WHITE PAPER

NERC CIP Standards for Threat Visibility and Detection

Standards for Threat Visibility and Detection

Vulnerability of Critical Electricity Infrastructure

Cybersecurity is often described as prevention, detection, response --- and recovery, if needed. What the Colonial Pipeline ransomware attack, the Oldsmar Florida Water poisoning attempt, and now the White House are all telling us is that prevention isn't perfect and therefore, we need to increase focus on detection, response, and recovery.

Shortly after the Colonial Pipeline ransomware attack, the White House issued the *National Security Memorandum to Improve Cybersecurity for Critical Infrastructure Control Systems*[1] ('NSM'). The NSM is a collaborative effort between the Federal Government and the critical infrastructure community to improve the cybersecurity of critical systems. The overall goal of the NSM is to defend the United States' infrastructure and encourage asset owners to deploy threat visibility and detection technologies to support incident response, incident recovery and information sharing.

The Challenge for Utilities Security Personnel

Grid modernization has created an explosion of network-connected equipment, exposing utilities to a wide range of potential threats from nation states, criminals, disgruntled employees, and accidental misconfiguration (which happens far more often than you might think). The problem isn't 'grid modernization' per se, but the 'explosion of network connected equipment', including SCADA equipment, which is exposing previously air gapped industrial control systems to the internet.

The Energy sector is particularly vulnerable to cyberattack because core cybersecurity strategies, like the use of SPAN ports as a means to direct bulk network data to security analysis systems, and physical air gaps to separate the Operational Technologies ('OT') network from the rest of the enterprise network have grown outdated.

When a human released a cyber worm known as 'Stuxnet' into a physically air gapped facility in 2010, it became obvious to the world that new cybersecurity strategies were needed.

Prevention Alone is Not Enough

This document outlines the use of TAPS or SPANs for Threat visibility, and how installing network TAPS can help meet NERC CIP compliance where SPANS might not. Also included are often missed cost considerations.

SCAN ME

TEMPEST KEYSIGHT TECHNOLOGIES

The 100-Day Plan to Address Cybersecurity Risk to the Electric System

The overall goal of the White House's *100-Day Plan to Address Cybersecurity Risk to the Electric System* (100-Day Plan) is to encourage critical infrastructure asset owners to deploy threat visibility and detection technologies to support their incident response and recovery capabilities, as well as provide greater information sharing potential. It is one of several recent motions from the United States federal government in conjunction with the NSM to address: 1) threat detection and monitoring; 2) incident response and recovery; 3) information sharing; and 4) supply chain security.

Threat detection and monitoring begins with the addition of network TAPS in power plants and substations at multiple levels of the SCADA network. TAPS give OT personnel and network managers secure and ready access to data from critical infrastructure systems without adding to the compliance footprint or requiring network changes. TAPS provide a vital, non-invasive, network-friendly means to monitor and examine large quantities of network traffic. Unlike SPAN ports, TAPS present no load on the network, ensure that no packets are dropped, no changes occur to the timing of frame interactions, and valuable resources are not wasted examining duplicate packets.

Once TAPS are installed, Network Packet Brokers can capture, filter, aggregate, regenerate and efficiently route network traffic to security tools for inspection and incident response, creating a tightly integrated compliant security solution for utilities. Because Keysight's TAPS and NPBs capture all the network packets, (not just representative sample data) they create a complete historical archive of required data to meet strict NERC audit requirements.

What NERC CIP says about Threat Visibility

The North American Electric Reliability Corporation (NERC) is a regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid. NERC's jurisdiction includes users, owners, and operators of the Bulk Electric System, which serves nearly 400 million people.

The NERC Critical Infrastructure Protection (CIP) standards include regulatory elements that make collecting and archiving network traffic more important than ever before. NERC CIP Standards require utilities to monitor network traffic data at the control center, the plant, and the substation. Utilities are subject to regular NERC Compliance audits and must also regularly conduct vulnerability assessments.

The next section outlines several (but not all) existing NERC CIP regulatory parts that invoke the potential use of TAPS or SPANs for threat visibility and detection and explains the use of network TAPS vs SPANS to achieve NERC Compliance.

NERC CIP-007-6 R1.1

Regulatory Text: Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.

What it Means: Constant monitoring of network packets is becoming increasingly critical to evidencing compliance with CIP-007-6 R1.1. Entities are required to provide listings of allowed ports and services for each device on the network and show that they are well-aware of what is: (1) permitted, and (2) in use.

The use of network TAPS to send copies of network packets for inspection is a significant and important measure. SPAN ports are not reliable under attack when malware is flooding switch SPAN ports.

How TAPS Help: The use of TAPS to route all network traffic to anti-malware assets for rapid examination is a highly effective way to show full compliance with CIP-007-6. TAPS can aid in detecting east/west malicious code, especially in situations where malware protection software cannot be installed on purpose-built industrial control devices. Unlike switch SPAN ports, TAPS are not hindered by the excessive traffic caused by malware attacks.

