SOLUTION BRIEF

Network Monitoring for Tough Spots

Keysight Visibility for Industrial Control Systems

Why your ICS Architecture needs Visibility

HMIs are the unsung heroes of industrial control systems. They control the automation that make life easier. From ATM machines that dispense cash, to entertainment screens in automobiles, HMIs are that human-machine-interface that make stuff happen in factories, plants, and in the field.

The HMI, with its simple on-screen commands that control the PLC has become a favorite target for hackers because the headless, ruggedized, mostly Window-based computer known as the programmable-logic-controller, controls the equipment. And the equipment does the work.

Note that the HMI controls not just one PLC, but typically multiple PLCs. In fact, the HMI could control all of the PLCs on the factory floor. It's easy to imagine what a hacker could do with the ability to issue commands through the HMI, to all of the equipment controlled by PLCs. Could they shut down the power for 225,000 people (Ukraine 2015)? Attempt to poison the water supply to 15,000 residents (Oldsmar Water 2021)? Or stop vaccine production, disable 37,000 computers, and ultimately cost $1.3B when insurance companies refuse to cover '*Acts of War'* (NotPetya 2017)?

Yes. But it wasn't always this way.

There was a time when keeping your ICS environment physically off the enterprise network was a major component of the ICS cybersecurity strategy. And for years, it worked. But in a world where just about everything-- from consumer goods to industrial goods-- are connected to the internet, that time has passed. Because hackers have already proven that the physical air gap can neither prevent malware intrusion, nor identify malware once it gets inside your network.

A strong cybersecurity strategy for ICS must now include the ability to see what network traffic is flowing inside your entire network; both the IT enterprise network, and the OT operational technology network. And we call that, Network Visibility. Why?

Because you can't protect what you can't see.

HMIs might be the unsung heroes of the ICS world, but the HMI is a hacker's dream.

KEYSIGHT TECHNOLOGIES

Network Taps or SPAN Ports?

For most utilities and industrial organizations, network visibility starts with the addition of a monitoring layer within your ICS environment.

But how? Do you install purpose-built monitoring devices called Network Taps, or do you enable the port mirroring capability of the switch, also known as the SPAN port? It's an age-old question that's been boiled down to this simple rule of thumb:

Tap where you can. SPAN where you can't. Why?

Because you can't realistically tap every link. But you would if you could because taps offer significant advantages over SPAN ports.

Several of the advantages of taps versus SPAN ports include:

- Taps are simple plug-and-play devices that don't need CLI configuration
- Taps pass 100% of traffic, including layer 1 and layer 2 traffic
- Taps don't drop packets
- Unmanaged taps can't be hacked (no IP address)
- Tap administration costs are $0
- Taps can be added where you need them
- Taps can be air gapped to prevent injection of malicious traffic

Now is the time for visibility in your Industrial Control environment. Which means you need taps that are purpose-built to withstand the same tough environments of your industrial equipment.

Tough Taps for Ruggedized Environments

Keysight's industrial visibility solutions interoperate with our enterprise visibility solutions. Together they create a complete portfolio of copper and fiber solutions for out of band ('OOB') network monitoring tools for security and performance. Tough Taps give you the visibility you need to enable security in your ICS environment.

Industrial Flex Taps

Keysight's Industrial Flex Tough Taps are TAA Compliant, and purpose-built to meet the extreme operating environment of your ICS environment.

Keysight's Industrial Flex Taps are optimized for "Run to Fail" fiber networks with both old and new fiber modes often seen in remote substations. Available in two models: 1G OM1 multimode fiber for older networks, and the newest OM5 multimode fiber for everything else. Flex Tough Taps are compatible with monitoring devices from all major manufacturers, including protocol analyzers, probes, intrusion detection systems, and ICS cybersecurity tools, and are protocol agnostic. Flex Tough Taps are TAA Compliant and compact, with each module holding 4 taps in one DIN mountable housing.

Flex Tough Taps are deployed at any inline connection on the network, have no IP address, don't drop packets, and add no additional overhead or management burden to network devices like SPAN ports do.

Industrial Copper Taps

Keysight's Industrial Copper Tough Taps are TAA Compliant, independently certified, and purpose-built to meet requirements to operate where you need them, in extreme operating temperatures.

The 10/100/1000Mbps Copper Tough Tap is a secure tap device which can operate in three modes: (1) simple tap, (2) 2:2 packet replication (breakout on aggregation mode) or (3) 2:1 packet replication (aggregation mode).

When operating in aggregation Mode, the Copper Tough Tap sends copies of the aggregated traffic through two monitoring ports, allowing for a primary and secondary tool.

Copper Tough Tap supports Power over Ethernet (PoE) pass through, and have physically air gapped monitor ports for intrusion protection. Copper Tough Taps fail-to-wire to continuously pass traffic even if the tap loses power.

Industrial Power Solutions

A TAA Compliant Power Rack for Tough Taps is used to power up to 16 copper Tough Taps with fully redundant power source supply (dual-redundant).

The Industrial power supply rack can support 48V DC or 110-220V AC input power, and support up to 32 x 5VDC powered devices. TAA Compliant, the 19" rack mount supports both AC and DC DIN mountable power supply convertors available separately from Keysight.

Industrial Packet Aggregator

Keysight's industrial network packet aggregator solves the challenge of getting visibility into remote sites with harsh environments, such as power substations, mining sites, and other unique locations that have a wide range of environmental requirements.

When used with Keysight's Copper and Flex Tough Taps, the Vision T1000 aggregates multiple input streams into multiple aggregated output streams--optimizing scarce tool port requirements within your substation. The Vision T1000 filters out unwanted traffic based on packet headers, eliminating unwanted traffic such as CCTV video feeds. The Vision T1000 also load balances traffic, optimizing usage of monitoring tools. It's built with an easy-to-use GUI interface, so most functions are just a few clicks away.

Keysight's industrial network packet aggregator is TAA Compliant, independently certified for harsh operating environments, and supports either AC or DC power requirements.

Keysight Visibility for Industrial Control Systems

Solorigate, Sunburst, and Supernova are the three faces of the backdoor supply chain malware also known as the SolarWinds hack. It's been called the most sophisticated attack ever seen. And while the news media has discussed what this means to the Enterprise IT environment, few have noted that the SolarWinds Orion platform hack also gave hackers access to ICS networks. After the 2010 Stuxnet malware, the 2015 Ukraine power grid hack, and now the 2019 SolarWinds Orion attack, more and more organizations are scrambling for network visibility solutions for their ICS environments, both inside and outside of the datacenter.

Keysight has been providing visibility solutions for conditioned datacenter environments since 1996. Now Keysight offers independently certified network monitoring solutions, purpose-built to give you visibility where you need it— in tough spots with harsh operating environments.

For a deeper dive, see Keysight Taps vs SPAN Port Monitoring at Keysight.com

To learn more about the SolarWinds Hack see Keysight Blogs

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications, or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES