HIRSCHMANN
A BELDEN BRAND

ICS Security Guide to Hirschmann Switches

Be certain.
Belden.

Availability, Integrity and Confidentiality
Switch Family
Classic Switch Software

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

You can get the latest version of this manual on the Internet at the Hirschmann product site (www.hirschmann.com).

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany
Tel.: +49 1805 141538

Contents

1 Motivation and Goals

This document is based on a template that was created by TÜV SÜD Rail on request from Hirschmann for Hirschmann devices.

1.1 Motivation

The switch is used in industrial automation and control technology in order to connect control technology, systems and office IT. This communication is requested by our customers more and more, because continuous communication speeds up production, lowers costs and can support our customers' business processes via close links.

However, cyber-attacks such as Stuxnet have shown that industrial automation and control technology systems are open to attack and can be manipulated. In particular, the links between industrial environments and office IT can be used to attack control technology. Therefore, you should secure these links and communication. The switch can help with this in a particular way.

However, for this it is absolutely necessary to determine the security requirements, create a secure concept, and integrate the product with a secure configuration of the product into this concept.

1.2 Objectives

It is practically impossible to set up secure networks without the support of the manufacturer of the network products. This manual is part of the undertaking by Hirschmann Automation and Control GmbH to improve the security of its products and support the planners and users in configuring and using the products securely.

However, there is no universally suitable configuration that can be seen as secure in all situations. This IT security manual helps the planner and the operator of the switches relevant to this document in performing the following actions:

- ☐ To determine sufficient and appropriate security requirements
- ☐ To implement the most secure configuration possible
- ☐ To perform an integration into the monitoring and operate this as securely as possible

1.3 Areas of Application

The switch supports you via its wide range of communication options and enables problem-free data exchange. It covers a broad spectrum of industries, including the energy sector, automation applications and rail transportation.

Common to all of these areas is the goal of connecting end devices. However, a distinction can be made between 2 application scenarios. The first case is an integration into an overall system, such as in a power transformation substation. The second is a closed system such as that integrated by a plant manufacturer into his system and then delivered to the customer. There the plant, and therefore also the switch, is incorporated into an overall system.

In both cases, the security of the switch contributes to the security of the overall system.

1.4 Further Information

You can register for a software update newsletter that informs you about new software versions that appear and their release notes.

If you find any possible vulnerabilities or security problems in Hirschmann Automation and Control GmbH products, please report then via the Belden Security website or directly via e-mail:
https://www.belden.com/security
BEL-SM-PSIRT@belden.com

The site contains the following:

- “Advisories”
  Reports about security vulnerabilities in our products which have not yet been fixed.
- “Bulletins”
  Reports about security vulnerabilities in our products which have been fixed.
- “Report Security Vulnerabilities”
  An online form for people to report vulnerabilities.

The site also contains a description of how Hirschmann Automation and Control GmbH handles reported vulnerabilities.

2 Description of the Product

The Hirschmann™ software provides a range of functions that are normally used in backbone systems of company networks. These include management, diagnostic and filter functions, various redundancy procedures, security mechanisms and real-time applications. The software used in the MACH, MICE, Rail and OCTOPUS managed switch series optimizes the bandwidth, the configuration functions and the service functions. In version 9 of our Classic Software, configuring one switch is sufficient to configure the entire ring. Additionally, configurations can also be performed offline, i.e. without an active connection to the switch.

Switching	
Layer 2 Basic (L2B)	Suitable for RSB20, OCTOPUS. The economical introduction to managed switch functions, including statistics, filters and redundancy technologies. The alternative to unmanaged switches.
Layer 2 Enhanced (L2E)	Suitable for RS20/RS30/RS40, MS20/MS30. Basic level plus a wide range of management, filter and diagnostic functions. Also supported: fast redundancy procedures, industrial profiles and security functions. Ideal for standard industrial applications.
Layer 2 Professional (L2P)	Suitable for RS20/RS30/RS40, MS20/MS30, OCTOPUS, PowerMICE, RSR20/RSR30, MACH100, MACH1000, MACH4000. Enhanced software plus enhanced diagnostic and filter properties, security functions and redundancy procedures. A software package for applications that attach great importance to the uncompromising security of the production plant and maximum availability.

Routing	
Layer 3 Enhanced (L3E)	Suitable for PowerMICE, MACH4000. Layer 2 Professional software plus additional security, static routing, and router and connection redundancy. The Layer 3 software is intended for smaller data networks and applications with increased security requirements.
Layer 3 Professional (L3P)	Suitable for PowerMICE, MACH1040, MACH4000. Layer 3 Enhanced plus a wide range of dynamic routing protocols, faster router redundancy and improved connection redundancy.

3 Framework Conditions

This document refers to software 7.1.05 for software variants L2E, L2P, L3E and L3P.

The basic software version for variant L2B is version 05.3.02.

The functions described in this document are relevant to later software versions.
Most of the functions described in this document are relevant to earlier software versions.

The EtherNet/IP and PROFINET product variants have default settings specific to industry protocols. Therefore, this IT security manual does not apply to product variants that contain EtherNet/IP or PROFINET in the product code. When you apply the content of this IT security manual to these switches, the switches lose their industry protocol-specific settings.

For the measures in chapter “Secure Configuration” on page 27, the following documents are used for the configuration:

Title	ID	Version
Reference Manual Command Line Interface Industrial ETHERNET Switch RSB20, OCTOPUS OS20/OS24 Managed	CLI L2B	Release 5.3 05/2012
Reference Manual Web-based Interface Industrial ETHERNET Switch RSB20, OCTOPUS OS20/OS24 Managed	GUI L2B	Release 5.3 05/2012
Reference Manual Command Line Interface Industrial ETHERNET (Gigabit) Switch RS20/RS30/RS40, RSB20, MS20/MS30, OCTOPUS	CLI L2E	Release 7.1 12/2011
Reference Manual GUI Graphical User Interface Industrial ETHERNET (Gigabit) Switch RS20/RS30/RS40, MS20/MS30, OCTOPUS	GUI L2E	Release 7.1 12/2011
Reference Manual Command Line Interface Industrial ETHERNET (Gigabit) Switch RS20/RS30/RS40, MS20/MS30, OCTOPUS, PowerMICE, RSR20/RSR30, MACH 100, MACH 1000, MACH 4000	CLI L2P	Release 7.1 12/2011

Title	ID	Version
Reference Manual GUI Graphical User Interface Industrial ETHERNET (Gigabit) Switch RS20/RS30/RS40, MS20/MS30, OCTOPUS, PowerMICE,RSR20/RSR30, MACH 100, MACH 1000, MACH 4000	GUI L2P	Release 7.1 12/2011
Reference Manual Command Line Interface Industrial ETHERNET (Gigabit) Switch PowerMICE, MACH 1040, MACH 4000	CLI L3E	Release 7.1 12/2011
Reference Manual Command Line Interface Industrial ETHERNET (Gigabit) Switch PowerMICE, MACH 1040, MACH 4000	CLI L3P	Release 7.1 12/2011
Reference Manual GUI Graphical User Interface Industrial ETHERNET (Gigabit) Switch PowerMICE, MACH 1040, MACH 4000	GUI L3E	Release 7.1 12/2011
Reference Manual GUI Graphical User Interface Industrial ETHERNET (Gigabit) Switch PowerMICE, MACH 1040, MACH 4000	GUI L3P	Release 7.1 12/2011
User Manual Basic Configuration	AHG L2P/ L3E	Release 7.1 12/2011
Basic Configuration Industrial ETHERNET (Gigabit) Switch PowerMICE, MACH 1040, MACH 4000	Basic L3P	Release 7.1 12/2011

3.1 System Preparation Process

Operators of an IT infrastructure in an industrial environment (shortened to “system” hereafter) should have a system preparation process (shortened to “SPP” hereafter). This is used to introduce, change and maintain the system with all the security requirements. The SPP is made up of the following main phases:

- ☐ Analysis of requirements
- ☐ Architecture
- ☐ Implementation
- ☐ Test
- ☐ Operation and maintenance
- ☐ Decommissioning

The operator of a system documents the SPP’s main phases and activities. He integrates the security aspects to be considered. He describes the responsibilities (roles and rights) that ensure that the SPP fulfills the defined quality and security requirements. For example, suitable quality management that also addresses security.

The operator audits the SPP regularly, makes improvements and monitors the implementation of the improvements. He also ensures that only qualified personnel are used to execute the SPP.

What is known as asset (or configuration) management must be established so that the system can be recorded with all of its components and software versions. Asset management is the basis of release and change management, and is therefore the foundation for the quality assurance for every change made to the system.

3.1.1 Analysis of Requirements

Perform an holistic threat analysis for the system that considers both the processes and the technologies used.

Starting from an application case (such as installation, administration, monitoring, etc.), based on the security goals you first identify all of the principle threat scenarios that could lead to risks. In describing the application cases, also consider assumptions that you have made with regard to the environs of the system for the application cases. Based on the identified threat scenarios and risks, derive security requirements and measures for the system (documented in a security requirements specification). Make sure that the security measures you derive from the security requirements completely cover all of the security requirements.

The security requirements specification must be subjected to a review based on a dual control principle. It is also used as the basis for deriving the tests for the system's security measures.

In chapter "Secure Configuration" on page 27 you will find examples of such application cases, including threats and the measures that you should take in order to operate the switch securely.

3.1.2 Architecture

An architecture document describes the system with all of its components and security measures. In particular, it represents interfaces between the individual components. A defense in depth strategy involves consecutive security measures, so that if an attacker overcomes one obstacle he is faced with the next one. If an attacker overcomes one security measure, the security of the overall system is maintained. Describe the interaction of the individual security measures.

Draw a complete picture of the security of the overall system that also shows the defense in depth strategy.

You will find an example of a defense in depth strategy for industrial use in article [1] (see references in Appendix).

3.1.3 Implementation

The implementation of the security measures is generally carried out by using projects. Therefore, monitor the implementation of the measures based on a project plan. Document the implementation of the security measures.

3.1.4 Test

Verify the effectiveness and correctness of the implemented measures by means of tests and audits. You perform the security tests and audits according to a test plan. If any gaps are discovered, propose improvement measures and document, implement and monitor them.

3.1.5 Operation and Maintenance

In the threat analysis, also identify risks resulting from the operation and maintenance, for example risks due to insufficiently secure remote maintenance. In particular, make every change to the system in accordance with a documented change management process, which authorizes changes based on a dual control principle. Document changes to the system. Define a security incident process with which you can react appropriately to security incidents in line with their criticality.

3.1.6 Decommissioning

Also consider security aspects when decommissioning a system or parts of the system. For example, delete sensitive data from memories so that you can rule out the data from being restored with a reasonable effort, or destroy the data carriers accordingly. Also represent the decommissioning in the change management process in order to rule out or consider undesired effects on other systems.

3.2 Physical Framework Conditions

Make sure that the physical protection of the device or the system fulfills the requirements in the underlying risk analysis. This can vary significantly depending on the environment and the threat situation.

3.3 Requirements for Personnel

IT security is not a state that can be created exclusively with just a product. The know-how and experience of the planner and the operator are also required. Hirschmann provides you with support via a range of training courses and certification options.

You will find our current training courses here:

http://www.beldensolutions.com/en/Service/competence-center/training/index.phtml

3.4 Patch Management

To maintain security during operation, it is important to be informed by the manufacturer in good time about the installation of recommended patches and releases, and to test these and implement them if applicable. Perform a risk evaluation, considering the risk of both implementation and non-implementation of the patch or the release. You should always implement security patches unless there are serious reasons against this.

3.5 (Security) Incident Handling

To maintain the IT security during operation, draw up a concept for handling disturbances, in particular security incidents, and rehearse the handling of disturbances. To avoid or limit damage, the handling of security incidents should be carried out quickly and efficiently. The possible damage resulting from a security incident can affect both the confidentiality or integrity of data and its availability.

3.6 Protection from Malware

Clearly regulate skills and responsibilities for protecting the industrial environment from malware (malicious software). You require a process that identifies preventive measures and reactive measures and the people responsible for them. Develop a concept for protecting against malware that specifies both technical and organizational regulations.

3.7 Managing Users and Rights

The management of users and rights organizes roles and their related rights that you require in the relevant environment, according to the description of the activity. Along with the creation of roles, this includes the assignment of people to the roles over the entire life cycle of the system.

Typical tasks that you consider are the creation, modification, monitoring and withdrawal of rights. These tasks must be represented in a process that regulates the identification of people and entities and authorizes the assignment of rights.

3.8 Requirements for the Documentation

Keep a record of information relevant to security. Organize the steering of these documents. These documents are used in the case of a security incident to verify that the security processes have been adhered to.

4 Secure Configuration

4.1 Starting Up

4.1.1 Threats

In the state on delivery, your device is prepared for a simple start. For the secure operation of the switch, further configuration settings are also required. The installation application case involves the following threats:

☐ Manipulation of the configuration
☐ Reading out of the configuration
☐ Limitation of the availability

4.1.2 Security Quick Check for “Starting Up”

Do you require?	If necessary	If not necessary
DHCP	Activate DHCP (Client)	Deactivate DHCP (Client)
BOOTP	Activate BOOTP	Deactivate BOOTP
PROFINET	Activate PROFINET	Deactivate PROFINET
EtherNet/IP	Activate EtherNet/IP	Deactivate EtherNet/IP
LLDP	Activate LLDP	Deactivate LLDP
AutoConfiguration Adapter (ACA)	Do not skip ACA when booting	Skip ACA when booting
Basic principle		
The measures follow the minimal principle in order to reduce the system load of the switch and its area of attack. Generally, you should deactivate services not required.		
General measures		
Read access for HiDiscovery Change the default access Deactivate password sync		

4.1.3 Measures

Activate DHCP (Client)

The switch can dynamically receive IP information via a DHCP server and also a TFTP server for configurations. An attacker can misuse this service.

For higher availability, select a static IP configuration for infrastructure components. Dynamic IP configurations require the existence of protocols, which present a target to attackers.

Action	Default setting	Recommended setting	Available		Further information
Activate DHCP client	On	Activate DHCP only if you require dynamic address assignment for your infrastructure components	L2B	Yes	GUI L2B Network CLI L2B network protocol
			L2E	Yes	GUI L2E Network CLI L2E network protocol
			L2P	Yes	GUI L2P Network CLI L2P network protocol
			L3E	Yes	GUI L3E Network CLI L3E network protocol
			L3P	Yes	GUI L3P network CLI L3P network protocol

Activate BOOTP

The switch can dynamically receive IP information via a BOOTP server and also a TFTP server for configurations. An attacker can misuse this service.