NERC CIP-007-6 R4.1

Regulatory Text: Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, at a minimum, each of the following type of events:

4.1.1 Detected successful login attempts

4.1.2 Detected failed access and failed login attempts

4.1.3 Detected malicious code

What it Means: Entities are required to evidence that they have viable and meaningful event logging measures. Event log data is typically sent over the network to a syslog server (or similar), where the data is evaluated and stored.

How TAPS Help: Because all network traffic is captured under all conditions, network TAPS, unlike any other solution, assures that no event log data is lost due to network flooding, switch problems, or malicious activity. Furthermore, network TAP data can be readily used by the SIEM to determine failed network access attempts, and/or identify unauthorized devices that might connect and disconnect from the network. Network TAPS help ensure full compliance with CIP-007-6 R4.1.

NERC CIP-007-6 R4.2

Regulatory Text: Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, at a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability):

4.2.1 Detected malicious code from Part 4.1

4.2.2 Detected failure of Part 4.1 event logging

What it Means: Entities are required to evidence that alerts are generated for at least detected malicious code and failure of event logging. Network TAPS pull the switch out of the detection mix (no SPAN port needed), which ensures that no alerts are missed. Likewise, having a TAP removes the possibility that the switch configuration was modified by an attacker – which they might do to cover their tracks—or misconfigured during legitimate testing or configuration changes.

How TAPS Help: The utilization of network TAPS, unlike any other solution, provides solid assurance that no security event alert (as required by CIP-007-6 R4.2) is missed or delayed. An additional benefit is that during change windows, no alerts would be missed.

Malware can cause network flooding and render a SPAN port on a switch nearly useless. This situation would cause a potential violation of both CIP-007-6 R4.2 and CIP-007-6 R4.1.

NERC CIP-009-6 R1.5

Regulatory Text: One or more processes to preserve data, per Cyber Asset capability, For determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.

What it Means: Regardless of the operational status of switches network data must be available and always processed. CIP-009-6 R1.5 requires utilities to preserve data from cyber security incidents.

How TAPS Help: Network TAPS capture all the data all the time, irrespective of the processing load on the switch (which could cause SPAN ports under attack to drop traffic). The use of network taps ensures that all network data is available and processed at all times. This helps ensure compliance with CIP-009-6 R1.5.

NERC CIP-010-3 R1.3

Regulatory Text: For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.

What it Means: There are known incidents where new devices were activated on a utility's network without having gone through the configuration change control process (of reprogramming the SPAN to include the new devices). The new devices remained activated for more than 30 calendar days, resulting in self-reports and possible violations. The use of network TAPS would have ensured that all devices were accounted for at all times, because network TAPS are set and forget and don’t need to go through configuration change control processes with the activation of new devices.

How TAPS Help: CIP-010-3 R1.3 requires utilities to update their baseline configuration data within 30 calendar days of implementing a change. The utilization of network TAPS -- an independent measure that ensures the consistent flow of network data to analysis equipment -- is one of the best methods to ensure compliance with CIP-010-3 R1.3.

Keysight Solution for Security and Compliance

Keysight TAPS are hardware devices built with a single purpose: to securely direct bulk network data to security analysis systems while preserving network uptime – even when your network is under attack (and an overloaded switch can fail to copy traffic to a SPAN port). Keysight TAPS cannot be used to inject malicious traffic into the network.

Network TAPS send traffic at line rate, even during high traffic levels seen during cyberattacks.

And should power failure cause a TAP to fail, Keysight TAPs automatically bypass monitoring functionality, and allow the continuous flow of network traffic, as if the TAP did not exist.

There's No Such Thing as a Free Lunch

Despite the commonly held (mis)belief that SPAN ports are free and TAPS are not, using SPAN ports for bulk collection of network data is considered technologically outdated, potentially risky to the performance of the network, and an unreliable solution.

And while one-time capital expenditures ('CAPEX') of SPAN ports might be inconsequential, the recurring operating expenses ('OPEX') associated with change management (reconfiguration and possible misconfiguration), and maintenance of SPAN ports are not.

The chart below is an estimate of the ongoing labor costs associated with using SPAN ports, which must be configured and reconfigured as your network changes. Costs for ongoing labor costs associated with TAPS are also shown. Because TAPS are purpose-engineered devices that require no CLI Programming, no planning, and no validation (QA testing), they have a much lower Total Cost of Ownership than SPAN ports.

OPEX costs associated with SPAN sessions start Day 1. Illustrated above is an estimate of the average annually recurring maintenance costs ($6,890) for SPAN sessions.

Costs include network engineering for CLI programming and filter validation at an estimated $100 per hour. Programming costs generally increase over time due to complexity.

