false negatives)
- Escalation process(es) that could include CIP-008 Cyber Security Incident response plan(s)
  - Formalize the hand-off to higher-level incident response protocols if the anomaly is confirmed as a threat

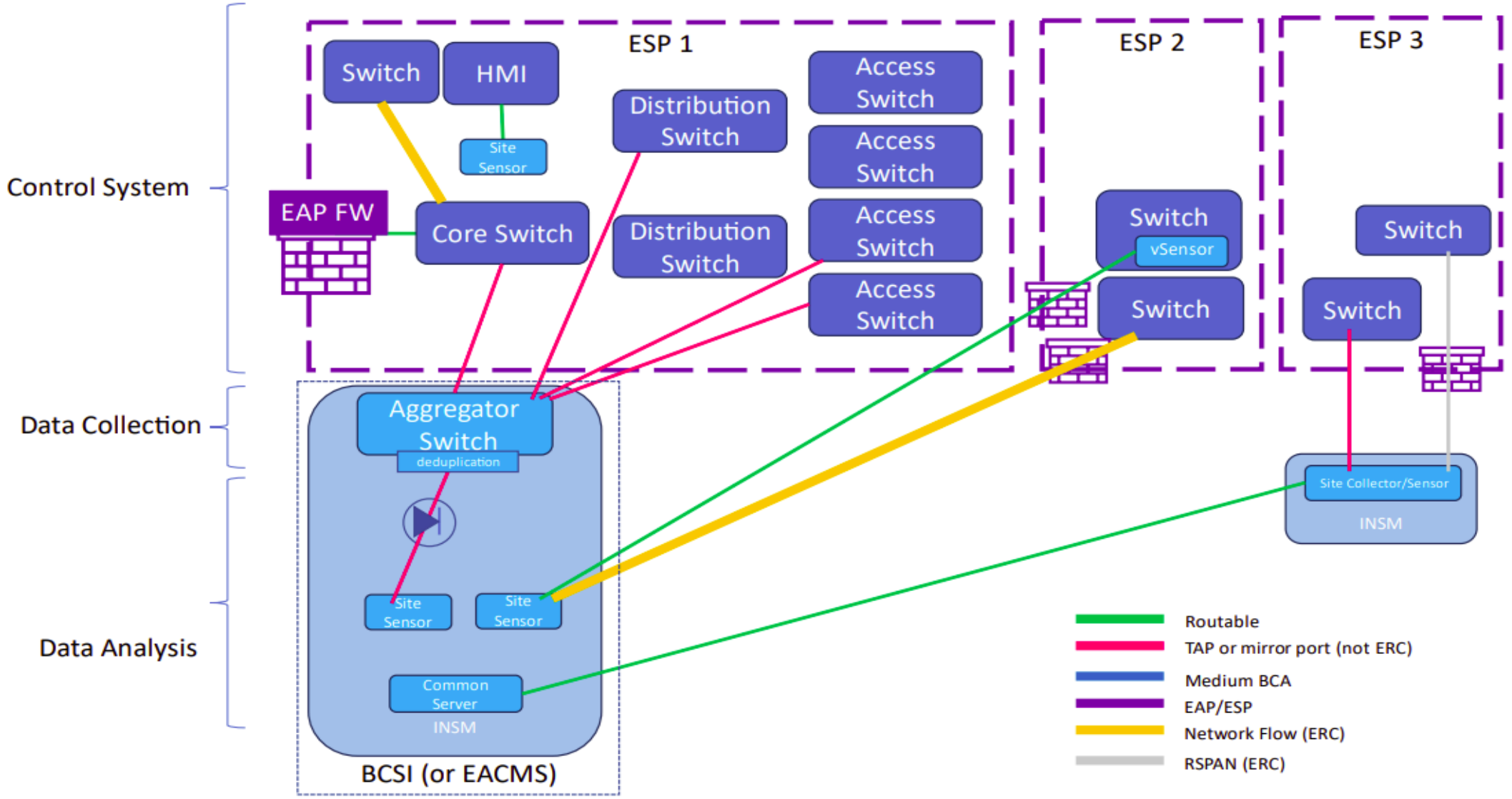
Integration with Incident Response

- Which scenarios could escalate to a Reportable Cyber Security Incident or a Cyber Security Incident that attempted to compromise an applicable system?
  - INSM assists with incident scoping.
  - Packet/flow data supports forensic reconstruction
- Do alerts feed directly into IR playbooks?
- Actions in response to detected anomalies
  - Execute the predefined technical or administrative steps to address the findings.
- Monitoring validates mitigation success.