For higher availability, select a static IP configuration for infrastructure components. Dynamic IP configurations require the existence of protocols, which present a target to attackers.

Action	Default setting	Recommended setting	Available		Further information
Activate BOOTP	Off	Activate BOOTP only if you require dynamic address assignment for your infrastructure components	L2B	Yes	GUI L2B Network CLI L2B network protocol
			L2E	Yes	GUI L2E Network CLI L2E network protocol
			L2P	Yes	GUI L2P Network CLI L2P network protocol
			L3E	Yes	GUI L3E Network CLI L3E network protocol
			L3P	Yes	GUI L3P Network CLI L3P network protocol

Activate PROFINET

PROFINET can be used to read and change specific properties of the switch. Only activate this option if you require PROFINET.

Action	Default setting	Recommended setting	Available		Further information
Activate PROFINET	Off	Activate PROFINET if the protocol is to be used	L2B	No	
			L2E	Yes	GUI L2E PROFINET IO CLI L2E profinetio
			L2P	Yes	GUI L2P PROFINET IO CLI L2P profinetio
			L3E	Yes	GUI L3E PROFINET IO CLI L3E profinetio
			L3P	Yes	GUI L3P PROFINET IO CLI L3P profinetio

Activate EtherNet/IP

EtherNet/IP can be used to read and change specific properties of the switch. Only activate this option if you require EtherNet/IP.

Action	Default setting	Recommended setting	Available		Further information
Activate EtherNet/IP	Off	Activate EtherNet/IP if the protocol is to be used	L2B	No	
			L2E	Yes	GUI L2E EtherNet/IP CLI L2E ethernet-ip
			L2P	Yes	GUI L2P EtherNet/IP CLI L2P ethernet-ip
			L3E	Yes	GUI L3E EtherNet/IP CLI L3E ethernet-ip
			L3P	Yes	GUI L3P EtherNet/IP CLI L3P ethernet-ip

Activate LLDP

The switch uses the Link Layer Discovery Protocol to send information about itself regularly to the network. This information can be an important aid for troubleshooting. However, this information also provides an attacker with valuable data and should therefore be used only when absolutely necessary.

LLDP-Med is and extension of LLDP. It is primarily intended for Voice over IP applications and should always remain deactivated if possible.

Action	Default setting	Recommended setting	Available		Further information
Activate LLDP	On	LLDP provides information about your switch. Only use when required.	L2B	Yes	GUI L2B Topology Discovery CLI L2B lldp
			L2E	Yes	GUI L2E Topology Discovery CLI L2E lldp
			L2P	Yes	GUI L2P Topology Discovery CLI L2P lldp
			L3E	Yes	GUI L3E Topology Discovery CLI L3E lldp
			L3P	Yes	GUI L3P Topology Discovery CLI L3P lldp

Do not skip ACA when booting

During the booting procedure, the device can load the configuration from the ACA. If the ACA is being used in your environment, then execute this procedure using the CLI command (see table below).

Action	Default setting	Recommended setting	Available		Further information
Do not skip ACA	Off	If the ACA is being used, the device can use it to load the configuration when booting.	L2B	No	
			L2E	Yes	CLI L2E skip-aca-on-boot
			L2P	Yes	CLI L2P skip-aca-on-boot
			L3E	Yes	CLI L3E skip-aca-on-boot
			L3P	Yes	CLI L3P skip-aca-on-boot

Deactivate DHCP (Client)

Note: The switch can dynamically receive IP information via a DHCP server and also a TFTP server for configurations. The DHCP server response can in turn contain a path to a remote configuration. Then the switch loads the configuration via TFTP when booting.

An attacker can misuse this service.

For higher availability, select a static IP configuration for infrastructure components. Dynamic IP configurations require the existence of protocols, which present a target to attackers.

Action	Default setting	Recommended setting	Available		Further information
Deactivate DHCP client	On	Off	L2B	Yes	GUI L2B Network CLI L2B network protocol
			L2E	Yes	GUI L2E Network CLI L2E network protocol
			L2P	Yes	GUI L2P Network CLI L2P network protocol
			L3E	Yes	GUI L3E Network CLI L3E network protocol
			L3P	Yes	GUI L3P Network CLI L3P network protocol

Deactivate BOOTP

Note: The switch can dynamically receive IP information via a BOOTP server and also a TFTP server for configurations. The BOOTP server response can in turn contain a path to a remote configuration. Then the switch loads the configuration via TFTP when booting.

An attacker can misuse this service.

For higher availability, select a static IP configuration for infrastructure components. Dynamic IP configurations require the existence of protocols, which present a target to attackers.

Action	Default setting	Recommended setting	Available		Further information
Deactivate BOOTP	Off	Off	L2B	Yes	GUI L2B Network CLI L2B network protocol
			L2E	Yes	GUI L2E Network CLI L2E network protocol
			L2P	Yes	GUI L2P Network CLI L2P network protocol
			L3E	Yes	GUI L3E Network CLI L3E network protocol
			L3P	Yes	GUI L3P Network CLI L3P network protocol

Deactivate PROFINET

PROFINET can be used to read and change specific properties of the switch. Only activate this option if you require PROFINET.

Action	Default setting	Recommended setting	Available		Further information
Deactivate PROFINET	Off	Off	L2B	No	
			L2E	Yes	GUI L2E PROFINET IO CLI L2E profinetio
			L2P	Yes	GUI L2P PROFINET IO CLI L2P profinetio
			L3E	Yes	GUI L3E PROFINET IO CLI L3E profinetio
			L3P	Yes	GUI L3P PROFINET IO CLI L3P profinetio

Deactivate EtherNet/IP

EtherNet/IP can be used to read and change specific properties of the switch. Only activate this option if you require EtherNet/IP.

Action	Default setting	Recommended setting	Available		Further information
Deactivate EtherNet/IP	Off	Off	L2B	No	
			L2E	Yes	GUI L2E EtherNet/IP CLI L2E ethernet-ip
			L2P	Yes	GUI L2P EtherNet/IP CLI L2P ethernet-ip
			L3E	Yes	GUI L3E EtherNet/IP CLI L3E ethernet-ip
			L3P	Yes	GUI L3P EtherNet/IP CLI L3P ethernet-ip

Deactivate LLDP

The switch uses the Link Layer Discovery Protocol (LLDP) to send information about itself regularly to the network. This information can be an important aid for troubleshooting. However, this information also supplies an attacker with valuable data.

Action	Default setting	Recommended setting	Available		Further information
Deactivate LLDP	On	Off	L2B	Yes	GUI L2B Topology Discovery CLI L2B lldp
			L2E	Yes	GUI L2E Topology Discovery CLI L2E lldp
			L2P	Yes	GUI L2P Topology Discovery CLI L2P lldp
			L3E	Yes	GUI L3E Topology Discovery CLI L3E lldp
			L3P	Yes	GUI L3P Topology Discovery CLI L3P lldp
Deactivate LLDP-MED	On	Off	L2B	No	
			L2E	No	
			L2P	Yes	GUI L2P LLDP MED CLI L2P lldp med
			L3E	Yes	GUI L3E LLDP MED CLI L3E lldp med
			L3P	Yes	GUI L3P LLDP MED CLI L3P lldp med

Note: PROFINET requires LLDP in order to operate.

Skip ACA when booting

If you are not using an ACA, you can use this to speed up the booting procedure and make unauthorized loading of a configuration during the start more difficult.

Action	Default setting	Recommended setting	Available		Further information
Skip ACA	Off	On	L2B	No	
			L2E	Yes	CLI L2E skip-aca-on-boot
			L2P	Yes	CLI L2P skip-aca-on-boot
			L3E	Yes	CLI L3E skip-aca-on-boot
			L3P	Yes	CLI L3P skip-aca-on-boot

Read access for HiDiscovery

HiDiscovery provides information about a device (read mode) or also allows changes to configuration parameters such as the IP address (read/write mode). An attacker has the option to gather information about a device or divert data traffic by diverting the default gateway to a system under his control. Therefore, it is recommended to allow read access only for HiDiscovery in the live environment.

Action	Default setting	Recommended setting	Available		Further information
HiDiscovery read access	On (reading and writing)	Off (reading)	L2B	Yes	GUI L2B Network CLI L2B network protocol
			L2E	Yes	GUI L2E Network CLI L2E network protocol
			L2P	Yes	GUI L2P Network CLI L2P network protocol
			L3E	Yes	GUI L3E Network CLI L3E network protocol
			L3P	Yes	GUI L3P Network CLI L3P network protocol

Change the default access

One of the first measures that an attacker carries out if he wants to gain access to a third-party system is a login attempt with standard access data. Therefore, change the access data during the installation.

Note: Changing the password in CLI only changes the SNMP v1/v2 password. In contrast, when the user password is changed in CLI, the user password and the SNMP v1/v2 passwords are changed. If a separate password is used for each of the user and SNMP v1/v2, deactivate the “Password Sync” function.
See “Deactivate password sync” on page 37.

Action	Default setting	Recommended setting	Available		Further information
Set password	User: admin=private user= public	Secure password of 16 characters	L2B	Yes	GUI L2B password / SNMP v3 access CLI L2B users passwd
			L2E	Yes	GUI L2E password / SNMP v3 access CLI L2E users passwd
			L2P	Yes	GUI L2P password / SNMP v3 access CLI L2P users passwd
			L3E	Yes	GUI L3E password / SNMP v3 access CLI L3E users passwd
			L3P	Yes	GUI L3P password / SNMP v3 access CLI L3P users passwd

Note: With the standard settings, the user password is synchronized with the SNMP v1/v2 community.

Deactivate password sync

In order to be able to assign different passwords for different users and SNMP access rights, deactivate the Password Sync function.

Action	Default setting	Recommended setting	Available		Further information
Deactivate password sync	On	Off	L2B	Yes	GUI L2B password / SNMP v3 access CLI L2B users passwd
			L2E	Yes	GUI L2E password / SNMP v3 access CLI L2E users passwd
			L2P	Yes	GUI L2P password / SNMP v3 access CLI L2P users passwd
			L3E	Yes	GUI L3E password / SNMP v3 access CLI L3E users passwd
			L3P	Yes	GUI L3P password / SNMP v3 access CLI L3P users passwd

4.2 Separating networks

4.2.1 Threats

Separating networks or network segments is an important aspect of network security. It can be used, for example, to form different confidentiality classes. The following threats exists for secure network separation:

- ☐ Incorrect configuration of port
- ☐ Incorrect configuration of VLAN
- ☐ Incorrect configuration of ACL
- ☐ Breaking through VLAN boundaries
- ☐ ARP flooding
- ☐ Faking an identity

When Layer 3 software (routing) is used, there are additional threats:

- ☐ Manipulation of VRRP/HiVRRP protocol
- ☐ Manipulation of routing via fake Router Discovery frames
- ☐ Manipulation of routing via fake RIPv1 or RIPv2 frames
- ☐ Manipulation of the routing paths via Proxy ARP frames
- ☐ Risk of incorrect configuration due to multiple IP subnetworks on the same subnetwork (multinetting)
- ☐ Network infrastructure revealed via Router Discovery frames

All of the threats named attempt to break through the separation of the networks or network segments from each other, or to manipulate the communication paths between network segments (Layer 2 and Layer 3).

4.2.2 Security Quick Check for “Separation of Networks”

This table helps you to identify which measures in your system environment should ideally be implemented on the switch in connection with the separation of networks for security reasons.

Do you require?	If necessary	If not necessary
VLANs	Do not use VLAN 1 Do not use VLAN 0 Deactivate GVRP Ports not in more than one VLAN Unique assignment of the switch ports to VLANs Do not use port mirroring Do not use DHCP Relay	Deactivate GVRP
Routing between subnetworks necessary?	Activate routing Deactivate Proxy ARP	Deactivate routing
Dynamic routing protocol RIP necessary?	Use RIPv2 with authentication	Use only static routes If applicable, Use OSPF only with encrypted authentication
Dynamic routing protocol OSPF necessary?	Use OSPF only with encrypted authentication If applicable, Use OSPF virtual links only with authentication	Use only static routes If applicable, Use RIPv2 with authentication
Are there different security zones for the connected networks?	Use IP Access Control Lists (ACLs)	
Dynamic multicast registration with GMRP	Activate Generic Multicast Registration Protocol (GMRP)	Deactivate Generic Multicast Registration Protocol (GMRP)
Basic principle		
Deactivate the services and functions that you do not require		
Further measures		
To increase the security, implement all the measures in the “Administration Access” section, because an attacker can use such an access to disable all the measures described here.		

4.2.3 Measures

Do not use VLAN 1

Use VLAN 1 only for the HIPER Ring protocol and ring coupling. This measure makes it more difficult to manipulate the ring protocols. Therefore, make the following settings:

Action	Default setting	Recommended setting	Available		Further information
Move the admin interface to a different VLAN	1	In the range 2-4042	L2B	No	
			L2E	Yes	GUI L2E VLAN CLI L2E network mgmt_vlan
			L2P	Yes	GUI L2P VLAN CLI L2P network mgmt_vlan
			L3E	Yes	GUI L3E VLAN CLI L3E network mgmt_vlan
			L3P	Yes	GUI L3PE VLAN CLI L3P network mgmt_vlan
Change the time server configuration to a different VLAN	1	Same VLAN as for admin interface	L2B	No	
			L2E	Yes	GUI L2E SNTP Configuration CLI L2E sntp anycast vlan
			L2P	Yes	GUI L2P SNTP Configuration CLI L2P sntp anycast vlan
			L3E	Yes	GUI L3E SNTP Configuration CLI L3E sntp anycast vlan
			L3P	Yes	GUI L3P SNTP Configuration CLI L3P sntp anycast vlan
Change all the switch ports from VLAN1 to a different VLAN	1	In the range 2-4042	L2B	No	
			L2E	Yes	GUI L2E VLAN Static CLI L2E vlan port pvid all
			L2P	Yes	GUI L2P VLAN Static CLI L2P vlan port pvid all
			L3E	Yes	GUI L3E VLAN Static CLI L3E vlan port pvid all
			L3P	Yes	GUI L3P VLAN Static CLI L3P vlan port pvid all

Note: For the ports via which the HIPER Ring protocol is running and for ports for ring/network couplings, the port must remain on VLAN 1 as otherwise operational problems occur.

Note: If you change the VLAN for the management interface, this can interrupt your connection to the switch. Make sure that you can also administer the switch with the new configuration.

