NEOX NETWORKS

NEXT GENERATION NETWORK VISIBILITY

www.neox-networks.com

WHITEPAPER

NETWORK TAPS IN THE CRITIS AREA

PROFESSIONAL DATA EXTRACTION FOR MONITORING, ANALYSIS AND SECURITY TOOLS IN CRITICAL INFRASTRUCTURES

SecurITy made in Germany

TeleTrusT Quality Seal
www.teletrust.de/itsmig

1. Introduction

According to the NIS2 Directive, operators of critical infrastructure (CRITIS), such as healthcare, digital infrastructure, transport, water supply, digital services, banking and financial services infrastructure, energy and, in addition, now also providers of public electronic communications networks or services, wastewater and waste management, manufacturers of certain critical products (e. g. pharmaceuticals, medical devices and chemicals), food manufacturers, digital service providers such as social networking platforms and data center services, aerospace, postal and courier services, and public administration in all 27 member states of the EU, plus Liechtenstein, Iceland and Norway, have to take comprehensive measures for the security of their network and information systems by Oct. 18, 2024.

This includes, among other things, the implementation of suitable tools that continuously monitor and protect the corporate network, whether it is an IT or OT network. But all these tools have one thing in common: they need a reliable source from which to obtain the network data, i. e. the data traffic.

We have already gone into the manifold reasons why it is not a good idea to use the SPAN/Mirror port of switches for this purpose in our whitepaper „Network TAP vs SPAN/Mirror port - Professional extraction of network data for monitoring, analysis & security tools".

If you have considered these reasons, for example the risk of compromising the switches, and the SPAN/Mirror port is consequently ruled out as a data source, then it becomes clear fairly quickly that Network TAPs are best used as a data source. But even here, caution is advised, because the term „Network TAP" is not legally protected.

For example, some manufacturers simply sell cheap standard switches with a permanently established SPAN/Mirror session as a Network TAP.

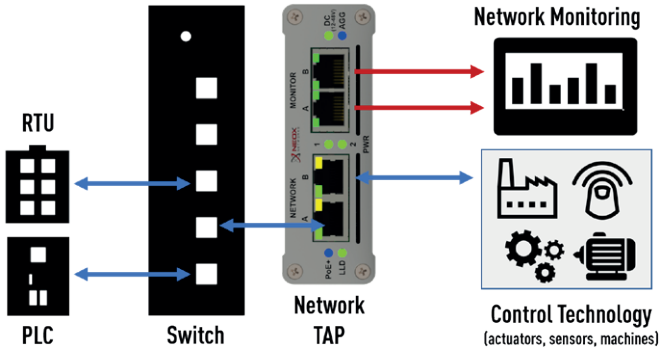
Therefore, when choosing should pay attention to certain criteria.

2. Features of real Network TAPs

Real Network TAPs implement the logic for routing out a copy of the network data in hardware, and not by means of software, as in the case of switch hardware with permanent SPAN/Mirror session!

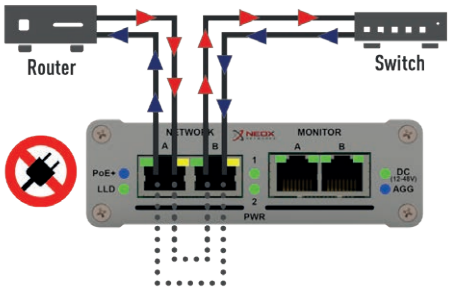
Very importantly, Network TAPs mirror 100% of the traffic and thus cleanly mirror not only FCS/CRC error-bearing packets, but also oversized packets and packets smaller than the minimum size defined by default.

Furthermore, packet loss must not occur under any circumstances when data packets are mirrored by Network TAPs.



Example placement of a Network TAP in the CRITIS network

The power supply for Network TAPs should always be redundant for reasons of reliable availability. For locations where only DC voltage is available, a Network TAP should also have an integrated DC power supply (e. g. 12V - 48V).



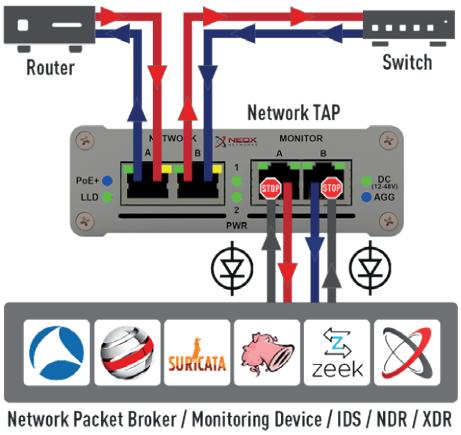
Failsafe function of Network-TAPs

In the event that a power failure nevertheless occurs, it is essential that Network TAPs have a failsafe function that ensures that the active network connection into which the Network TAP is looped is re-established without external interference even in the absence of power.

For professional mounting, mounting options such as rack mounting and DIN rail mounting should be available for the Network TAPs.

