HIRSCHMANN
A BELDEN BRAND

Advancing NIS2 Objectives with HiOS

TECHNICAL BULLETIN

Ensuring NIS2 Compliance: The Role of Industrial Ethernet Switches in OT Networks

As industries increasingly integrate their operational technology (OT) environments with information technology (IT), the need for robust cybersecurity measures is clear. The Network and Information Systems (NIS2) Directive, an evolution of the original NIS Directive, sets stringent cybersecurity standards for essential and important services within the European Union. Achieving NIS2 compliance is crucial for safeguarding critical infrastructure from cyber threats. One pivotal component in this cybersecurity framework is the industrial Ethernet switch, which plays a significant role in ensuring the security, reliability, and efficiency of OT networks.

BRS Switch

RSP Switch

BXP Switch

GRS 106 Switch

DRAGON MACH4000 Switch

The Role of Industrial Ethernet Switches

Hirschmann Industrial Ethernet switches, running the Hirschmann Operating System (HiOS), are critical components in OT networks, facilitating seamless communication between various control systems, devices, and sensors. The functionality offered by HiOS can significantly contribute to achieving NIS2 compliance in several ways:

1. Network Segmentation and Isolation

HiOS enables the segmentation of OT networks into smaller, isolated segments. This limits the spread of cyber threats and ensures that a breach in one segment does not compromise the entire network. Proper segmentation aligns with NIS2's requirement for robust risk management practices.

2. Enhanced Security Features

HiOS comes equipped with advanced security features such as Denial of Service protection, Dynamic ARP Inspection, and DHCP Snooping. These features help detect and mitigate cyber threats in real-time, aligning with NIS2's emphasis on proactive threat management and incident response.

3. Access Control and Authentication

Ensuring that only authorized devices and personnel can access the network is a fundamental aspect of NIS2 compliance. HiOS supports network access control mechanisms, including 802.1X authentication, which verifies the identity of devices attempting to connect to the network. This reduces the risk of unauthorized access and potential cyberattacks.

4. Network Monitoring and Visibility

Effective monitoring and visibility of network traffic are crucial for identifying anomalies and potential security incidents. HiOS provides detailed logging and monitoring capabilities, allowing organizations to detect and respond to suspicious activities promptly. This aligns with NIS2's requirement for continuous monitoring and incident reporting.

5. High Availability and Redundancy

HiOS enables high availability and redundancy, ensuring uninterrupted network operation even in the event of a failure. Features like Multiple Spanning Tree Protocol (MSTP) and Media Redundancy Protocol (MRP) enhance network resilience, aligning with NIS2's focus on ensuring the continuity of essential services.

Detailed Functionality

Category	Functionality	Description
Access Control and Authentication	802.1X Authentication / LDAP	802.1X Authentication: Implementing port-based network access control is essential to ensure that only authenticated devices can connect to the network, thereby preventing unauthorized devices from accessing critical control systems.
	TACACS+ *	Separating authentication from authorization, TACACS+ enables fine-grained authorization policies based on user roles, groups, or other criteria, allowing precise control over user access to commands and resources on network devices.
	MAC Address Filtering	Utilizing MAC address filtering allows only known devices to communicate on the network, effectively blocking unauthorized devices from gaining network access.
	Role-Based Access Control (RBAC)	Defining access permissions based on user roles ensures that only authorized personnel can perform critical operations, thus reducing the risk of accidental or malicious changes.
	IP Access Restriction	Limits access to the switch management agent. Allows access to switch management only from specific IP address ranges, and for specific management applications.
	Management VLAN	Putting the management agent of network infrastructure devices into a separate VLAN hides these devices from other users on the network.
Network Segmentation	VLAN Support	Virtual Local Area Networks (VLANs) facilitate the segmentation of the network, isolating different parts and reducing the risk of a security breach spreading across the entire system.
	Private VLANs	Further isolating ports within the same VLAN prevents unauthorized communication between devices, enhancing internal security.
Intrusion Detection and Prevention	Port Security	Configuring port security to limit the number of MAC addresses per port protects against MAC flooding attacks, which can overwhelm network switches and disrupt operations.
	DHCP Snooping	Implementing DHCP snooping monitors DHCP messages, ensuring that only authorized DHCP servers can assign IP addresses, thus preventing rogue DHCP servers from disrupting the network.
	Dynamic ARP Inspection	Enabling DAI validates ARP packets on the network, protecting against ARP spoofing attacks that can redirect network traffic and compromise sensitive data.
	Denial of Service Protection	Protects against some Denial of Service attacks. Applies filters to prevent widely used scanning techniques and protocol attacks.
Logging and Monitoring	Secure Syslog support	Protects Syslog messages from eavesdropping and tampering by transmitting them over a connection which is encrypted using TLS.
	sFlow	sFlow is a packet sampling and export technology that collects traffic statistics by randomly sampling packets and interface counters from network devices.
Security and Firmware Updates	Secure Boot	Ensures that switches boot using only trusted software. Prevents unauthorized or malicious code from running during the startup process.
	Firmware Integrity Checking / Signed software	Verifies the uploaded software's authenticity and integrity using a digital signature, before allowing it to be installed in a switch.
Traffic Filtering and Control	Access Control Lists (ACLs) L2 & 3	Defining ACLs to filter traffic based on IP addresses, port numbers, and protocols provides granular control over network access and protects against unauthorized access and malicious traffic.
	Rate limiter	A rate limiter restricts the amount of traffic that can pass through a specific port or interface. It helps control network bandwidth usage. It also mitigates attacks which are based on bandwidth consumption.
Encryption	SSH and HTTPS	Securing management interfaces using SSH for command-line access and HTTPS for web-based management ensures that management communications are encrypted and protected from eavesdropping.
	MACsec (802.1AE) *	Implementing MACsec to encrypt data at the link layer provides confidentiality and integrity for data transmitted between network devices, protecting against interception and tampering.

High Availability and Redundancy	Link Aggregation Control Protocol (LACP)	Combining multiple physical links into a single logical link provides redundancy and increased bandwidth, ensuring continued network operation even if one link fails.
	Spanning Tree Protocol (STP)	Using STP to create a loop-free network topology prevents network loops that can cause broadcast storms and network instability.
	MRP	Media Redundancy Protocol (MRP) is a standard protocol used in industrial networking to provide network redundancy and ensure high availability of communication links.
	Loop Protection	Loop Protection detects and temporarily blocks unintended loops which would otherwise cause the network to fail.
Compliance and Reporting	Audit Trails	Maintaining detailed logs of all configuration changes and access attempts provides a record for auditing and forensic analysis, helping to demonstrate compliance and investigate incidents.
	Persistent logging	Hackers frquently reboot compromised switches to hide traces of their activity. Persistent log files retain their contents even after a reboot.
Hardware Reliability	Redundant power supplies	Equipping switches with redundant power supplies ensures continuous operation even if one power supply fails.
	Security status indicator	A physical security status indicator, such as an LED, provides an externally visible indication of a security misconfiguration.
Certification	ISA/IEC 62443-4-1	A device developed according to ISA/IEC 62443-4-1 benefits from enhanced cybersecurity resilience, ensuring it is robust against cyber threats throughout its lifecycle.
	ISA/IEC 62443-4-2	A device certified to ISA/IEC 62443-4-2 supports robust cybersecurity features tailored to industrial control systems, ensuring it meets stringent security requirements for reliable and secure operation.

* Available as a software update in 2025.

Conclusion

NIS2 compliance is a critical objective for organizations operating in essential and important sectors within the EU. Hirschmann Industrial Ethernet switches running HiOS, with their robust security features, network segmentation capabilities, and high availability, are integral to achieving this compliance. By strategically implementing these switches within OT networks, organizations can enhance their cybersecurity posture, protect against emerging threats, and ensure the resilience and reliability of their critical infrastructure.

In an era where cyber threats are ever-evolving, the role of industrial Ethernet switches in OT networks cannot be overstated. They are not just networking devices but pivotal elements in the broader cybersecurity strategy required to meet the stringent demands of NIS2 compliance.