Note: VLANs 4043-4095 are used for port-based routing internally in the switch in order to implement the separation of the maximum possible 52 physical ports in the switch internally, and therefore they may not be used by the user. With port-based routing, the ingress filtering is active. Therefore the switch discards frames with VLAN tags.

Do not use VLAN 0

VLAN 0 has a further special role in the switch and must be considered separately.

Note: The use of PROFINET and GOOSE can cause limitations.

Action	Default setting	Recommended setting	Available		Further information
Deactivate VLAN0 transparent mode	Off	Off	L2B	No	
			L2E	Yes	GUI L2E VLAN Global CLI L2E vlan0-transparent-mode
			L2P	Yes	GUI L2P VLAN Global CLI L2P vlan0-transparent-mode
			L3E	Yes	GUI L3E VLAN Global CLI L3E vlan0-transparent-mode
			L3P	Yes	GUI L3P VLAN Global CLI L3P vlan0-transparent-mode

Deactivate GVRP

GVRP (GARP VLAN Registration Protocol) allows another device to create a VLAN in a switch or register a port in a VLAN. The switch functions as a security component for the network separation between VLANs. Deactivate GVRP so that no other device can change the VLAN configuration.

Action	Default setting	Recommended setting	Available		Further information
Configure VLAN participation	auto	include or exclude	L2B	No	
			L2E	Yes	GUI L2E VLAN Port CLI L2E vlan participation
			L2P	Yes	GUI L2P VLAN Port CLI L2P vlan participation
			L3E	Yes	GUI L3E VLAN Port CLI L3E vlan participation
			L3P	Yes	GUI L3P VLAN Port CLI L3P vlan participation

Note: If you still want to use GVRP, deactivate GVRP on all untrusted ports.

Ports not in more than one VLAN

The switch allows you to assign multiple VLANs to a port. This can cancel the separation between the VLANs. Therefore, assign to each switch port (user port) exactly one VLAN (setting U = untagged or T = tagged).

Action	Default setting	Recommended setting	Available in SW version		Further information
Assignment to exactly one VLAN	- : not a member but GVRP allowed	When used, either U or T	L2B	No	
			L2E	Yes	GUI L2E VLAN Port CLI L2E vlan
			L2P	Yes	GUI L2P VLAN Port CLI L2P vlan
			L3E	Yes	GUI L3E VLAN Port CLI L3E vlan
			L3P	Yes	GUI L3P VLAN Port CLI L3P vlan

Unique assignment of the switch ports to VLANs

The separation of the VLANs from each other mainly depends on the settings for the ports (- = not a member, T = tagged, U = untagged and F = forbidden). In general, the default setting for every port in every VLAN should be F = forbidden. This means that when a new VLAN is created, every port in this VLAN should be initially set to F (not a member and GVRP forbidden) and be assigned to exactly one VLAN only when required.

Configure the switch so that when a frame without a VLAN tag is received at a port, this frame is not assigned to another VLAN in the switch.

Action	Default setting	Recommended setting	Available		Further information
Set default setting of switch port to F	- : not a member but GVRP allowed	When GVRP is deactivated, - = not a member is sufficient, otherwise F = forbidden as the default setting and then assignment to one VLAN if required	L2B	No	
			L2E	Yes	GUI L2E VLAN Static CLI L2E vlan participation
			L2P	Yes	GUI L2P VLAN Static CLI L2P vlan participation
			L3E	Yes	GUI L3E VLAN Static CLI L3E vlan participation
			L3P	Yes	GUI L3P VLAN Static CLI L3P vlan participation
Assign untagged frames to VLAN	1	Same VLAN as was activated for this port	L2B	No	
			L2E	Yes	GUI L2E VLAN Static CLI L2E vlan tagging
			L2P	Yes	GUI L2P VLAN Static CLI L2P vlan tagging
			L3E	Yes	GUI L3E VLAN Static CLI L3E vlan tagging
			L3P	Yes	GUI L3P VLAN Static CLI L3P vlan tagging

Action	Default setting	Recommended setting	Available		Further information
Allow tagged frames only at T port	admitAll	At ports configured with T=tagged: admitOnlyVlanTagged	L2B	No	
			L2E	Yes	GUI L2E VLAN Port CLI L2E vlan acceptframe
			L2P	Yes	GUI L2P VLAN Port CLI L2P vlan acceptframe
			L3E	Yes	GUI L3E VLAN Port CLI L3E vlan acceptframe
			L3P	Yes	GUI L3P VLAN Port CLI L3P vlan acceptframe
Evaluate VLAN tags (ingress filtering)	Off	On	L2B	No	
			L2E	Yes	GUI L2E VLAN Port CLI L2E vlan ingressfilter
			L2P	Yes	GUI L2P VLAN Port CLI L2P vlan ingressfilter
			L3E	Yes	GUI L3E VLAN Port CLI L3E vlan ingressfilter
			L3P	Yes	GUI L3P VLAN Port CLI L3P vlan ingressfilter

Note: Protocols IGMP (from L2E) and GMRP (from L2P) work without VLAN tags. IGMP requests are flooded to all ports, regardless of their VLAN assignment.

Note: If port-based routing has been activated, ingress filtering is also activated.

Separate Spanning Tree instance for each VLAN

The network structure can be influenced by manipulated Spanning Tree frames. Additionally, it cannot be ruled out that specific Spanning Tree frames (BPDUs) can be transported across switch and VLAN boundaries and thus open the way for an advanced attack scenario.

Using a separate Spanning Tree instance for each VLAN provides better separation here.

Action	Default setting	Recommended setting	Available in SW version		Further information
Configuring MSTP	Off	On	L2B	No	
			L2E	No	
			L2P	Yes	GUI L2P MSTP (Multiple Spanning Tree) CLI L2P spanning-tree mst
			L3E	No	GUI L3E MSTP (Multiple Spanning Tree) CLI L3E spanning-tree mst
			L3P	Yes	GUI L3P MSTP (Multiple Spanning Tree) CLI L3P spanning-tree mst

Do not use port mirroring

The mirroring of the network traffic from one or more ports to a destination port (port mirroring) enables traffic from other network segments to be intercepted. This can put the confidentiality of this network segment at risk.

Action	Default setting	Recommended setting	Available in SW version		Further information
No port mirroring	Off	Off	L2B	Yes	GUI L2B Port Mirroring CLI L2B monitor session
			L2E	Yes	GUI L2E Port Mirroring CLI L2E monitor session
			L2P	Yes	GUI L2P Port Mirroring CLI L2P monitor session
			L3E	Yes	GUI L3E Port Mirroring CLI L3E monitor session
			L3P	Yes	GUI L3P Port Mirroring CLI L3P monitor session

Do not use DHCP Relay

The DHCP Relay function provides the option to assign a defined IP address to a switch on a specific switch port via DHCP Option 82. This function can be used to always assign the same IP address to a device on a specific switch port so that you can manage the device better. If you are not using this function, deactivate this option.

Action	Default setting	Recommended setting	Available in SW version		Further information
Do not configure any DHCP server IP addresses	0.0.0.0 (disabled) for all 4 possible server entries	0.0.0.0 (disabled) for all 4 possible server entries	L2B	Yes	GUI L2B DHCP Relay Agent CLI L2B dhcp-relay
			L2E	Yes	GUI L2E DHCP Relay Agent CLI L2E dhcp-relay
			L2P	Yes	GUI L2P DHCP Relay Agent CLI L2P dhcp-relay
			L3E	Yes	GUI L3E DHCP Relay Agent CLI L3E dhcp-relay
			L3P	Yes	GUI L3P DHCP Relay Agent CLI L3P dhcp-relay

Activate routing

If the switch is to function as a router, activate the routing.

Action	Default setting	Recommended setting	Available in SW Version		Further information
Activate routing globally	Off	On	L2B	No	
			L2E	No	
			L2P	No	
			L3E	Yes	GUI L3E Routing Global CLI L3E Routing Commands
			L3P	Yes	GUI L3P Routing Global CLI L3P Routing Commands

Action	Default setting	Recommended setting	Available in SW Version		Further information
Activate routing on the required ports	Off	On	L2B	No	
			L2E	No	
			L2P	No	
			L3E	Yes	GUI L3E Router Interfaces Configure CLI L3E routing
			L3P	Yes	GUI L3P Router Interfaces Configure CLI L3P routing

Deactivate routing

If you do not want the switch to perform any routing between Layer 3 subnetworks, deactivate the routing function completely.

Action	Default setting	Recommended setting	Available in SW version		Further information
Deactivate routing globally	Off	Off (default)	L2B	No	
			L2E	No	
			L2P	No	
			L3E	Yes	GUI L3E Routing Global CLI L3E Routing Commands
			L3P	Yes	GUI L3P Routing Global CLI L3P Routing Commands

Deactivate Proxy ARP

The Proxy ARP function allows end devices to communicate via the device working as a router without them having the required routing entries. However, this enables devices that are connected without authorization, for example, to communicate through the router with all subnetworks that the router knows. Therefore, deactivate Proxy ARP.

Action	Default setting	Recommended setting	Available in SW version		Further information
Deactivate Proxy ARP on every port	Off	Off (default)	L2B	No	
			L2E	No	
			L2P	No	
			L3E	Yes	GUI L3E Router Interfaces Configure CLI L3E ip proxy-arp
			L3P	Yes	GUI L3P Router Interfaces Configure CLI L3P ip proxy-arp

Deactivate net-directed broadcasts

Net-directed broadcasts enable broadcasts to be sent to other subnetworks via the router. This behavior can be used to attack the availability (Denial of Service, DoS). Therefore, deactivate this function. RFC 2644 “Changing the Default for Directed Broadcasts in Routers” defines that the default behavior of routers should be that directed broadcasts are not forwarded by default.

Note: All net-directed broadcasts (255.255.255.255) are discarded.

Action	Default setting	Recommended setting	Available in SW version		Further information
Deactivate net-directed broadcasts	Off	Off (default)	L2B	No	
			L2E	No	
			L2P	No	
			L3E	Yes	GUI L3E Router Interfaces Configure CLI L3E ip netdirbcast
			L3P	Yes	GUI L3P Router Interfaces Configure CLI L3P ip netdirbcast

Activate ARP selective learning

In the default setting, the router learns all the MAC addresses that it sees at its ports and keeps these addresses for 1,200 seconds (= 20 minutes) in its memory before deleting them again. Sending fake frames with invalid or non-existent MAC addresses can cause the table on the router to overflow and thus compromise the availability or integrity (“man in the middle” attack). Therefore, the router should only put MAC addresses that it explicitly requested into its table.

Note: If this option is activated, the 1st frame of a connection takes somewhat longer because of the ARP request that is then required.

Action	Default setting	Recommended setting	Available in SW version		Further information
Activate ARP selective learning	Off	On	L2B	No	
			L2E	No	
			L2P	No	
			L3E	Yes	Set GUI L3E ARP parameters CLI L3E arp selective-learning
			L3P	Yes	Set GUI L3P ARP parameters CLI L3P arp selective-learning

Known limitations:

When a device sets up a connection for the 1st time via the router, this can take slightly longer.

Deactivate router discovery

Router advertisement can be used for a range of attacks on the IT security. Here the problem is not the router itself, but the terminal devices that react to such advertisement frames and then send the frames to (fake) routers. These routers can then intercept or corrupt the traffic and forward it to the real router, or discard the traffic (Denial of Service).

Therefore, ICMP router advertisement (router and terminal devices) should generally be foregone.

Action	Default setting	Recommended setting	Available in SW version		Further information
Deactivate router discovery	Off	Off	L2B	No	
			L2E	No	
			L2P	No	
			L3E	Yes	GUI L3E configuration Router Discovery CLI L3E ip irdp
			L3P	Yes	GUI L3P configuration Router Discovery CLI L3P ip irdp

Use RIPv2 with authentication

When an application case requires the use of a dynamic routing protocol, use only RIP v2 with MD5 authentication. In this way you can prevent an attacker without authentication from manipulating the routing paths by means of fake RIP v1 frames or RIP v2 frames. The consequences of this can be interception, corruption or suppression of network traffic.

Known limitation:

Using RIPv2 can make some attacks via the routing protocol more difficult, but it also provides a further protection level.

Action	Default setting	Recommended setting	Available in SW version		Further information
Activate RIP	Off	On	L2B	No	
			L2E	No	
			L2P	No	
			L3E	Yes	GUI L3E RIP CLI L3E ip rip
			L3P	Yes	GUI L3P RIP CLI L3P ip rip

Action	Default setting	Recommended setting	Available in SW version		Further information
Set the RIP send version	ripVersion2	ripVersion2 (default)	L2B	No	
			L2E	No	
			L2P	No	
			L3E	Yes	GUI L3E RIP CLI L3E ip rip send version
			L3P	Yes	GUI L3P RIP CLI L3P ip rip send version
Set the authentication	noAuthentication	md5	L2B	No	
			L2E	No	
			L2P	No	
			L3E	Yes	GUI L3E RIP CLI L3E ip rip authentication
			L3P	Yes	GUI L3PE RIP CLI L3P ip rip authentication
Enter a key	<empty>	Secure password of 16 characters	L2B	No	
			L2E	No	
			L2P	No	
			L3E	Yes	GUI L3E RIP CLI L3E ip rip authentication
			L3P	Yes	GUI L3P RIP CLI L3P ip rip authentication
Define key ID	0	Shared ID with the other routers with which this router communicates	L2B	No	
			L2E	No	
			L2P	No	
			L3E	Yes	GUI L3E RIP CLI L3E ip rip authentication
			L3P	Yes	GUI L3P RIP CLI L3P ip rip authentication

Use only static routes

If the application does not require a dynamic routing protocol, use only static routes. To prevent possible attacks via routing protocols, deactivate all functions of these protocols.

Action	Default setting	Recommended setting	Available in SW version		Further information
Deactivate RIP	Off	Off (default)	L2B	No	
			L2E	No	
			L2P	No	
			L3E	Yes	GUI L3E RIP CLI L3E ip rip
			L3P	Yes	GUI L3P RIP CLI L3P ip rip

Use OSPF only with encrypted authentication

When OSPF is being used as the routing protocol, the routers should authenticate themselves to each other. This makes it more difficult for attackers to change routing information in the network via fake routing frames or routing frames that they have smuggled in.

Action	Default setting	Recommended setting	Available in SW version		Further information
Activate OSPF authentication	none	encrypt	L2B	No	
			L2E	No	
			L2P	No	
			L3E	No	
			L3P	Yes	CLI L3P ip ospf authentication

Use OSPF virtual links only with authentication

If virtual links are to be used for OSPF routing, these should be authenticated to make it more difficult to manipulate the routing information in the network.