Purdue Model



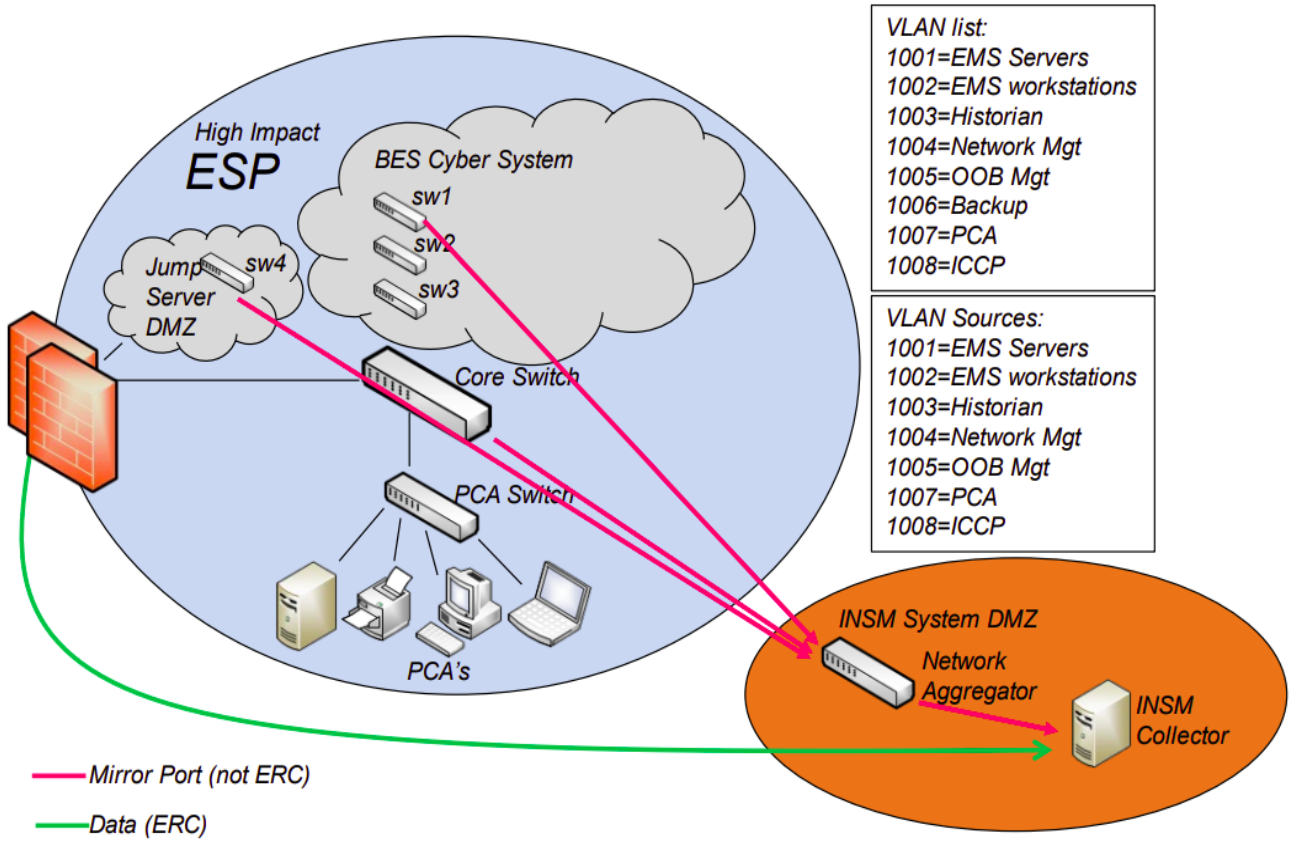
INSM Architecture



https://www.nerc.com/globalassets/standards/projects/2023-03/2023-03-technical-rationale-fb-clean.pdf