Estimated SPAN Port First Year Labor		
PROVISIONING	TAP COST	SPAN COST
Initial Set-up	$0	$530
CLI Programming + Filter Validation	$0	$97
CLI Programming + Filter Validation	$0	$302
CLI Programming + Filter Validation	$0	$540
CLI Programming + Filter Validation	$0	$864
CLI Programming + Filter Validation	$0	$957
SPAN session planning	$0	$3,600
Averaged Total	$0	**$6,890**

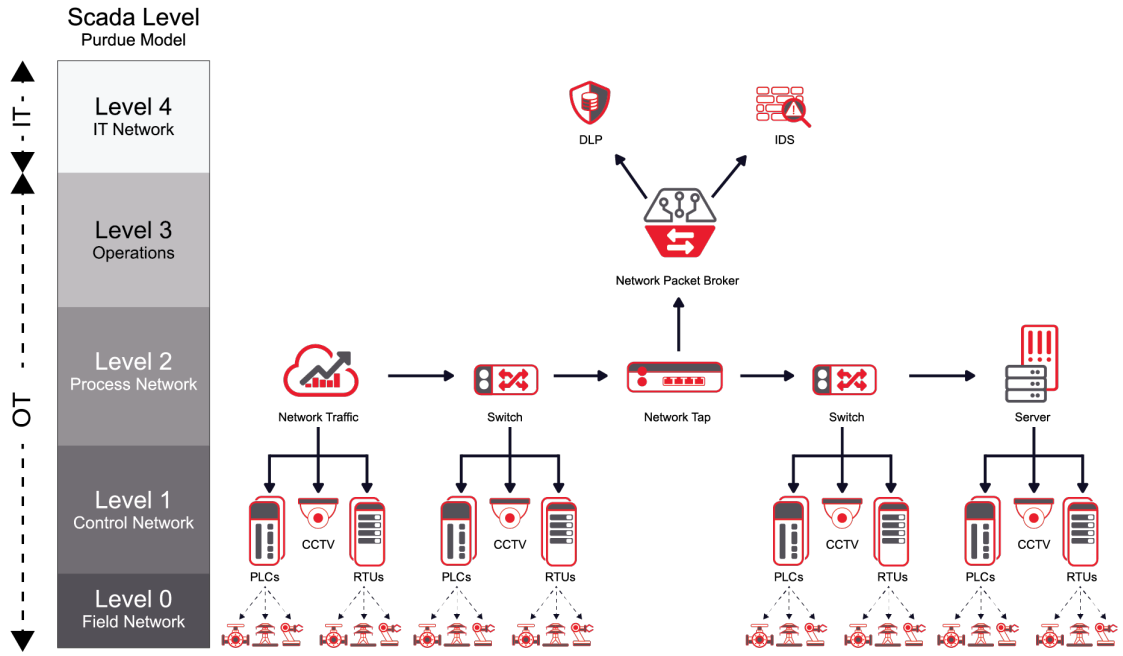
The Hidden Costs of not Network Monitoring

To get a complete picture of the cost of network monitoring, you might also want to consider the intangible costs of not implementing network monitoring. Intangible costs would include things like: the cost of a security breach cleanup, lost revenue due to down time, regulatory audit fines, PR cleanup, and overall eroded trust in your brand.

And cyber Insurance is another subject going through the courts, as many policies have policy exclusions for Acts of War.

ICS/OT Security Visibility Reference Architecture

Keysight TAPS are installed at multiple layers of the Purdue Reference Model starting at Level 2, to capture SCADA traffic from devices such as PLCs, RTUs, and HMIs. Network traffic is then aggregated at Level 3, where Network Packet Brokers filter, aggregate, (and remove unwanted traffic like CCTV) to speed up inspection and reduce costs for Threat Detection and Monitoring.



Conclusion

The *National Security Memorandum to Improve Cybersecurity for Critical Infrastructure Control Systems* is one of several recent motions from the federal government, such as the 100-Day Plan to Address Cybersecurity Risks to the U.S. Electric System, the Department of Energy Request for Information on Securing Critical Electric Infrastructure, the Federal Energy Regulatory Commission Request For Information on Potential Enhancements to the Critical Infrastructure Protection Reliability Standards and Executive Orders 13920 and 14028 – all of which have similar components:

1. Threat detection and monitoring
2. Incident response and recovery
3. Information sharing
4. Supply chain security

This volume of activity focused on cybersecurity for the critical infrastructure sectors is a strong indicator that action is expected – and may even be inevitable.

With utilities becoming an increasingly popular target by nation states with seemingly unlimited resources, CSO's and IT teams are on the lookout for new strategies, tools, and expertise to be both secure and compliant. And with regulatory compliance for threat detection and monitoring coming soon, TAPS can provide a quick and low cost solution for meeting compliance requirements.