Action	Default setting	Recommended setting	Available in SW version		Further information
Activate authentication for OSPF virtual links	Off	Off (default)	L2B	No	
			L2E	No	
			L2P	No	
			L3E	No	
			L3P	Yes	CLI L3P area virtual-link

Use IP Access Control Lists (ACLs)

When coupling different Layer 3 networks via a switch with Layer 3 software (L3E or L3P), configure Access Control Lists (ACLs) on the switch to prevent unauthorized access between the networks. This can be used to limit the traffic using IP addresses, IP protocols or port numbers.

In this way, basic security is possible without a special firewall.

Action	Default setting	Recommended setting	Available in SW version		Further information
Use IP ACLs	Off	Off (default)	L2B	No	
			L2E	No	
			L2P	No	
			L3E	Yes	CLI L3E QoS IP ACL
			L3P	Yes	CLI L3P Qos IP ACL

Activate Generic Multicast Registration Protocol (GMRP)

The GMRP protocol gives a client the option to enter itself in a multicast group on Layer 2. Only activate this protocol if you really require it.

Action	Default setting	Recommended setting	Available in SW version		Further information
Deactivate GMRP	Off	On	L2B	No	
			L2E	No	
			L2P	Yes	GUI Switching GMRP CLI set gmrp adminmode
			L3E	Yes	GUI Switching GMRP CLI set gmrp adminmode
			L3P	Yes	GUI Switching GMRP CLI set gmrp adminmode

Deactivate Generic Multicast Registration Protocol (GMRP)

The GMRP protocol gives a client the option to enter itself in a multicast group on Layer 2. Deactivate this protocol if you do not really require it.

Action	Default setting	Recommended setting	Available in SW version		Further information
Deactivate GMRP	Off	Off (default)	L2B	No	
			L2E	No	
			L2P	Yes	GUI Switching GMRP CLI no set gmrp adminmode
			L3E	Yes	GUI Switching GMRP CLI no set gmrp adminmode
			L3P	Yes	GUI Switching GMRP CLI no set gmrp adminmode

4.3 Administrative Access

4.3.1 Threats

Write access to a switch is required throughout the entire life cycle of the switch.

This results in the following threats:
☐ Identity theft
☐ Expanding the rights
☐ Manipulation of the configuration
☐ Configuration error

You can counteract threats with the following configuration items:

Adhere to the confidentiality and integrity of the administration access. Use secure connections for the administration. Depending on the software version, the switching platform provides the following options for increasing the security:
☐ SNMP v3
☐ SSH

The administration access via telnet and SNMP v1/v2 does not provide any protection in terms of confidentiality and integrity. The protocols named are classified as insecure because information is transferred in clear text and spying and manipulation cannot be prevented.

The switch also provides the option of configuration via the web interface. Here a Java application is loaded and the actual communication is via SNMP v3 – including the login. This application is supplied via HTTP. If an attacker has access to the network, he can fake the login page and access login data.

The following section “Security Quick Check for “Administration Access”” on page 56 is used to select only services that are required. This reduces the load and decreases the area of attack. Only use encrypted connections to transfer login data and configuration parameters.

4.3.2 Security Quick Check for “Administration Access”

This table helps you to identify which measures in your system environment should ideally be implemented on the switch in connection with administration access to the switch.

Do you require?	If necessary	If not necessary
GUI	Configuration of SNMP v3 Write Access	Deactivate HTTP and HTTPS
CLI Remote	Activate SSH	Deactivate SSH
	Deactivate Telnet	Deactivate Telnet
CLI Serial	Timeout for Serial CLI	Timeout for Serial CLI
Central management	Configuration of SNMP v3 Write Access	Deactivate SNMP v1/2
	Deactivate SNMP v1/2	See alsoLimit SNMP read access to specific IP addresses
Basic principle		
The measures follow the minimal principle in order to reduce the system load of the switch and its area of attack. Generally, you should deactivate services not required.		
General measures		
Regardless of the type of administration access, implement the following measures to increase the security: ☐ Limiting the Administration on IP Address Ranges ☐ Configuration of the Central User Management via RADIUS ☐ M3.14 Blocking a user		

Table 1: Security Quick Check for “Administration Access”

4.3.3 Measures

Configuration of SNMP v3 Write Access

Use SNMP v3 rather than versions 1 and 2, as versions 1 and 2 transfer passwords that are used for the authentication in clear text. The same applies to the exchange of data.

The encryption method used is DES (Data Encryption Standard). SHA1 (Secure Hash Algorithm) hashes are used for the integrity protection.

Note: DES is seen as a weak encryption method. Therefore, change the keys at regular, short intervals.

Action	Default setting	Recommended setting	Available in SW version		Further information
Create user	-	Use unique users	L2B	Yes	CLI L2B users name
			L2E	Yes	CLI L2E users name
			L2P	Yes	CLI L2P users name
			L3E	Yes	CLI L3E users name
			L3P	Yes	CLI L3P users name
Define write access for users	-	Readwrite	L2B	Yes	CLI L2B users access
			L2E	Yes	CLI L2E users access
			L2P	Yes	CLI L2P users access
			L3E	Yes	CLI L3E users access
			L3P	Yes	CLI L3P users access
Set password	-	Secure password of 16 characters	L2B	Yes	CLI L2B users passwd
			L2E	Yes	CLI L2E users passwd
			L2P	Yes	CLI L2P users passwd
			L3E	Yes	CLI L3E users passwd
			L3P	Yes	CLI L3P users passwd

Action	Default setting	Recommended setting	Available in SW version		Further information
Issue SNMP v3 access	-	Readwrite	L2B	Yes	CLI L2B users SNMP v3 accessmode
			L2E	Yes	CLI L2E users SNMP v3 accessmode
			L2P	Yes	CLI L2P users SNMP v3 accessmode
			L3E	Yes	CLI L3E users SNMP v3 accessmode
			L3P	Yes	CLI L3P users 3 accessmode
SNMP v3 authentication	-	SHA	L2B	Yes	CLI L2B users SNMP v3 authentication
			L2E	Yes	CLI L2E users SNMP v3 authentication
			L2P	Yes	CLI L2P users SNMP v3 authentication
			L3E	Yes	CLI L3E users SNMP v3 authentication
			L3P	Yes	CLI L3P users SNMP v3 authentication
SNMP v3 encryption	-	DES key with a length of 16 characters	L2B	No	
			L2E	No	
			L2P	Yes	CLI L2P users SNMP v3 encryption
			L3E	Yes	CLI L3E users SNMP v3 encryption
			L3P	Yes	CLI L3P users SNMP v3 encryption
Force SNMP v3 encryption	Off	On	L2B	No	
			L2E	No	
			L2P	Yes	CLI L2P users SNMP v3 encryption
			L3E	Yes	CLI L3E users SNMP v3 encryption
			L3P	Yes	CLI L3P users SNMP v3 encryption

Note: If no encryption can be activated, all the messages are transferred in clear text.

Activate SSH

SSH provides integrity and confidentiality. Telnet, in contrast, cannot guarantee this because both the login and the actual communication are transferred in clear text.

Action	Default setting	Recommended setting	Available in SW version		Further information
Transfer SSH key	-	Only use in trusted networks	L2B	No	
			L2E	No	
			L2P	Yes	Replace faulty devices
			L3E	Yes	
			L3P	Yes	Prepare basic L3P SSH access
Activate SSH server	On	On	L2B	No	
			L2E	No	
			L2P	Yes	GUI L2P description of SSH access CLI L2P network mgmt-access modify
			L3E	Yes	GUI L3E description of SSH access CLI L3E network mgmt-access modify
			L3P	Yes	GUI L3P description of SSH access CLI L3P network mgmt-access modify

Timeout for Serial CLI

Use a password to improve the access protection for CLI. If CLI is not being used, the user is automatically logged out. This protects against unauthorized access.

Action	Default setting	Recommended setting	Available in SW version		Further information
Set the timeout	5 (minutes)	5 (minutes)	L2B	Yes	CLI L2B serial timeout
			L2E	Yes	CLI L2E serial timeout
			L2P	Yes	CLI L2P serial timeout
			L3E	Yes	CLI L3E serial timeout
			L3P	Yes	CLI L3P serial timeout

Deactivate HTTP and HTTPS

Known limitations:

HTTP and HTTPS can only be deactivated together.

Action	Default setting	Recommended setting	Available in SW version		Further information
Deactivate http and HTTPS servers	On	If no web access is required, deactivate HTTP and HTTPS	L2B	Yes	GUI L2B web access CLI L2B ip http server
			L2E	Yes	GUI L2E Telnet/web access CLI L2E ip http server
			L2P	Yes	GUI L2P Telnet/web/SSH access CLI L2P ip http server
			L3E	Yes	GUI L3E Telnet/web/SSH access CLI L3E ip http server
			L3P	Yes	GUI L3P Telnet/web/SSH access CLI L3P ip http server

Deactivate SNMP v1/2

With SNMP v1/v2, the community is used as the password and is transferred unencrypted. If you do not require any external access, deactivate SNMP v1/2 or at least limit SNMP v1/2 to read access.

Action	Default setting	Recommended setting	Available		Further information
Deactivate SNMP v1/2 server	On	Off	L2B	No	
			L2E	Yes	GUI L2E SNMP v1/v2 access settings CLI L2E snmp-access version
			L2P	Yes	GUI L2P SNMP v1/v2 access settings CLI L2P snmp-access version
			L3E	Yes	GUI L3E SNMP v1/v2 access settings CLI L3E snmp-access version
			L3P	Yes	GUI L3P SNMP v1/v2 access settings CLI L3P snmp-access version

Deactivate Telnet

Telnet transfers the data unencrypted via the network and therefore should not be used.

Known limitation:

If the Telnet service has been deactivated, the Command Line Interface (CLI) does not work in the web interface any more.

Action	Default setting	Recommended setting	Available		Further information
Deactivate Telnet server	On	Off	L2B	No	
			L2E	Yes	GUI L2E Telnet/web access CLI L2E telnet
			L2P	Yes	GUI L2P Telnet/web/SSH access CLI L2P telnet
			L3E	Yes	GUI L3E Telnet/web/SSH access CLI L3E telnet
			L3P	Yes	GUI L3P Telnet/web/SSH access CLI L3P telnet

Note: If a user calls up the Telnet service via the web interface with HTTP or HTTPS, the access data is still transferred as clear text.

Deactivate SSH

Action	Default setting	Recommended setting	Available		Further information
Activate Deactivate server	Off	Deactivate if no remote access to the console is required	L2B	No	
			L2E	No	
			L2P	Yes	GUI L2P Telnet/web/SSH access CLI L2P network mgmt-access modify
			L3E	Yes	GUI L3E Telnet/web/SSH access CLI L3E network mgmt-access modify
			L3P	Yes	GUI L3P Telnet/web/SSH access CLI L3P network mgmt-access modify

Create a Read Access

For the following reasons, you should generally avoid using the standard user “user”:

- ☐ The user name is publicly known and therefore makes it significantly easier to attack by guessing the password.
- ☐ Actions on the switch cannot be assigned to any user (traceability of configuration changes)

Therefore, create a separate account for every employee.

Action	Default setting	Recommended setting	Available		Further information
Create user	-	Use unique users	L2B	No	
			L2E	No	GUI L2E password / SNMP v3 access CLI L2E users name
			L2P	Yes	GUI L2P password / SNMP v3 access CLI L2P users name
			L3E	Yes	GUI L3E password / SNMP v3 access CLI L3E users name
			L3P	Yes	GUI L3P password / SNMP v3 access CLI L3P users name
Define write access for users	-	Readonly	L2B	No	
			L2E	No	GUI L2E password / SNMP v3 access CLI L2E users access
			L2P	Yes	GUI L2P password / SNMP v3 access CLI L2P users access
			L3E	Yes	GUI L3E password / SNMP v3 access CLI L3E users access
			L3P	Yes	GUI L3P password / SNMP v3 access CLI L3P users access

Action	Default setting	Recommended setting	Available		Further information
Set password	-	Secure password of 16 characters	L2B	No	
			L2E	Yes	GUI L2E password / SNMP v3 access CLI L2E users passwd
			L2P	Yes	GUI L2P password / SNMP v3 access CLI L2P users passwd
			L3E	Yes	GUI L3E password / SNMP v3 access CLI L3E users passwd
			L3P	Yes	GUI L3P password / SNMP v3 access CLI L3P users passwd

Create a Write Access

Action	Default setting	Recommended setting	Available		Further information
Create user	-	Use unique users	L2B	Yes	GUI L2B password / SNMP v3 access CLI L2B users name
			L2E	Yes	GUI L2E password / SNMP v3 access CLI L2E users name
			L2P	Yes	GUI L2P password / SNMP v3 access CLI L2P users name
			L3E	Yes	GUI L3E password / SNMP v3 access CLI L3E users name
			L3P	Yes	GUI L3P password / SNMP v3 access CLI L3P users name

Action	Default setting	Recommended setting	Available		Further information
Define write access for users	-	readwrite	L2B	Yes	GUI L2B password / SNMP v3 access CLI L2B users access
			L2E	Yes	GUI L2E password / SNMP v3 access CLI L2E users access
			L2P	Yes	GUI L2P password / SNMP v3 access CLI L2P users access
			L3E	Yes	GUI L3E password / SNMP v3 access CLI L3E users access
			L3P	Yes	GUI L3P password / SNMP v3 access CLI L3P users access
Set password	-	Secure password of 16 characters	L2B	Yes	GUI L2B password / SNMP v3 accessCLI L2B users passwd
			L2E	Yes	GUI L2E password / SNMP v3 access CLI L2E users passwd
			L2P	Yes	GUI L2P password / SNMP v3 access CLI L2P users passwd
			L3E	Yes	GUI L3E password / SNMP v3 access CLI L3E users passwd
			L3P	Yes	GUI L3P password / SNMP v3 access CLI L3P users passwd

Limiting the Administration on IP Address Ranges

Limit the administration of the switch not only with regard to the services, but also the networks from which access is possible.