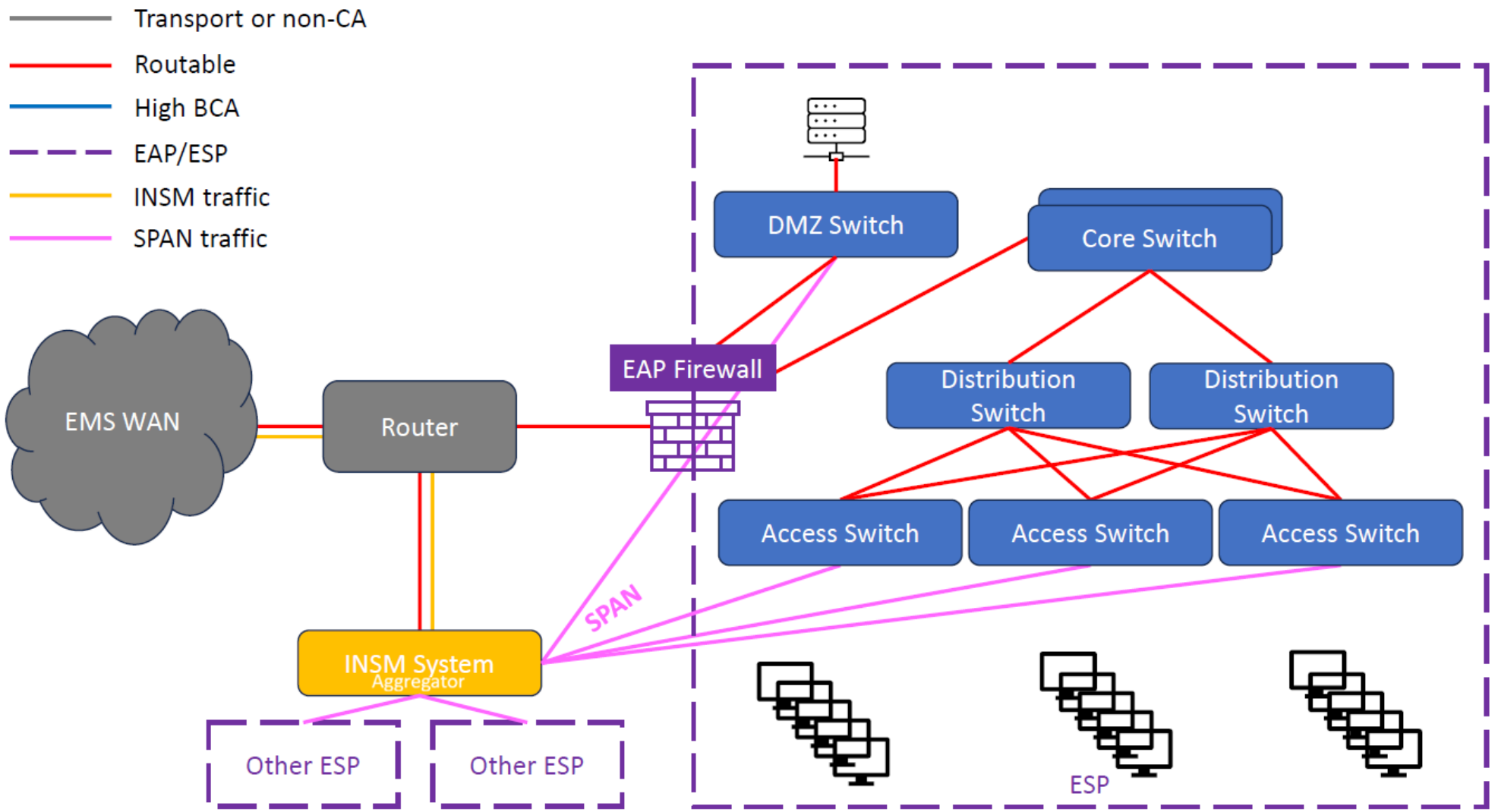
INSM Architecture

Network Data Feed	Collection Implemented	Network Location	Collection Method	Rationale



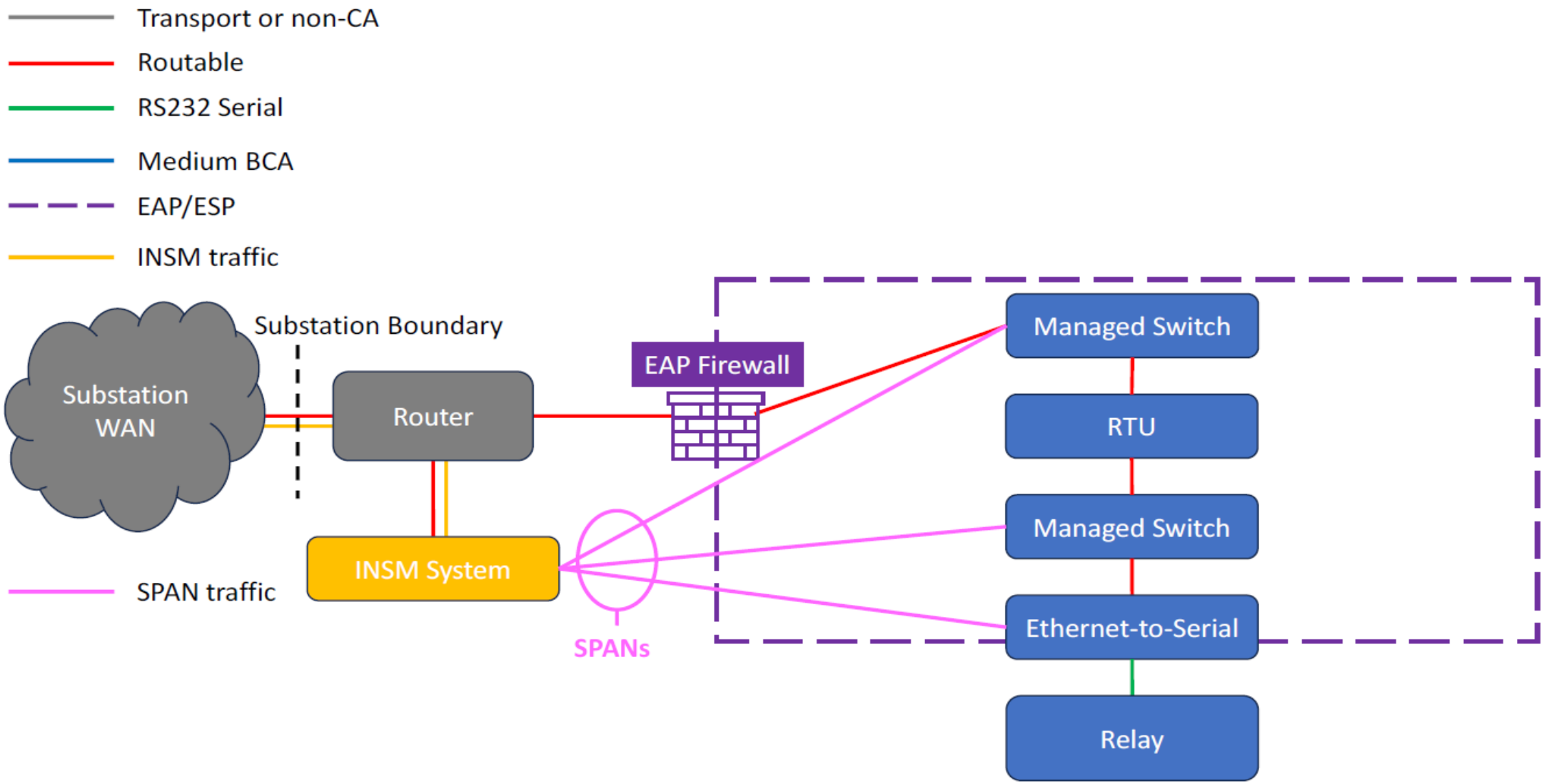
https://www.nerc.com/globalassets/standards/projects/2023-03/2023-03-technical-rationale-fb-clean.pdf