In addition, if possible, Network TAPs should absolutely have a data diode function that ensures that no data can get into the primary network connected to the network ports via the monitoring ports of the Network TAP, whether intentionally or unintentionally.

A Network TAP that has such a function is thus free of repercussions.



Data diode function of Network TAPs

3. The cybersecurity standard IEC 62443

IEC 62443 is a series of standards that represents an international cybersecurity standard and is aimed at operators, manufacturers and integrators of OT systems and networks. OT stands for Operational Technology, i. e. industrial control systems and networks. The IEC 62443 standard is also attracting increasing attention in IT (Information Technology).

IEC62443
APPROVED

The standard also covers the security of critical infrastructures. The standards it contains describe measures and methods for identifying and avoiding any vulnerabilities in networks and systems that could be exploited in attacks on them.

Therefore, it is highly recommended for CRITIS operators to use Network TAPs that comply with the technical requirements from IEC 62443.

4. Network TAPs hardened according to IEC 62443

IEC 62443 gives rise to a number of requirements that apply to Network TAPs and according to which Network TAPs must be hardened for compliance with the standard. In the following, we provide an overview of some of these requirements relevant for Network TAPs and show how hardened Network TAPs can meet these requirements:

Requirement from IEC 62443: The component must support a segmented network.

IEC 62443 hardened Network TAPs should behave transparently in terms of network segmentation and support any kind of protocols. VLAN or even other segmentations should be passed through 1:1, hardened Network TAPs should work on the physical layer and pass on all network transmissions, including all Ethernet packets on all OSI layers, protocol-independently and transparently.

Requirement from IEC 62443: The component must have a way to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services.

To meet this requirement, hardened Network TAPs should not have a management interface that can be used to enable or disable functions. The Network TAPs should be supplied with only the functionality as required by the particular customer. DIP switches that could be used to set the functionality could be deactivated in this case, so that a configuration other than the desired one cannot be made under any circumstances.

Requirement from IEC 62443: The network device must be protected against unauthorized use of the physical factory diagnostic and test interfaces.

Hardened Network TAPs should not have a diagnostic and test interface. Furthermore, hardened Network TAPs should be supplied without any internal interface in accordance with this requirement. Unauthorized access for possible manipulation of the firmware is then technically impossible.

Requirement from IEC 62443: The network device must provide protection against malicious code either directly or via compensating control.

This can be ensured by ensuring that hardened Network TAPs do not have a protocol layer, MAC address or IP address and therefore do not provide an attack surface for the execution of unauthorized software, for example via the network ports. Further, hardened Network TAPs should not have a management interface for possible installation of third-party software. Furthermore, hardened Network TAPs should also not have an internal interface when delivered.

Requirement from IEC 62443: Network devices must be tamper-proof and have a detection mechanism.

Hardened Network TAPs should have a secure, stable and robust housing, making physical access difficult. Furthermore, hardened Network TAPs should be equipped with self-destructing security seals to detect unauthorized access. In addition, hardened Network TAPs should be mounted with security screws. Ordinary screws have a drive that can be loosened or tightened with standard tools. Security screws, on the other hand, have a screw head that can only be used with special tools.

Requirement from IEC 62443: Ability to provide and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more „Roots of Trust" at the time of device manufacture.

To meet this requirement, hardened Network TAPs should have a mechanism to verify that the firmware is the original firmware applied by the manufacturer.

Requirement from IEC 62443: Network devices must verify the integrity of the firmware, software, and configuration data required for the component boot and runtime process before use.

To meet this requirement, hardened Network TAPs should have a special chip with a function that checks the authenticity of the installed firmware before the Network TAPs are booted (secure boot function). The hardened Network TAPs then only start the installed firmware in the event of a positive test result and prevent the execution of a manipulated version.

5. Conclusion

Are you a CRITIS operator or another operator of an OT or IT network and want to be compliant with the IEC 62443 cybersecurity standard? Then play it safe and use Hardened PacketRaven Network TAPs for the leakage of your network data!

We would be happy to advise you on our various PacketRaven Network TAPs and their features, as well as your individual requirements. You will find our contact details below!

NEOX NETWORKS GmbH
Monzastr. 4 · 63225 Langen · Germany
+49 6103 / 37 215 910 · solutions@neox-networks.com · www.neox-networks.com

// NEOX**PacketSolutions**

NEOX NETWORKS

PACKETRAVEN

Modular, portable and virtual NETWORK TAPS for up to 400G

PACKETLION

High end NETWORK PACKET BROKER for up to 400G

PACKETTIGER

Cost efficient next gen NETWORK PACKET BROKER
as Appliance or virtual

PACKETWOLF

Advanced PACKET PROCESSING up to 400Gbps

PACKETFALCON

Portable & compact PACKET CAPTURE appliances

PACKETGRIZZLY

Modular & scalable NETWORK FORENSICS solution

NEOX NETWORKS

NEOX NETWORKS GmbH
Monzastr. 4 · 63225 Langen · Germany
+49 6103 / 37 215 910 · solutions@neox-networks.com · www.neox-networks.com