Action	Default setting	Recommended setting	Available		Further information
restricted management access Activate (RMA)	-	On	L2B	No	
			L2E	Yes	L2E limited management access CLI L2E network mgmt-access operation
			L2P	Yes	L2P limited management access CLI L2P network mgmt-access operation
			L3E	Yes	L3E limited management access CLI L3E network mgmt-access operation
			L3P	Yes	L3P limited management access CLI L3P network mgmt-access operation
Add RMA	-	Up to 16 RMAs can be created	L2B	No	
			L2E	Yes	L2E limited management access CLI L2E network mgmt-access add
			L2P	Yes	L2P limited management access CLI L2P network mgmt-access add
			L3E	Yes	L3E limited management access CLI L3E network mgmt-access add
			L3P	Yes	L3P limited management access CLI L3P network mgmt-access add

Action	Default setting	Recommended setting	Available		Further information
Configure (RMA)	-	If the Security Quick Check does not require the use of a protocol, deactivate it globally. If the application requires a protocol, activate it for the management network	L2B	No	
			L2E	Yes	L2E limited management access CLI L2E network mgmt-access modify
			L2P	Yes	L2P limited management access CLI L2P network mgmt-access modify
			L3E	Yes	L3E limited management access CLI L3E network mgmt-access modify
			L3P	Yes	L3P limited management access CLI L3P network mgmt-access modify

Configuration of the Central User Management via RADIUS

In bigger networks, the local management of users and their passwords on the switch reaches its limitations when you want to change passwords, create new users or delete users.

Therefore, central user management on RADIUS servers is recommended.

Known limitations:

If the RADIUS servers can no longer be reached, it is not possible to login to the switch with a “RADIUS” user. This scenario is to be considered here. It is always recommended to create an emergency access user on the switch, keep its password safe, and access the switch with this user in an emergency. Afterwards, this password must be changed.

Action	Default setting	Recommended setting	Available		Further information
Configure RADIUS server	radius server host {auth | acct} <ipaddr> [<port>]	“auth” configures an authentication server	L2B	No	
			L2E	No	
			L2P	Yes	GUI L2P RADIUS server settings for IEEE 802.1X CLI L2P radius server host
			L3E	Yes	GUI L3E RADIUS server settings for IEEE 802.1X CLI L3E radius server host
			L3P	Yes	GUI L3P RADIUS server settings for IEEE 802.1X CLI L3P radius server host
Configure shared secret	-	Assign a shared secret of 20 characters	L2B	No	
			L2E	No	
			L2P	Yes	GUI L2P RADIUS server settings for IEEE 802.1X CLI L2P radius server key
			L3E	Yes	GUI L3E RADIUS server settings for IEEE 802.1X CLI L3E radius server key
			L3P	Yes	GUI L3P RADIUS server settings for IEEE 802.1X CLI L3P radius server key

Action	Default setting	Recommended setting	Available		Further information
Create authentication list for RADIUS	authentication login <listname> [method1 [method2 [method3]]]	Method must be “radius”	L2B	No	
			L2E	No	
			L2P	Yes	GUI L2P IEEE 802.1X-Port-Authentication CLI L2P authentication login
			L3E	Yes	GUI L3E IEEE 802.1X Port Authentication CLI L3E authentication login
			L3P	Yes	GUI L3P IEEE 802.1X Port Authentication CLI L3P authentication login
Create users and assign RADIUS authentication	None	users login <user> <listname>	L2B	No	
			L2E	No	
			L2P	Yes	CLI L2P users login
			L3E	Yes	CLI L3E users login
			L3P	Yes	CLI L3P users login

4.4 Monitoring

4.4.1 Threats

Monitoring is necessary for the traceability of actions carried out and for ensuring that the state of the switch is error-free. If more than one switch is being used, central monitoring is recommended. Document configuration changes in a traceable way using suitable logging. This results in the following threats:

- ☐ Loss of availability, confidentiality and integrity due to
- ☐ Configuration error
- ☐ Manipulation of the configuration
- ☐ Hardware and software errors

The information that a switch sends to the central monitoring software can be specifically suppressed, changed or intercepted, depending on the configuration. This can infringe on confidentiality and integrity.

4.4.2 Security Quick Check for “Monitoring”

Control question	If necessary	If not necessary
Is the availability of the network important?	Activate SNMP v1/v2 read access	Deactivate SNMP v1/v2
	Activate SNMP v3 read access	Deactivate SNMP v1/v2
	Assign secure SNMP passwords (communities)	
	Limit SNMP read access to specific IP addresses	Send SNMP traps
	Send SNMP traps	
	Assign secure SNMP passwords (communities)	
	Configure alarm for specific errors	
	Activate port monitor	
Are there (legal) specifications for logging changes to the configuration?	Central logging of SNMP write accesses via syslog Activate PTP time synchronization Do not accept SNTP broadcasts	Deactivate central logging of SNMP write accesses via syslog (Default setting)
Should it be possible to clear up a security incident?	M4.8 or 4.12 (time synchronization) Central logging via syslog	This is not an option for security-relevant applications if no syslog server is available Deactivate syslog
Is an SNTP time source available in the network?	Activate and configure SNTP client Deactivate SNTP client Deactivate PTP time synchronization	Deactivate PTP time synchronization
Is a PTP time source available in the network?	Deactivate SNTP client Deactivate SNTP server Activate PTP time synchronization	Activate and configure SNTP client Deactivate SNTP server Do not accept SNTP broadcasts
Is device monitoring with a signal contact planned?	Monitor the device status via the signal contact	
Is there an environment with which the device status can be monitored via PROFINET?	Activate PROFINET	Deactivate PROFINET (see also Deactivate PROFINET)
Is VRRP or HiVRRP being used?	Send SNMP traps when using VRRP/HiVRRP	
Basic principles		

Table 2: Security Quick Check for “Monitoring”

Control question	If necessary	If not necessary
Central monitoring Traceability of changes to the configuration Shared time on all systems Central logging		
General measures to be implemented		
☐ Configuration of switch name ☐ Configuration of system prompt ☐ Configuration of switch location and contact person		

Table 2: Security Quick Check for "Monitoring" (cont.)

Known limitations:

- ☐ At present, the log data can only be transferred unencrypted and via UDP protocol (possible frame loss and risk of fake log data).
- ☐ Syslog uses port 514 as the source port. This makes the Stateful Inspection of the traffic on a firewall more difficult.
- ☐ SNMP v3 (encrypted) is currently only available in the Professional software variant.

4.4.3 Measures

You can counteract the threats with the following configuration items:

Activate SNMP v1/v2 read access

In addition to using Ping to test device reachability, activation of SNMP v1/v2 read access gives network management software without SNMP v3 the option to read system-internal values, such as the temperature or the status of the power supply units, along with the availability of the switch.

Action	Default setting	Recommended setting	Available in SW version		Further information
Activate SNMP v1/v2 read access	SNMP v1 on SNMP v2 on	SNMP v1 on SNMP v2 on	L2B	Yes	GUI L2B SNMP v1/v2 access settings CLI L2B snmp-access version
			L2E	Yes	GUI L2E SNMP v1/v2 access settings CLI L2E snmp-access version
			L2P	Yes	GUI L2P SNMP v1/v2 access settings CLI L2P snmp-access version
			L3E	Yes	GUI L3E SNMP v1/v2 access settings CLI L3E snmp-access version
			L3P	Yes	GUI L3P SNMP v1/v2 access settings CLI L3P snmp-access version

Activate SNMP v3 read access

In addition to using Ping to test device reachability, activation of SNMP v3 read access gives network management software the option to read system-internal values, such as the temperature or the status of the power supply units, along with the availability of the switch. In contrast to versions 1 and 2, SNMP v3 is encrypted and therefore preferable.

Action	Default setting	Recommended setting	Available in SW version		Further information
Activate SNMP v3 read access	On	On	L2B	Yes	GUI L2B password / SNMP v3 access CLI L2B users SNMP v3 accessmode
			L2E	Yes	GUI L2E password / SNMP v3 access CLI L2E users SNMP v3 accessmode
			L2P	Yes	GUI L2P password / SNMP v3 access CLI L2P users SNMP v3 accessmode
			L3E	Yes	GUI L3E password / SNMP v3 access CLI L3E users SNMP v3 accessmode
			L3P	Yes	GUI L3P password / SNMP v3 access CLI L3P users SNMP v3 accessmode

Assign secure SNMP passwords (communities)

When reading out and writing values with SNMP v1 and v2, what is known as a community string (a kind of password) is used as authentication. The default values are generally known standard values and therefore cannot be seen as secure in any way. Change these values.

Action	Default setting	Recommended setting	Available in SW version		Further information
Assign secure SNMP passwords	“public” and “private”	Community string with a length of 16 characters	L2B	Yes	GUI L2B SNMP v1/v2 access settings CLI L2B snmp-server community
			L2E	Yes	GUI L2E SNMP v1/v2 access settings CLI L2E snmp-server community
			L2P	Yes	GUI L2P SNMP v1/v2 access settings CLI L2P snmp-server community
			L3E	Yes	GUI L3E SNMP v1/v2 access settings CLI L3E snmp-server community
			L3P	Yes	GUI L3P SNMP v1/v2 access settings CLI L3P snmp-server community

Limit SNMP read access to specific IP addresses

Access with SNMP allows, in addition to regulation with the community string, the regulation of the access to an IP address or to IP address ranges.

Action	Default setting	Recommended setting	Available in SW version		Further information
Limit SNMP access to specific IP addresses	0.0.0.0/0.0.0.0 (access allowed from any address)	Address of the network management	L2B	Yes	GUI L2B SNMP v1/v2 access settings CLI L2B snmp-server community ipaddr
			L2E	Yes	GUI L2E SNMP v1/v2 access settings CLI L2E snmp-server community ipaddr
			L2P	Yes	GUI L2P SNMP v1/v2 access settings CLI L2P snmp-server community ipaddr
			L3E	Yes	GUI L3E SNMP v1/v2 access settings CLI L3E snmp-server community ipaddr
			L3P	Yes	GUI L3P SNMP v1/v2 access settings CLI L3P snmp-server community ipaddr

Deactivate SNMP v1/v2

SNMP v1 and v2 do not allow encrypted data transfer. Additionally, values can be read via the switch and the connected devices that can be used to prepare or carry out attacks.

Action	Default setting	Recommended setting	Available in SW version		Further information
Deactivate SNMP v1/v2	v1 and v2 active	v1 and v2 off	L2B	Yes	GUI L2B SNMP v1/v2 access settings CLI L2B snmp-access version
			L2E	Yes	GUI L2E SNMP v1/v2 access settings CLI L2E snmp-access version
			L2P	Yes	GUI L2P SNMP v1/v2 access settings CLI L2P snmp-access version
			L3E	Yes	GUI L3E SNMP v1/v2 access settings CLI L3E snmp-access version
			L3P	Yes	GUI L3P SNMP v1/v2 access settings CLI L3P snmp-access version

Send SNMP traps

Along with reading out status information via SNMP read access, the switches provide the option to send messages about error statuses via SNMP traps (notification) to a network management system. Activate this function.

Action	Default setting	Recommended setting	Available in SW version		Further information
Send SNMP traps	No trap destination configured	Activate all existing trap triggers (e.g. authentication, link up/down)	L2B	Yes	GUI L2B alarms (traps) CLI L2B snmp-server enable traps
			L2E	Yes	GUI L2E alarms (traps) CLI L2E snmp-server enable traps
			L2P	Yes	GUI L2P alarms (traps) CLI L2P snmp-server enable traps
			L3E	Yes	GUI L3E alarms (traps) CLI L3E snmp-server enable traps
			L3P	Yes	GUI L3P alarms (traps) CLI L3P snmp-server enable traps

Deactivate sending of SNMP traps

Along with reading out status information via SNMP read access, the switches provide the option to send messages about error statuses via SNMP traps (notification) to a network management system. If no network management system (for example, Industrial HiVision) is being used, deactivate this function to avoid making unnecessary information available in the network.

Action	Default setting	Recommended setting	Available in SW version		Further information
Send SNMP traps	No trap destination configured	Deactivate all existing trap triggers (e.g. authentication, link up/down)	L2B	Yes	GUI L2B alarms (traps) CLI L2B snmp-server enable traps
			L2E	Yes	GUI L2E alarms (traps) CLI L2E snmp-server enable traps
			L2P	Yes	GUI L2P alarms (traps) CLI L2P snmp-server enable traps
			L3E	Yes	GUI L3E alarms (traps) CLI L3E snmp-server enable traps
			L3P	Yes	GUI L3P alarms (traps) CLI L3P snmp-server enable traps

Activate and configure SNTP client

For all SNMP traps and log entries, the time of the message plays a major role. In particular when clearing up a security incident, it helps to have the precise, identical time on all devices. Therefore synchronize the clock of the switch permanently with a central time source. If a 2nd time server is available, then also configure this.

Action	Default setting	Recommended setting	Available in SW version		Further information
Configuration of SNTP client	Off	On, at least one SNTP server configured and tested	L2B	Yes	GUI L2B SNTP configuration CLI L2B sntp client
			L2E	Yes	GUI L2E SNTP configuration CLI L2E sntp client
			L2P	Yes	GUI L2P SNTP configuration CLI L2P sntp client
			L3E	Yes	GUI L3E SNTP configuration CLI L3E sntp client
			L3P	Yes	GUI L3P SNTP configuration CLI L3P sntp client

Deactivate SNTP client

If there is no time source in the network, deactivate the SNTP service. Also deactivate the SNTP client when using PTP.

Action	Default setting	Recommended setting	Available in SW version		Further information
Deactivate SNTP client	Off	Off (see text description above)	L2B	Yes	GUI L2B SNTP configuration CLI L2B sntp operation
			L2E	Yes	GUI L2E SNTP configuration CLI L2E sntp operation
			L2P	Yes	GUI L2P SNTP configuration CLI L2P sntp operation
			L3E	Yes	GUI L3E SNTP configuration CLI L3E sntp operation
			L3P	Yes	GUI L3P SNTP configuration CLI L3P sntp operation

Deactivate SNTP server

Every service running unnecessarily on the switch provides an area of attack. Therefore, also deactivate the SNTP server service when you are not operating the switch as an SNTP server.

Action	Default setting	Recommended setting	Available in SW version		Further information
Configuration of SNTP server	On (if SNTP has been activated)	Off	L2B	Yes	GUI L2B SNTP configuration CLI L2B sntp operation
			L2E	Yes	GUI L2E SNTP configuration CLI L2E sntp operation
			L2P	Yes	GUI L2P SNTP configuration CLI L2P sntp operation
			L3E	Yes	GUI L3E SNTP configuration CLI L3E sntp operation
			L3P	Yes	GUI L3P SNTP configuration CLI L3P sntp operation

Do not accept SNTP broadcasts

SNTP broadcasts can be sent from random devices within the same subnetwork. This enables the manipulation of the local time in the switch. Additionally, when the receipt of SNTP broadcasts with another service in the network is activated, the switch can be addressed. Therefore, deactivate the receipt of SNTP broadcasts.

Action	Default setting	Recommended setting	Available in SW version		Further information
Do not accept SNTP broadcasts	Accept	Do not accept	L2B	Yes	GUI L2B SNTP configuration CLI L2B sntp client accept-broadcast
			L2E	Yes	GUI L2E SNTP configuration CLI L2E sntp client accept-broadcast
			L2P	Yes	GUI L2P SNTP configuration CLI L2P sntp client accept-broadcast
			L3E	Yes	GUI L3E SNTP configuration CLI L3E sntp client accept-broadcast
			L3P	Yes	GUI L3P SNTP configuration CLI L3P sntp client accept-broadcast

Activate PTP time synchronization

For SNMP traps and log entries, the time of the message plays a major role. In particular when clearing up a security incident, it helps to have the precise, identical time on all devices. Therefore synchronize the clock of the switch permanently with a central time source. As an alternative to SNTP, PTP is a more precise variant. Use the newer version 2 of PTP.

Action	Default setting	Recommended setting	Available in SW version		Further information
Activate PTP	Off	On	L2B	Yes	GUI L2B PTP (IEEE 1588) CLI L2B lldp tlv ptp
			L2E	Yes	GUI L2E PTP (IEEE 1588) CLI L2E lldp tlv ptp
			L2P	Yes	GUI L2P PTP (IEEE 1588) CLI L2P lldp tlv ptp
			L3E	Yes	GUI L3E PTP (IEEE 1588) CLI L3E lldp tlv ptp
			L3P	Yes	GUI L3P PTP (IEEE 1588) CLI L3P lldp tlv ptp

Deactivate PTP time synchronization

If no time is available in the network via PTP, or the time is synchronized with SNTP on the switch, deactivate PTP.

Action	Default setting	Recommended setting	Available in SW version		Further information
Deactivate PTP	Off	Off (see text above)	L2B	Yes	GUI L2B PTP (IEEE 1588) CLI L2B lldp tlv ptp
			L2E	Yes	GUI L2E PTP (IEEE 1588) CLI L2E lldp tlv ptp
			L2P	Yes	GUI L2P PTP (IEEE 1588) CLI L2P lldp tlv ptp
			L3E	Yes	GUI L3E PTP (IEEE 1588) CLI L3E lldp tlv ptp
			L3P	Yes	GUI L3P PTP (IEEE 1588) CLI L3P lldp tlv ptp

Known limitations:

☐ At present there is no option for authenticating the communication partners using the time synchronization (as it would be possible, for example, with NTPv3 using MD5 check sums).

Central logging via syslog

The central storage of log messages enables faster clarification of security incidents and faster troubleshooting for malfunctions. Additionally, storing the log data on a different system makes it more difficult to manipulate the log data.

Action	Default setting	Recommended setting	Available in SW version		Further information
Activate sending of log entries via syslog	Off	On	L2B	No	
			L2E	Yes	GUI L2E Syslog CLI L2E logging host
			L2P	Yes	GUI L2P Syslog CLI L2P logging host
			L3E	Yes	GUI L3E Syslog CLI L3E logging host
			L3P	Yes	GUI L3P Syslog CLI L3P logging host

Action	Default setting	Recommended setting	Available in SW version		Further information
Set up and activate the sending of log entries via syslog to at least one server	No server defined	At least one syslog server that is configured as “active”	L2B	No	
			L2E	Yes	GUI L2E Syslog CLI L2E logging host
			L2P	Yes	GUI L2P Syslog CLI L2P logging host
			L3E	Yes	GUI L3E Syslog CLI L3E logging host
			L3P	Yes	GUI L3P Syslog CLI L3P logging host
Sending of log entries via syslog with “informational” and higher	Debug	Informational	L2B	No	
			L2E	Yes	GUI L2E Syslog CLI L2E logging host
			L2P	Yes	GUI L2P Syslog CLI L2P logging host
			L3E	Yes	GUI L3E Syslog CLI L3E logging host
			L3P	Yes	GUI L3P Syslog CLI L3P logging host

Deactivate syslog

If no syslog server is available, deactivate the sending of log entries via syslog.

Action	Default setting	Recommended setting	Available in SW version		Further information
Syslog	Off	Off	L2B	No	
			L2E	Yes	GUI L2E Syslog CLI L2E logging host remove
			L2P	Yes	GUI L2P Syslog CLI L2P logging host remove
			L3E	Yes	GUI L3E Syslog CLI L3E logging snmp-requests set operation
			L3P	Yes	GUI L3P Syslog CLI L3P logging snmp-requests set operation

Central logging of SNMP write accesses via syslog

To be able to trace changes or manipulations of the configuration of the switch, log the SNMP write accesses and send the log entries to the central syslog server.

Action	Default setting	Recommended setting	Available in SW version		Further information
Log SNMP write requests	Off	On, severity “informational”	L2B	No	
			L2E	Yes	GUI L2E Syslog CLI L2E logging snmp-requests set operation
			L2P	Yes	GUI L2P Syslog CLI L2P logging snmp-requests set operation
			L3E	Yes	GUI L3E Syslog CLI L3E logging snmp-requests set operation
			L3P	Yes	GUI L3P Syslog CLI L3P logging snmp-requests set operation

Deactivate central logging of SNMP write accesses via syslog

If no syslog server is available, deactivate the logging of SNMP write accesses via syslog.

Action	Default setting	Recommended setting	Available in SW version		Further information
Log SNMP write requests	Off	Off	L2B	No	
			L2E	Yes	GUI L2E Syslog CLI L2E logging snmp-requests set operation
			L2P	Yes	GUI L2P Syslog CLI L2P logging snmp-requests set operation
			L3E	Yes	GUI L3E Syslog CLI L3E logging snmp-requests set operation
			L3P	Yes	GUI L3P Syslog CLI L3P logging snmp-requests set operation

Configuration of switch name

During an installation with more than one switch, to be able to distinguish the switches from each other easily, give the switch a name. This also makes it easier to identify the switch in a network management system, which can read out this value via SNMP.

Action	Default setting	Recommended setting	Available in SW version		Further information
Configure switch name	<Product>-<part of the MAC address>	<Name>	L2B	Yes	GUI L2B System CLI L2B snmp-server sysname
			L2E	Yes	GUI L2E System CLI L2E snmp-server sysname
			L2P	Yes	GUI L2P System CLI L2P snmp-server sysname
			L3E	Yes	GUI L3E System CLI L3E snmp-server sysname
			L3P	Yes	GUI L3P System CLI L3P snmp-server sysname

Configuration of system prompt

During an installation with more than one switch, to be able to distinguish the switches from each other easily, assign a system prompt that the CLI displays. This helps avoid incorrect configurations.

Action	Default setting	Recommended setting	Available in SW version		Further information
Configure system prompt	(Hirschmann Railswitch)	<Name>	L2B	Yes	CLI L2B set prompt
			L2E	Yes	CLI L2E set prompt
			L2P	Yes	CLI L2P set prompt
			L3E	Yes	CLI L3E set prompt
			L3P	Yes	CLI L3P set prompt

Configuration of switch location and contact person

During an installation with more than one switch, to be able to determine the location and the responsible contact person faster, store these in the switch. This makes it easier to identify the switch in a network management system, which can read these values via SNMP.

Action	Default setting	Recommended setting	Available in SW version		Further information
Configure location	Hirschmann Railswitch	<Location name>	L2B	Yes	GUI L2B System CLI L2B snmp-server location
			L2E	Yes	GUI L2E System CLI L2E snmp-server location
			L2P	Yes	GUI L2P System CLI L2P snmp-server location
			L3E	Yes	GUI L3E System CLI L3E snmp-server location
			L3P	Yes	GUI L3P System CLI L3P snmp-server location
Configure contact person	Hirschmann Automation and Control GmbH	<Contact person>	L2B	Yes	GUI L2B System CLI L2B snmp-server contact
			L2E	Yes	GUI L2E System CLI L2E snmp-server contact
			L2P	Yes	GUI L2P System CLI L2P snmp-server contact
			L3E	Yes	GUI L3E System CLI L3E snmp-server contact
			L3P	Yes	GUI L3P System CLI L3P snmp-server contact

Configure alarm for high network load

If you want to be notified when the network load exceeds a specific threshold value, activate this alarm for each port. The upper threshold value depends on the installation environment of the switch. Therefore, determine the upper threshold value on site.

Action	Default setting	Recommended setting	Available in SW version		Further information
Alarm for high network load (upper threshold value)	0.00%	<Depending on network environment>, activate alarm	L2B	Yes	GUI L2B load (network load)
			L2E	Yes	GUI L2E load (network load)
			L2P	Yes	GUI L2P load (network load)
			L3E	Yes	GUI L3E load (network load)
			L3P	Yes	GUI L3P load (network load)

Configure alarm for specific errors

The switch enables specific error statuses to be reported via SNMP trap. Use this option so that you can detect error statuses quickly.

Action	Default setting	Recommended setting	Available in SW version		Further information
Generate trap when status changes	Off	On	L2B	Yes	GUI L2B trap setting CLI L2B snmp trap link-status
			L2E	Yes	GUI L2E trap setting CLI L2E snmp trap link-status
			L2P	Yes	GUI L2P trap setting CLI L2P snmp trap link-status
			L3E	Yes	GUI L3E trap setting CLI L3E snmp trap link-status
			L3P	Yes	GUI L3P trap setting CLI L3P snmp trap link-status

Action	Default setting	Recommended setting	Available in SW version		Further information
Monitoring	Monitor power supply unit 1 Monitor power supply unit 2 Ignore temperature Ignore module removal Ignore ACA removal Ignore asynchronous ACA Ignore connection error Ignore ring redundancy	Monitor power supply unit 1 Monitor power supply unit 2 (if connected) Monitor temperature Remove ACA (depending on application case) ACA asynchronous (depending on application case, not L2B) Monitor connection error Monitor ring redundancy (if used, not L2B) Monitor ring/network coupling (if used, not L2B)	L2B	Yes	GUI L2B device status CLI L2B device-status monitor
			L2E	Yes	GUI L2E device status CLI L2E device-status monitor
			L2P	Yes	GUI L2P device status CLI L2P device-status monitor
			L3E	Yes	GUI L3E device status CLI L3E device-status monitor
			L3P	Yes	GUI L3P device status CLI L3P device-status monitor

Monitor the device status via the signal contact

The switch enables specific error statuses to be reported via the signal contact. Use this option so that you can detect error statuses quickly.

Action	Default setting	Recommended setting	Available in SW version		Further information
Signal Contact Mode	Signal contact 1: device status Signal contact 2: manual setting (contact closed)	Function Monitoring	L2B	Yes	GUI L2B signal contact CLI L2B signal contact
			L2E	Yes	GUI L2E signal contact CLI L2E signal contact
			L2P	Yes	GUI L2P signal contact CLI L2P signal contact
			L3E	Yes	GUI L3E signal contact CLI L3E signal contact
			L3P	Yes	GUI L3P signal contact CLI L3P signal contact

Action	Default setting	Recommended setting	Available in SW version		Further information
Generate trap when status changes	Off	Off (already not configured in M4.21)	L2B	Yes	GUI L2B trap setting CLI L2B snmp trap link-status
			L2E	Yes	GUI L2E trap setting CLI L2E snmp trap link-status
			L2P	Yes	GUI L2P trap setting CLI L2P snmp trap link-status
			L3E	Yes	GUI L3E trap setting CLI L3E snmp trap link-status
			L3P	Yes	GUI L3P trap setting CLI L3P snmp trap link-status
Monitoring	Monitor power supply unit 1 Monitor power supply unit 2 Ignore temperature Ignore module removal Ignore ACA removal Ignore asynchronous ACA Ignore connection error Ignore ring redundancy	Monitor power supply unit 1 Monitor power supply unit 2 (if connected) Monitor temperature (not L2B) Remove ACA (depending on application case) ACA asynchronous (depending on application case, not L2B) Monitor connection error Monitor ring redundancy (if used, not L2B) Monitor ring/network coupling (if used, not L2B)	L2B	Yes	GUI L2B device status CLI L2B device-status monitor
			L2E	Yes	GUI L2E device status CLI L2E device-status monitor
			L2P	Yes	GUI L2P device status CLI L2P device-status monitor
			L3E	Yes	GUI L3E device status CLI L3E device-status monitor
			L3P	Yes	GUI L3P device status CLI L3P device-status monitor

Activate PROFINET

If it is possible to monitor PROFINET components in the network environment, activate PROFINET on the switch and import the GSDML file into the configuration environment of the PROFINET environment.

Action	Default setting	Recommended setting	Available in SW version		Further information
Activate PROFINET	Off	On	L2B	No	
			L2E	Yes	GUI L2E PROFINET IO CLI L2E PROFINET IO
			L2P	Yes	GUI L2P PROFINET IO CLI L2P PROFINET IO
			L3E	Yes	GUI L3E PROFINET IO CLI L3E PROFINET IO
			L3P	Yes	GUI L3P PROFINET IO CLI L3P PROFINET IO

Deactivate PROFINET

If it is not possible to monitor the switch via PROFINET, deactivate the PROFINET protocol on the switch (default setting).

Action	Default setting	Recommended setting	Available in SW version		Further information
Deactivate PROFINET	Off	Off	L2B	No	
			L2E	Yes	GUI L2E PROFINET IO CLI L2E PROFINET IO
			L2P	Yes	GUI L2P PROFINET IO CLI L2P PROFINET IO
			L3E	Yes	GUI L3E PROFINET IO CLI L3E PROFINET IO
			L3P	Yes	GUI L3P PROFINET IO CLI L3P PROFINET IO

Activate port monitor

The port monitor functions can detect link changes and CRC errors and report them. You can use this to detect when devices are plugged in and out. You can also detect faulty connections (e.g. defective cables) in this way.

Action	Default setting	Recommended setting	Available in SW version		Further information
Activate port monitor globally	Off	On	L2B	No	
			L2E	No	
			L2P	Yes	GUI L2P Port Monitor CLI L2P port-monitor (Global Config)
			L3E	Yes	GUI L3E Port Monitor CLI L3E port-monitor (Global Config)
			L3P	Yes	GUI L3P Port Monitor CLI L3P port-monitor (Global Config)
Activate port monitor for each port	Off	On	L2B	No	
			L2E	No	
			L2P	Yes	GUI L2P Port Monitor CLI L2P port-monitor (Global Config)
			L3E	Yes	GUI L3E Port Monitor CLI L3E port-monitor (Global Config)
			L3P	Yes	GUI L3P Port Monitor CLI L3P port-monitor (Global Config)
Activate detection of link change for each port	Off	On	L2B	No	
			L2E	No	
			L2P	Yes	GUI L2P Port Monitor CLI L2P port-monitor condition link-flap (Global Config)
			L3E	Yes	GUI L3E Port Monitor CLI L3E port-monitor condition link-flap (Global Config)
			L3P	Yes	GUI L3P Port Monitor CLI L3P port-monitor condition link-flap (Global Config)

Action	Default setting	Recommended setting	Available in SW version		Further information
Activate detection of CRC/fragment errors for each port	Off	On	L2B	No	
			L2E	No	
			L2P	Yes	GUI L2P Port Monitor CLI L2P port-monitor condition crc-fragment (Global Config)
			L3E	Yes	GUI L3E Port Monitor CLI L3E port-monitor condition crc-fragment (Global Config)
			L3P	Yes	GUI L3P Port Monitor CLI L3P port-monitor condition crc-fragment (Global Config)
Action: Activate sending of trap for each port	Deactivate port	Send trap	L2B	No	
			L2E	No	
			L2P	Yes	GUI L2P Port Monitor CLI L2P port-monitor action
			L3E	Yes	GUI L3E Port Monitor CLI L3E port-monitor action
			L3P	Yes	GUI L3P Port Monitor CLI L3P port-monitor action

Send SNMP traps when using VRRP/HiVRRP

When you are using router redundancy with VRRP or HiVRRP, get the switch to report important status changes to you via SNMP traps:

☐ When the router becomes master

☐ When the router receives VRRP frames with incorrect authentication

Action	Default setting	Recommended setting	Available in SW version		Further information
Send VRRP master trap	Off	On	L2B	No	
			L2E	No	
			L2P	No	
			L3E	Yes	GUI L3E VRRP/HiVRRP CLI L3E vrrp trap
			L3P	Yes	GUI L3P VRRP/HiVRRP CLI L3P vrrp trap
Send VRRP authentication trap	Off	On	L2B	No	
			L2E	No	
			L2P	No	
			L3E	Yes	GUI L3E VRRP/HiVRRP CLI L3E vrrp trap
			L3P	Yes	GUI L3P VRRP/HiVRRP CLI L3P vrrp trap

4.5 Service Level Management (Network Quality)

4.5.1 Threats

One of the main goals of IT security is to protect availability. In industrial environments, network availability is more than just the actual reachability of systems. Depending on the application, the following aspects play a role:

- ☐ Quality of service (QoS)
- ☐ Integrity of the network
- ☐ High availability (ring structure, meshed structure)

The following threats exist for the switch, and thus for the network:

- ☐ Loss of connection due to failure of the switch
- ☐ Loss of connection due to cable defect
- ☐ Loss of connection due to overload
- ☐ Loss of connection due to attack on the redundancy mechanisms
- ☐ Latencies due to overload
- ☐ Jitter due to overload
- ☐ Limitation of availability due to connection of undesired devices

4.5.2 Security Quick Check for “Service Level Management”

Do you require?	If necessary	If not necessary
High network availability	Set up network as ring structure Activate HIPER-Ring protocol Activate MRP Activate faster ring configuration Deactivate Spanning Tree protocol	
High network availability and network separation via VLAN	Prioritize switch management frames Configuration of trust mode	
Are different priority classes required for the network traffic?	Configuration of priority classes for each port Configuration of mapping of VLAN priority classes to traffic class Configuration of mapping of IP DSCP to traffic class	
Can the unauthorized connection of devices to the network limit the service level of the network?	Configuration of MAC-based port security Configuration of IP-based port security Configuration of 802.1x port security	
Can the overloading of the network lead to problems?	Set threshold value for upper threshold of the network load and notify via SNMP trap Configuration of rate limiter	
Is the switch being used as a router in an environment with high availability requirements?	Use redundant routers	
Basic principle		
The measures follow the minimal principle in order to reduce the system load of the switch and its area of attack. Generally, you should deactivate services not required.		
General measures		
Activate RAM self-test Activate Cold start for undefined software behavior		

Table 3: Security Quick Check for “Service Level Management”

4.5.3 Measures

Known limitations:
☐ Depending on the switch model, 4 or 8 traffic classes are possible

Set up network as ring structure

With its redundancy protocols, the ring structure provides greater reliability in high availability networks. Therefore, set up the network as a ring.

Action	Default setting	Recommended setting	Available in SW version		Further information
Set up the network as a ring structure	None	None	L2B	Yes	GUI L2B Ring Redundancy CLI L2B HIPER-Ring
			L2E	Yes	GUI L2E Ring Redundancy CLI L2E HIPER-Ring
			L2P	Yes	GUI L2P Ring Redundancy CLI L2P HIPER-Ring
			L3E	Yes	GUI L3E Ring Redundancy CLI L3E HIPER-Ring
			L3P	Yes	GUI L3P Ring Redundancy CLI L3P HIPER-Ring

Activate HIPER-Ring protocol

The HIPER-Ring protocol supports high availability in networks with a ring-shaped structure. It also offers defined switching times and comprehensive logging and alarm options when a section fails. HIPER-Ring is a protocol developed by Hirschmann that has stood the test of time very well in practice over many years.

Note: Either HIPER-Ring or MRP can be used.

Action	Default setting	Recommended setting	Available in SW version		Further information
Activate HIPER-Ring protocol	On	On	L2B	Yes	Configure GUI L2B HIPER-Ring CLI L2B hiper-ring
			L2E	Yes	Configure GUI L2E HIPER-Ring CLI L2E hiper-ring
			L2P	Yes	Configure GUI L2P HIPER-Ring CLI L2P hiper-ring
			L3E	Yes	Configure GUI L3E HIPER-Ring CLI L3E hiper-ring
			L3P	Yes	Configure GUI L3P HIPER-Ring CLI L3P hiper-ring

Activate MRP

Like HIPER Ring, the MRP protocol also provides the functions required for the operation of high availability networks in ring form. However, MRP is an open, standardized protocol that can be operated with the products of other manufacturers. Additionally, in the case of a ring failure it provides guaranteed switching times while adhering to the specified framework conditions. Also, the VLAN can be defined freely for the Ring protocol.

Note: Either HIPER-Ring or MRP can be used.

Action	Default setting	Recommended setting	Available in SW version		Further information
Activate MRP	Off	On	L2B	Yes	Configure GUI L2B MRP ring CLI L2B mrp current-domain
			L2E	Yes	Configure GUI L2E MRP ring CLI L2E mrp current-domain
			L2P	Yes	Configure GUI L2E MRP ring CLI L2E mrp current-domain
			L3E	Yes	Configure GUI L3E MRP ring CLI L3E mrp current-domain
			L3P	Yes	Configure GUI L3P MRP ring CLI L3P mrp current-domain

Activate faster ring configuration

If a section fails within a network with a ring-shaped structure, this option provides faster restoring of the data transfer in the ring.

Where possible, use a faster ring configuration. However, exceptions to this may be very large rings, a lot of traffic or a high rate of lost frames.

Action	Default setting	Recommended setting	Available in SW version		Further information
Activate faster ring configuration	Standard	activated	L2B	Yes	Configure GUI L2B HIPER-Ring CLI L2B hiper-ring recovery-delay
			L2E	Yes	Configure GUI L2E HIPER-Ring CLI L2E hiper-ring recovery-delay
			L2P	Yes	Configure GUI L2P HIPER-Ring CLI L2P hiper-ring recovery-delay
			L3E	Yes	Configure GUI L3E HIPER-Ring CLI L3E hiper-ring recovery-delay
			L3P	Yes	Configure GUI L3P HIPER-Ring CLI L3P hiper-ring recovery-delay

Deactivate Spanning Tree protocol

If the network has a completely ring-shaped structure and the formation of loops in the network can be ruled out, the Spanning Tree protocol should be deactivated. Otherwise every status change at a switch port causes a reconfiguration of the spanning tree in the network and impedes the network traffic for several seconds, and for up to several minutes.

Action	Default setting	Recommended setting	Available in SW version		Further information
Deactivate Spanning Tree protocol	Off	Off	L2B	Yes	GUI L2B Global CLI L2B spanning-tree
			L2E	Yes	GUI L2E Global CLI L2E spanning-tree
			L2P	Yes	GUI L2P Global CLI L2P spanning-tree
			L3E	Yes	GUI L3E Global CLI L3E spanning-tree
			L3P	Yes	GUI L3P Global CLI L3P spanning-tree

Prioritize switch management frames

The switches provide the option to prioritize management frames for the configuration and monitoring of the switches. This enables the management traffic to be transmitted more reliably when there is a high network load. Especially in error situations, access to the switches is very important for identifying the cause and removing the error. Therefore, activate this option.

The prioritizing is effective for HTTP, HTTPS, Telnet and other IP traffic to the management IP address of the switch.

Action	Default setting	Recommended setting	Available in SW version		Further information
Prioritize switch management frames	0	7	L2B	Yes	GUI L2B Global CLI L2B network priority
			L2E	Yes	GUI L2E Global CLI L2E network priority
			L2P	Yes	GUI L2P Global CLI L2P network priority
			L3E	Yes	GUI L3E Global CLI L3E network priority
			L3P	Yes	GUI L3P Global CLI L3P network priority

Configuration of trust mode

The trust mode defines whether and how the switch evaluates QoS tags in received frames and prioritizes the frames accordingly.

Action	Default setting	Recommended setting	Available in SW version		Further information
Configuration of trust mode	trustDot1p	When using VLAN on this port: “trustDot1p”, otherwise “trustDscp”	L2B	Yes	GUI L2B Global CLI L2B classofservice trust
			L2E	Yes	GUI L2E Global CLI L2E classofservice trust
			L2P	Yes	GUI L2P Global CLI L2P classofservice trust
			L3E	Yes	GUI L3E Global CLI L3E classofservice trust
			L3P	Yes	GUI L3P Portkonfiguration CLI L3P classofservice trust

Configuration of priority classes for each port

Frames that cannot be prioritized with the “trustDot1p” or “trustDscp” mode, or frames that are received in the “untrusted” mode, are prioritized based on the configured priority of the switch port. Therefore, configure the priorities on the switch ports (as a backup solution).

Action	Default setting	Recommended setting	Available in SW version		Further information
Port priority	0	Depending on the application, between 0 and 7	L2B	Yes	Enter GUI L2B port priority CLI L2B vlan port priority all
			L2E	Yes	Enter GUI L2E port priority CLI L2E vlan port priority all
			L2P	Yes	Enter GUI L2P port priority CLI L2P vlan port priority all
			L3E	Yes	Enter GUI L3E port priority CLI L3E vlan port priority all
			L3P	Yes	Enter GUI L3P port priority CLI L3P vlan port priority all

Configuration of mapping of VLAN priority classes to traffic class

The following switches support 4 traffic class divisions:

RS20/30/40; MS20/30; Octopus; MACH102; RSR; MACH1020/1030; RSB

In the VLAN based on 802.1d, however, 8 priorities are supported. Therefore, map the VLAN priorities to the internal traffic class. The default settings are usually sufficient. In your specific application case, check the default settings and adjust them if necessary.

Action	Default setting	Recommended setting	Available in SW version		Further information
Mapping 802.1q to traffic class	0 1 2 3 4 5 6 7	1 (default) 0 (default) 0 (default) 1 (default) 2 (default) 2 (default) 3 (default) 3 (default)	L2B	Yes	GUI L2B 802.1D/p Mapping CLI L2B classofservice dot1p-mapping
			L2E	Yes	GUI L2E 802.1D/p Mapping CLI L2E classofservice dot1p-mapping
			L2P	Yes	GUI L2P 802.1D/p Mapping CLI L2P classofservice dot1p-mapping
			L3E	Yes	GUI L3E 802.1D/p Mapping CLI L3E classofservice dot1p-mapping
			L3P	Yes	GUI L3P 802.1D/p Mapping CLI L3P classofservice dot1p-mapping

Configuration of mapping of IP DSCP to traffic class

Most versions of the switches support 4 traffic class divisions. Exception: In software versions L3E and L3P, the switches support 8 traffic classes. However, IP DSCP supports 63 DSCP values. Therefore, map the DSCP values to the internal traffic classes. The default settings are usually sufficient. In your specific application case, check the default settings and adjust them if necessary.

Action	Default setting	Recommended setting	Available in SW version		Further information
Mapping DSCP to traffic class	See CLI documentation	Default settings	L2B	Yes	GUI L2B IP DSCP Mapping CLI L2B classofservice ip-dscp-mapping
			L2E	Yes	GUI L2E IP DSCP Mapping CLI L2E classofservice ip-dscp-mapping
			L2P	Yes	GUI L2P IP DSCP Mapping CLI L2P classofservice ip-dscp-mapping

Configuration of MAC-based port security

To prevent undesired devices from connecting to the network, the switches allow you to permit specific devices for each port based on their MAC addresses. For environments in which the physical access control for a switch port is not sufficient, this can be used to improve the security.

Action	Default setting	Recommended setting	Available in SW version		Further information
Configuration of MAC-based port security	No MAC addresses defined	MAC addresses that are to be permitted at the switch port	L2B	No	
			L2E	Yes	GUI L2E Port Security CLI L2E port-sec allowed-mac
			L2P	Yes	GUI L2P Port Security CLI L2P port-sec allowed-mac
			L3E	Yes	GUI L3E Port Security CLI L3E port-sec allowed-mac
			L3P	Yes	GUI L3P Port Security CLI L3P port-sec allowed-mac

Possible negative effects:

Availability: When connected devices are replaced (e.g. in a service situation), the MAC address changes and the device does not get a network connection until the switch port has been reconfigured.

Known limitations:

In many systems, the MAC address can be changed manually to break through the protection. A maximum of 10 addresses can be configured at a time via the CLI. A total of 50 addresses are possible via individual Add/Delete commands.

Configuration of IP-based port security

To prevent undesired devices from connecting to the network, the switches allow you to permit specific devices for each port based on their IP addresses.

Action	Default setting	Recommended setting	Available in SW version		Further information
Configuration of IP-based port security	No IP addresses defined	IP addresses that are to be permitted at the switch port	L2B	No	
			L2E	Yes	GUI L2E Port Security CLI L2E port-sec allowed-ip
			L2P	Yes	GUI L2P Port Security CLI L2P port-sec allowed-ip
			L3E	Yes	GUI L3E Port Security CLI L3E port-sec allowed-ip
			L3P	Yes	GUI L3P Port Security CLI L3P port-sec allowed-ip

Known limitations:

Filtering based on IP addresses provides little protection in most cases. A maximum of 10 IP addresses can be configured per port.