Control Center INSM



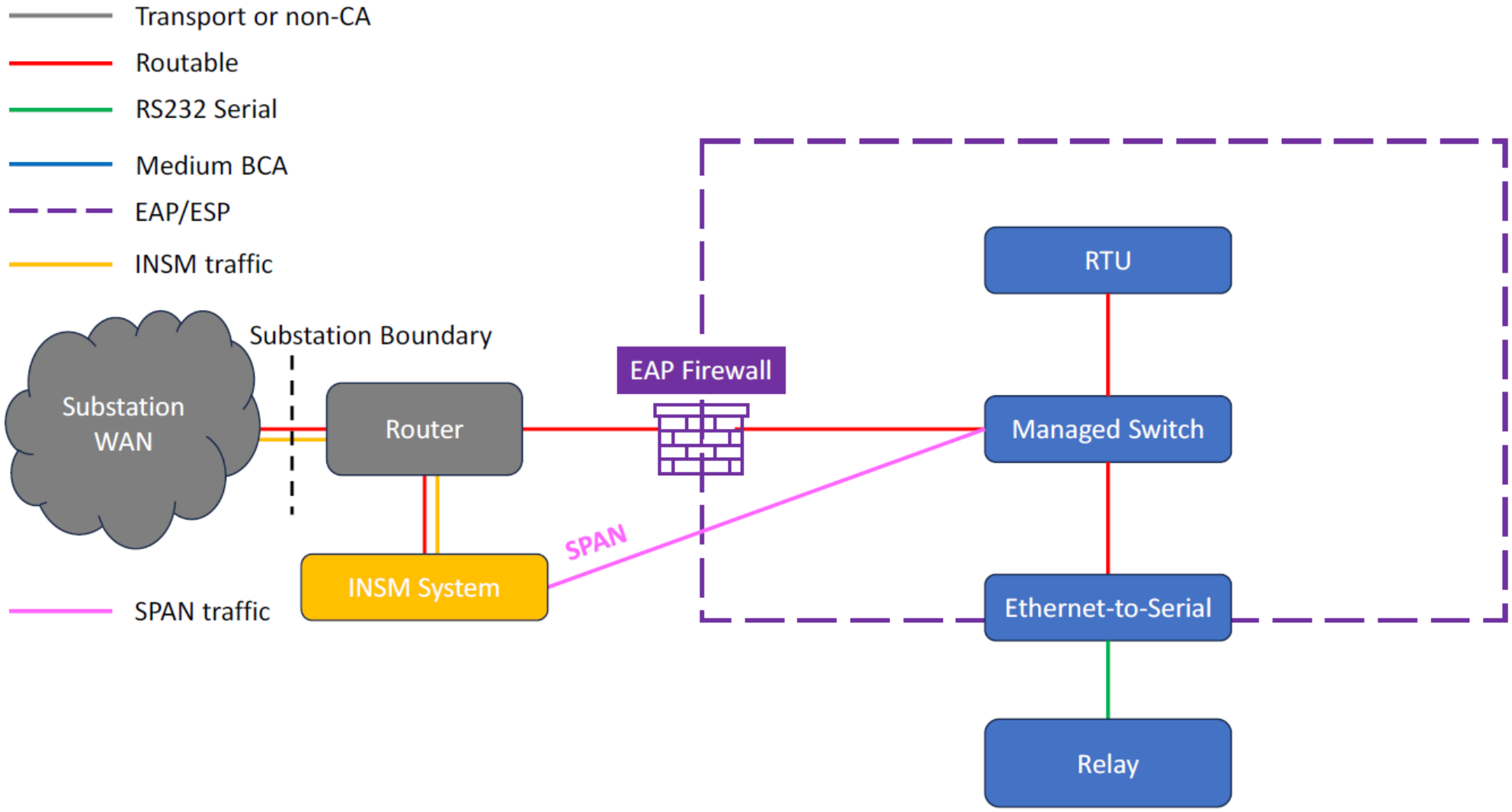
https://www.natf.net/docs/natfnetlibraries/documents/resources/supply-chain/natf-cip-015-insm-implementation-guidance.pdf

Substation INSM



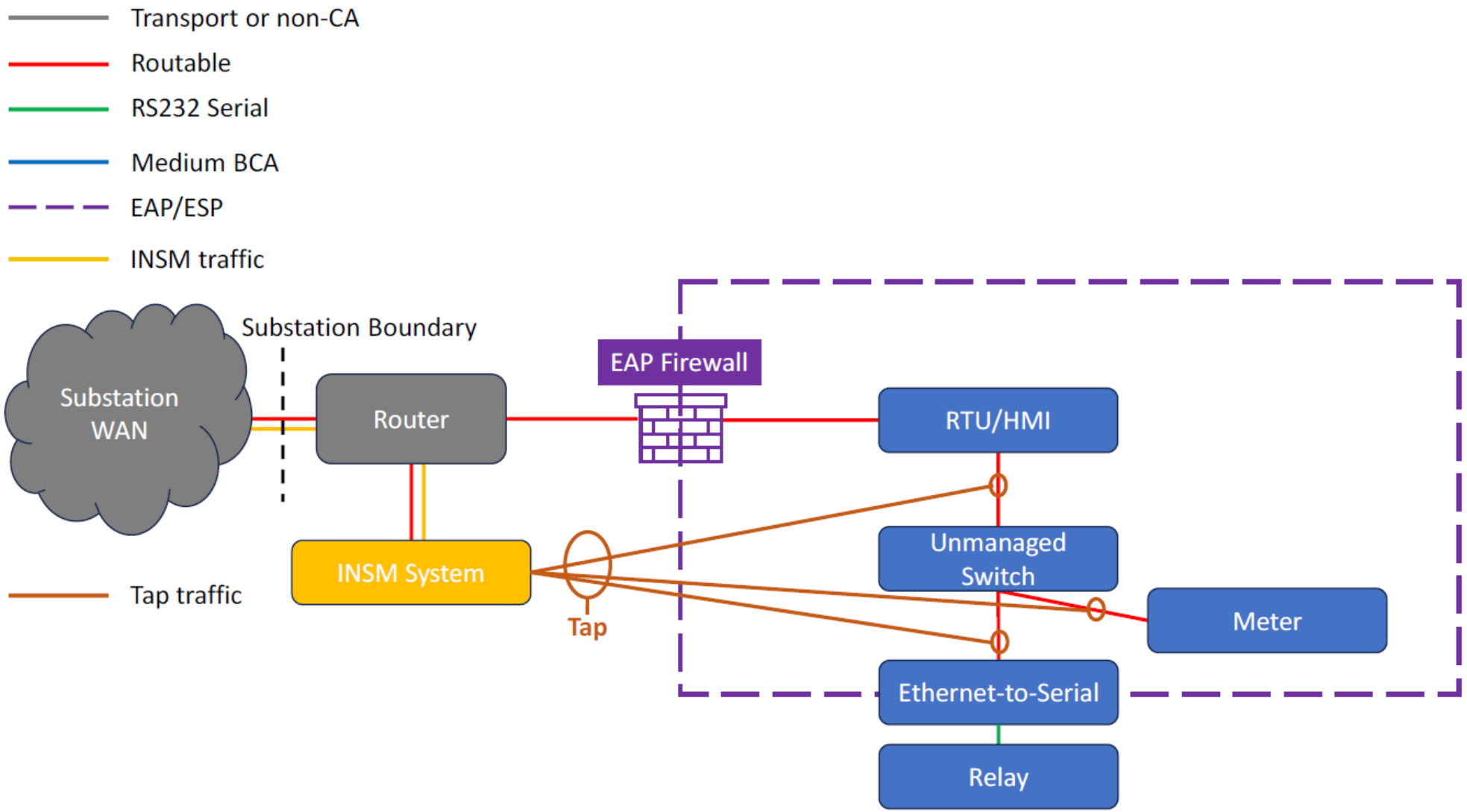
https://www.natf.net/docs/natfnetlibraries/documents/resources/supply-chain/natf-cip-015-insm-implementation-guidance.pdf

Substation INSM



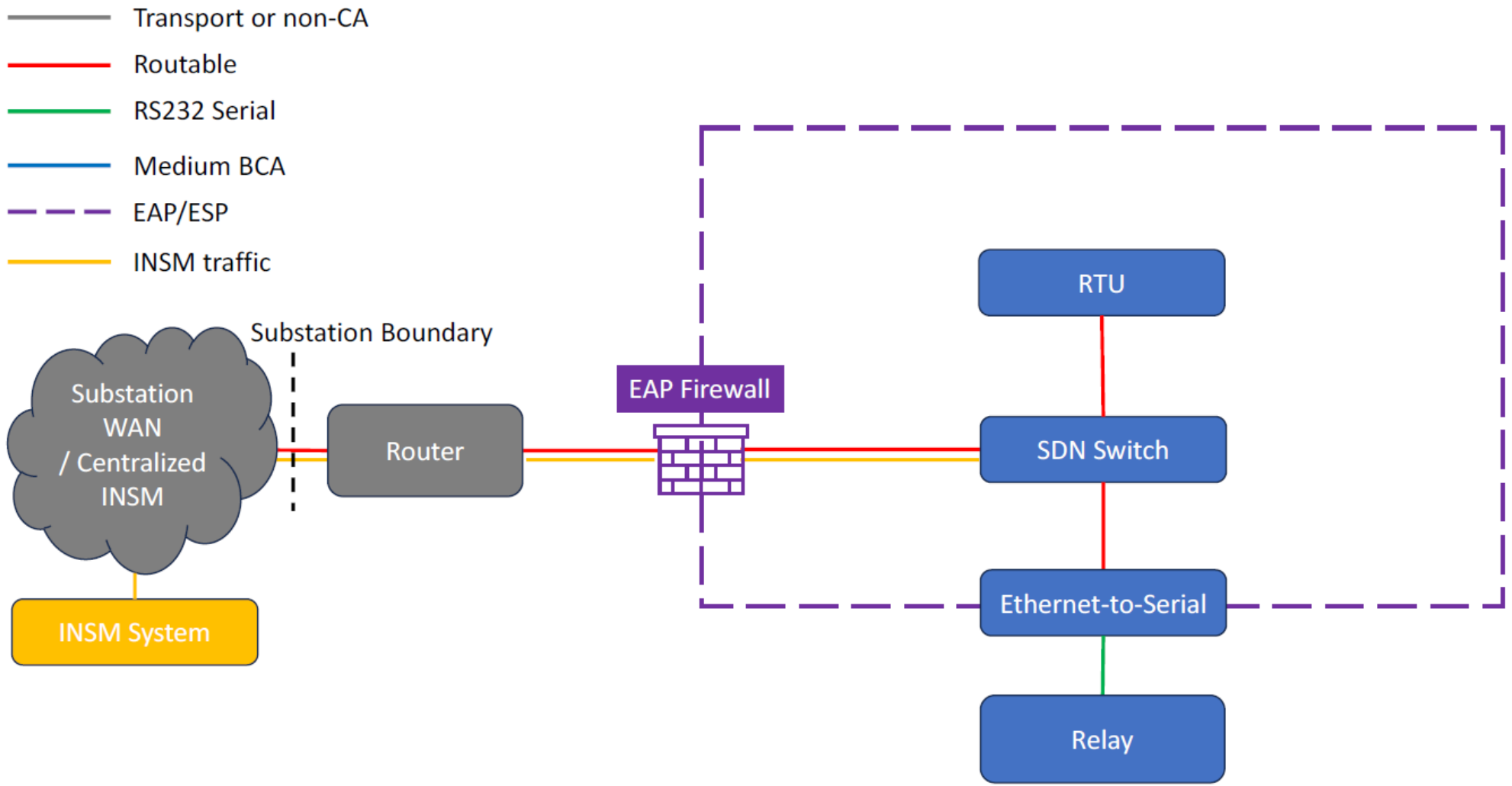
https://www.natf.net/docs/natfnetlibraries/documents/resources/supply-chain/natf-cip-015-insm-implementation-guidance.pdf

Substation ISNM



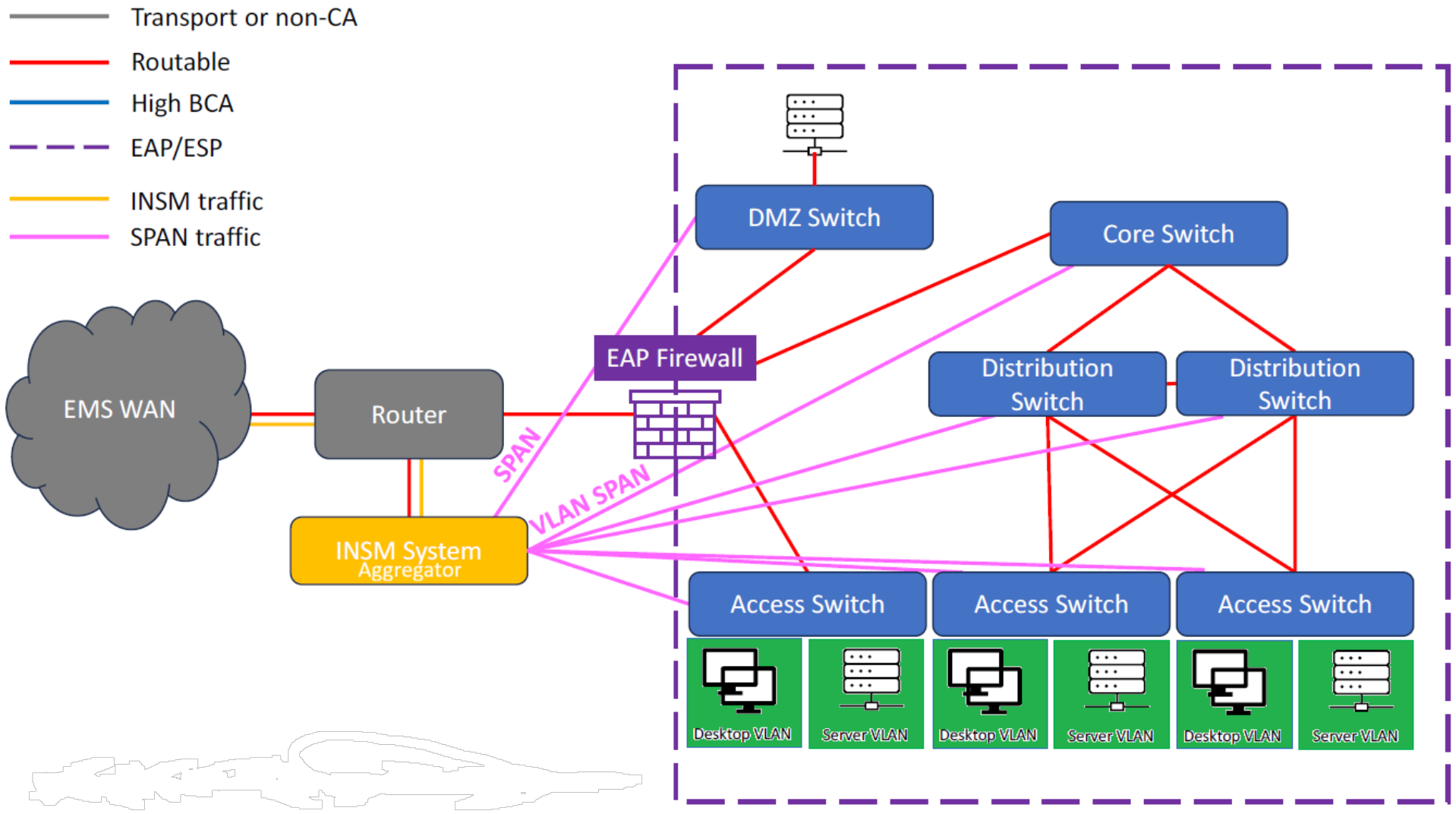
https://www.natf.net/docs/natfnetlibraries/documents/resources/supply-chain/natf-cip-015-insm-implementation-guidance.pdf

SDN INSM



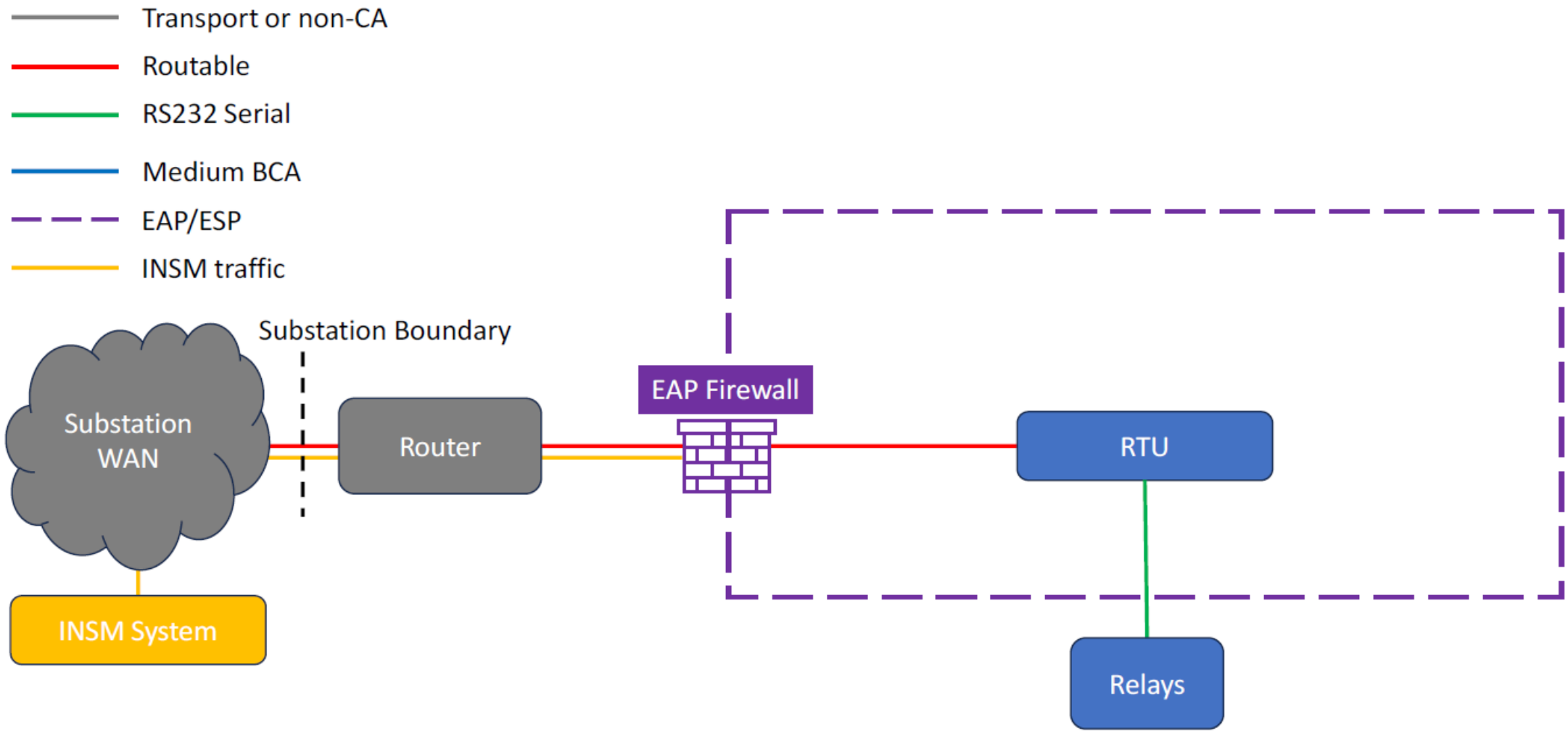
https://www.natf.net/docs/natfnetlibraries/documents/resources/supply-chain/natf-cip-015-insm-implementation-guidance.pdf

Endpoint Detection Telemetry



https://www.natf.net/docs/natfnetlibraries/documents/resources/supply-chain/natf-cip-015-insm-implementation-guidance.pdf

Substation INSM

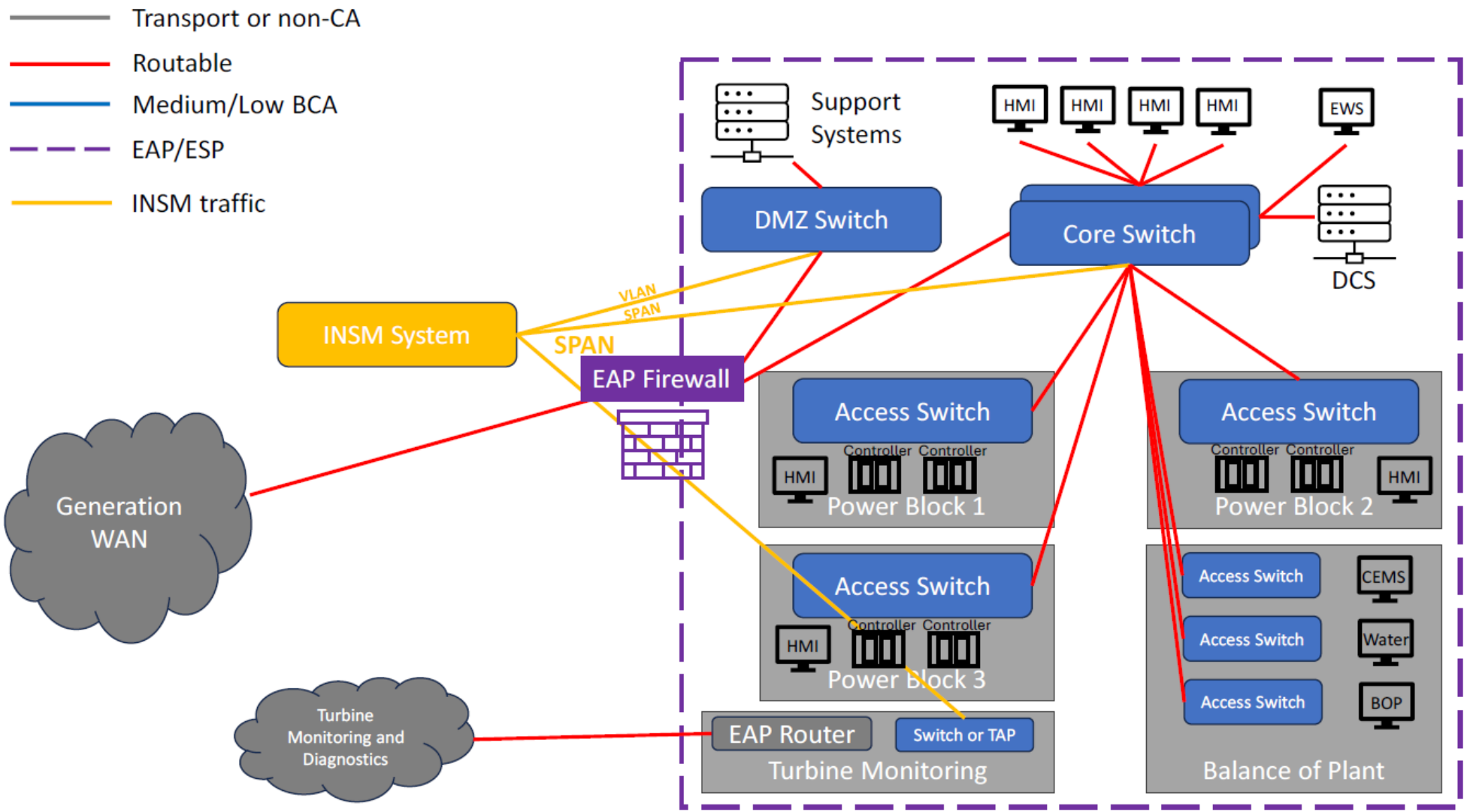


https://www.natf.net/docs/natfnetlibraries/documents/resources/supply-chain/natf-cip-015-insm-implementation-guidance.pdf

Future Definitions

- Electronic Security Perimeter
  - The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol; or a logical boundary defined by one or more Electronic Access Points
- Electronic Access Point
  - An electronic policy enforcement point or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems that controls routable communication to and from one or more BES Cyber Systems or their associated Protected Cyber Assets

Generation INSM



https://www.natf.net/docs/natfnetlibraries/documents/resources/supply-chain/natf-cip-015-insm-implementation-guidance.pdf

Success Metrics

- Mean Time to Detect (MTTD)
  - Average amount of time to discover that a security incident or breach has occurred
- Alert fidelity rate
  - Accuracy of detections (precision)
- Coverage of critical traffic flows
  - Percentage of infrastructure or traffic actively monitored
- Mean Time to Mitigation (MTTM)
  - Average time to after a potential security threat or anomaly is confirmed to when it is neutralized or contained

Challenges

- Encrypted packets
- Sensor placement limitations
  - Visibility gaps
- Tool complexity
  - Multiple platforms and feeds generate conflicting signals
- Noisy intelligence
  - Raw data without context slows response times
- Alert fatigue and false positives
  - Unrefined monitoring rules and lack of context-aware correlation
- Packet duplication
  - Analysis and storage

Retain INSM Data

- Data retention process(es)
  - How applicable data is identified, flagged, and stored
- System configuration(s)
- Duration
  - Escalation following the Responsible Entities Incident Response plan
  - No action
  - Further investigation
  - Tuning of the INSM system to reduce false positive notifications or adjust severity level
  - Other actions as determined by the Responsible Entity

Compliance Monitoring Process

- 1.2. 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 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.

INSM Data Protection

- Data protection process(es)
  - Data collected in support of Requirement R1
  - Data retained in support of Requirement R2 to mitigate the risks of unauthorized deletion or modification
- Ensure tools used to collect and store INSM data are secured
  - EACMS or not?
- Evaluate for BCSI
  - Ensure IPP includes a process for information sharing

FAQ

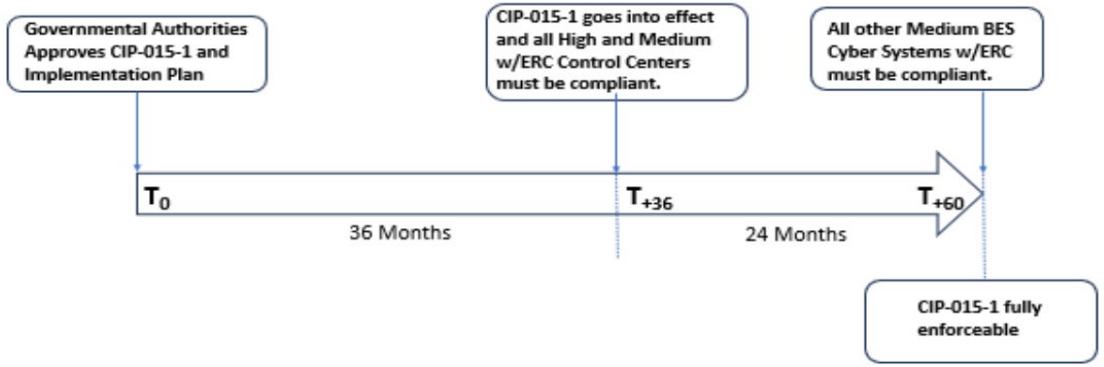
- What are the risk factors that an entity must consider to calculate risk-based rationale score?
  - What is the minimum criteria supporting risk-based rationale?
- Is a specific tool or method prescribed for detecting anomalous network activity?
- Is monitoring required to be continuous or periodic?

Project 2025-02 Internal Network Security Monitoring Standard Revision Drafting Team

- CIP-015-2
  - Passed ballot with 87.33%
  - Implementation plan passed with 86.93%
  - All devices that were originally subject to monitoring in CIP-015-1 R1 are still subject to monitoring in CIP-015-2, with the change of target
  - Changes the target of the monitoring from the network itself to Cyber Systems that are a part of Applicable Systems that match NERC definitions
    - Network location of the devices is no longer part of the scoping
  - Shared Cyber Infrastructure (SCI) is now added in scope of R1 for CIP-015-2, and this is now an additional Applicable System
    - Part of the CIP-005 Requirements; however, ESP is no longer a consideration in CIP-015-2

Implementation Plans

- CIP-015-1



- CIP-015-2
  - Modified the IP to remove references to CIP-015-1 implementation
  - Picks up at 12 months after the effective date of CIP-015-1
    - Removes the network location consideration and introduces the Applicable System references
  - Recasts the remaining phase of CIP-015-1 in terms of CIP-015-2 for medium w/ERC not at a Control Center

ELECTRIC RELIABILITY & SECURITY FOR THE WEST

ENGAGE WITH WECC