Configuration of 802.1x port security

To prevent undesired devices from connecting to the network, the switches allow you to control the login centrally via 1 or 2 RADIUS servers. Permitted MAC addresses are configured centrally and also the assignment to specific VLANs, if required.

Action	Default setting	Recommended setting	Available in SW version		Further information
Configuration of 802.1x Port Security	See CLI documentation	Default settings	L2B	No	
			L2E	No	
			L2P	Yes	GUI L2P IEEE 802.1X Port Authentication CLI L2P dot1x port-control
			L3E	Yes	GUI L3E IEEE 802.1X Port Authentication CLI L3E dot1x port-control
			L3P	Yes	GUI L3P IEEE 802.1X Port Authentication CLI L3P dot1x port-control

Possible negative effects:

Availability: If all the RADIUS servers fail, or the network connection to there, no device can login to the network any more.

Set threshold value for upper threshold of the network load and notify via SNMP trap

In order to detect an overload situation, the switch provides the option to send an alarm for each port when a threshold value for the network load is exceeded. Activate this function to detect an overload situation quickly.

Action	Default setting	Recommended setting	Available in SW version		Further information
Configure threshold value for network load and alarm	0.00 % and deactivated for every interface	Load values depend on application situation; alarm on	L2B	Yes	GUI L2B load (network load)
			L2E	Yes	GUI L2E load (network load)
			L2P	Yes	GUI L2P load (network load)
			L3E	Yes	GUI L3E load (network load)
			L3P	Yes	GUI L3P load (network load)

Configuration of rate limiter

The function of the rate limiter allows incoming or outgoing frames (broadcasts, multicasts, unicasts from MAC addresses not learned yet) to be filtered in terms of a specific bandwidth (Kbit/s) or in terms of frames (depends on the product used). This improves the protection against overloading for both the switch and the devices behind it.

Only use the rate limiter if the effects on the network can be estimated and you can estimate and accept the risks of using this function.

Action	Default setting	Recommended setting	Available in SW version		Further information
Incoming frame types	BC (broadcasts)	BC (default)	L2B	No	
			L2E	Yes	GUI L2E Rate Limiter CLI L2E storm-control broadcast
			L2P	Yes	GUI L2P Rate Limiter CLI L2P storm-control broadcast
			L3E	Yes	GUI L3E Rate Limiter CLI L3E storm-control broadcast
			L3P	Yes	GUI L3P Rate Limiter CLI L3P storm-control broadcast
Ingress limiter	Off	On	L2B	No	
			L2E	Yes	GUI L2E Rate Limiter CLI L2E storm-control ingress-limiting
			L2P	Yes	GUI L2P Rate Limiter CLI L2P storm-control ingress-limiting
			L3E	Yes	GUI L3E Rate Limiter CLI L3E storm-control ingress-limiting
			L3P	Yes	GUI L3P Rate Limiter CLI L3P storm-control ingress-limiting

Action	Default setting	Recommended setting	Available in SW version		Further information
Ingress limiting rate per port	0 (off)	5% of the port bandwidth	L2B	No	
			L2E	Yes	GUI L2E Rate Limiter CLI L2E storm-control ingress-limit
			L2P	Yes	GUI L2P Rate Limiter CLI L2P storm-control ingress-limit
			L3E	Yes	GUI L3E Rate Limiter CLI L3E storm-control ingress-limit
			L3P	Yes	GUI L3P Rate Limiter CLI L3P storm-control ingress-limit
Egress limiter BC	Off	Off (default)	L2B	No	
			L2E	Yes	GUI L2E Rate Limiter CLI L2E storm-control broadcast
			L2P	Yes	GUI L2P Rate Limiter CLI L2P storm-control broadcast
			L3E	Yes	GUI L3E Rate Limiter CLI L3E storm-control broadcast
			L3P	Yes	GUI L3P Rate Limiter CLI L3P storm-control broadcast
Egress limiting rate BC per port	0 (off)	0 (off, default)	L2B	No	
			L2E	Yes	GUI L2E Rate Limiter CLI L2E storm-control broadcast (port-related)
			L2P	Yes	GUI L2P Rate Limiter CLI L2P storm-control broadcast (port-related)
			L3E	Yes	GUI L3E Rate Limiter CLI L3E storm-control broadcast (port-related)
			L3P	Yes	GUI L3P Rate Limiter CLI L3P storm-control broadcast (port-related)

Action	Default setting	Recommended setting	Available in SW version		Further information
Egress limiting rate all	Off	Off (default)	L2B	No	
			L2E	Yes	GUI L2E Rate Limiter CLI L2E storm-control egress-limiting
			L2P	Yes	GUI L2P Rate Limiter CLI L2P storm-control egress-limiting
			L3E	Yes	GUI L3E Rate Limiter CLI L3E storm-control egress-limiting
			L3P	Yes	GUI L3P Rate Limiter CLI L3P storm-control egress-limiting
Egress limiting rate all per port	0 (off)	0 (off, default)	L2B	No	
			L2E	Yes	GUI L2E Rate Limiter CLI L2E storm-control egress-limit
			L2P	Yes	GUI L2P Rate Limiter CLI L2P storm-control egress-limit
			L3E	Yes	GUI L3E Rate Limiter CLI L3E storm-control egress-limit
			L3P	Yes	GUI L3P Rate Limiter CLI L3P storm-control egress-limit

Use redundant routers

When using the switch as a router in an environment with high availability requirements, use an additional router to increase the availability in the case of a failure (redundancy). This router communicates via the VRRP or HiVRRP protocol to determine when the other router takes over the data transmission. Here it is also possible to use fake (Hi)VRRP frames to impair the availability of the network.

Action	Default setting	Recommended setting	Available in SW version		Further information
Activate VRRP/HiVRRP	Off	On	L2B	No	
			L2E	No	
			L2P	No	
			L3E	Yes	GUI L3E VRRP/HiVRRP Configuration CLI L3E ip vrrp
			L3P	Yes	GUI L3P VRRP/HiVRRP Configuration CLI L3P ip vrrp
Activate authentication on interface (in wizard)	noAuthentication	simpleTextPassword	L2B	No	
			L2E	No	
			L2P	No	
			L3E	Yes	GUI L3E VRRP/HiVRRP Configuration CLI L3E ip vrrp authentication
			L3P	Yes	GUI L3P VRRP/HiVRRP Configuration CLI L3P ip vrrp authentication
Enter key (in wizard)	<empty>	Secure password of 16 characters	L2B	No	
			L2E	No	
			L2P	No	
			L3E	Yes	GUI L3E VRRP/HiVRRP Configuration CLI L3E ip vrrp authentication
			L3P	Yes	GUI L3P VRRP/HiVRRP Configuration CLI L3P ip vrrp authentication

Activate RAM self-test

The RAM self-test tests the RAM of the switch during the booting procedure for possible errors and can thus prevent errors during operation.

Action	Default setting	Recommended setting	Available in SW version		Further information
RAM test	On	On	L2B	Yes	GUI L2B Selftest CLI L2B selftest
			L2E	Yes	GUI L2E Selftest CLI L2E selftest ramtest
			L2P	Yes	GUI L2P Selftest CLI L2P selftest ramtest
			L3E	Yes	GUI L3E Selftest CLI L3E selftest ramtest
			L3P	Yes	GUI L3P Selftest CLI L3P selftest ramtest

Cold start for undefined software behavior

If undefined behavior occurs in the software of the switch during operation, the switch can restart itself. This function helps to prevent errors and problems during operation due to individual subsystems that are not working (correctly) any more.

Action	Default setting	Recommended setting	Available in SW version		Further information
Cold start for undefined software behavior	On	On	L2B	Yes	GUI L2B Selftest CLI L2B selftest reboot-on-error
			L2E	Yes	GUI L2E Selftest CLI L2E selftest reboot-on-error
			L2P	Yes	GUI L2P Selftest CLI L2P selftest reboot-on-error
			L3E	Yes	GUI L3E Selftest CLI L3E selftest reboot-on-error
			L3P	Yes	GUI L3P Selftest CLI L3P selftest reboot-on-error

4.6 Updates

4.6.1 Threats

Hirschmann regularly expands and improves the software of the switch. Hirschmann makes the resulting updates available for downloading from the product page on the Internet. Implement the updates on the switch.

This results in the following threats:
- ☐ Implementation of defective/damaging software
- ☐ Interruption of the update process
- ☐ Misuse of the update function

A defective or malicious update can be implemented deliberately, and this can impair the confidentiality and integrity and even the availability of the switch.

You can counteract the threats with the following configuration items:

4.6.2 Security Quick Check

Do you require?	If necessary	If not necessary
Security for your application	Regularly check on security-relevant updates and their installation	

Basic principle
New security gaps are discovered every day in the widest variety of systems. Close these gaps quickly in security-relevant systems. They can often be caused by the installation of new software on the switch.
General measures
☐ Regularly check on updates to remove errors and their installation ☐ Obtain updates from a trusted source ☐ No updates during ongoing operation

Table 4: Security Quick Check for “Updates”

4.6.3 Measures

Regularly check on security-relevant updates and their installation

You can close many security gaps that have been discovered by means of an update that closes these gaps. Please note the following:

☐ Inform yourself regularly at Hirschmann about security gaps that have been discovered.

☐ As soon as new software closes the gaps, implement this new software.

You will find information sources in section 1.4 “Further Information”.

Regularly check on updates to remove errors and their installation

Along with security problems, you can also use updates to remove functional problems, including those that may exist but have not become apparent as yet.

Please note the following:

- ☐ Inform yourself regularly at Hirschmann about security gaps that have been discovered.
- ☐ As soon as new software closes the gaps, implement this new software.

You will find information sources in section 1.4 “Further Information”.

Obtain updates from a trusted source

Only obtain the software directly from the manufacturer in a ZIP archive at http://www.hirschmann.de/de/Hirschmann/Industrial_Ethernet/Software/Software_Platforms/index.phtml. Using check sums, the ZIP archive can detect whether the updates were damaged by transfer errors during the transfer process.

Known limitations: The updates are not digitally signed and are therefore not protected against manipulation on the way from Hirschmann to the switch.

The JAR file (JAVA applet) in the software contains SHA-1 check sums. Additionally, the JAR file is signed with a code signing certificate from Hirschmann (Digital ID Class 3 Java Object Signing) that was issued by Verisign.

When the validity of the certificate has elapsed, the user receives a warning notice to this effect. It is not possible to extend the certificate. You may possibly be able to implement a newer certificate via an update to a current software version of the switch. You can read about this in the release notes if necessary.

No updates during ongoing operation

During the update, the processor of the switch is subject to an additional load and may possibly behave differently. Also, after the update the switch requests a restart. This can limit network availability, particularly when Spanning Tree is being used.

4.7 Decommissioning

4.7.1 Threats

When a switch has reached the end of the planned period of use, decommission it.

This results in the following threats:
☐ Reading out of the configuration after decommissioning
☐ Reconnection due to human error/sabotage
☐ Reading out of secret keys (SSL and SSH)

4.7.2 Security Quick Check

Do you require?	If necessary	If not necessary
Security after planned life cycle	Regularly check on security-relevant updates and their installation Reset the configuration (clear config) Delete the Auto-Configuration Adapter (ACA)	
Basic principle		
Reading out the configuration can compromise the confidentiality because passwords can be read out, for example.		

4.7.3 Measures

You can counteract the threats with the following configuration items:

Reset the configuration

If a switch is accidentally or carelessly connected to a network, the availability can be impaired. Examples of this are Spanning Tree calculation times or IP address conflicts

Action	Default setting	Recommended setting	Available		Further information
Clear Config	-	Clear config factory	L2B	Yes	GUI L2B Configuration Load/Save CLI L2B clear config factory
			L2E	Yes	GUI L2E Configuration Load/Save CLI L2E clear config factory
			L2P	Yes	GUI L2P Configuration Load/Save CLI L2P clear config factory
			L3E	Yes	GUI L3E Configuration Load/Save CLI L3E clear config factory
			L3P	Yes	GUI L3P Configuration Load/Save CLI L3P clear config factory

Delete the Auto-Configuration Adapter (ACA)

The mere removal of the existing files on the ACA does not provide sufficient protection to prevent a third party from restoring them. For safe deletion of flash memories such as the ACA, the Federal Office for Information Security (BSI) recommends: “Where there is a high security requirement, the entire memory area must be overwritten three times using suitable software.” [2]

You will find an option for suitable software on the BSI website. [3]

4.8 Disturbance

4.8.1 Threats

The switch supplied is a high-quality product in terms of hardware and software. However, defects are still possible here, such as when a device is operated outside the recommended specifications.

This results in the following threats:

- Limitation of the availability
- Reading out of the configuration
- Reading out of secret keys (SSL and SSH), passwords and SNMP community strings

4.8.2 Security Quick Check for “Disturbance”

Do you require?	If necessary	If not necessary
Confidentiality in very sensitive areas and you are replacing the device	Regularly check on security-relevant updates and their installation. The Help Desk can evaluate your diagnosis of the defect and start the RMA process. If, against expectations, the error is a configuration error, taking the route via the Help Desk saves time compared with sending the device in directly.As the memory cannot be deleted safely for technological reasons, no guarantee is made for the stored data. Contact the Help Desk	Contact the Help Desk

Basic principle

Reading out the configuration can compromise the confidentiality because passwords can be read out, for example. In very sensitive areas, this can be classified as not acceptable.

4.8.3 Measures

Contact the Help Desk

Contact the Help Desk so that your case can be processed as quickly as possible. You can reach the Help Desk via the following portal.

https://hirschmann-support.belden.eu.com

The Help Desk can evaluate your diagnosis of the defect and start the RMA process. If, against expectations, the error is a configuration error, taking the route via the Help Desk saves time compared with sending the device in directly.

As the memory cannot be deleted safely for technological reasons, no guarantee is made for the stored data.

Physical Destruction

If you have installed the device in a highly sensitive area, do not send in the device but dispose of it yourself by physically destroying it.

A References

[1] Homeland Security (2009) Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies

[2] Bundesamt für Sicherheit in der Informationstechnik (2011) IT-Grundschutz-Katalog - M 2.167 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten

[3] Bundesamt für Sicherheit in der Informationstechnik - So löschen Sie Daten richtig https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/RichtigLoeschen/richtigloeschen_node.html

B Readers' Comments

What is your opinion of this manual? We are always striving to provide as comprehensive a description of our product as possible, as well as important information that will ensure trouble-free operation. Your comments and suggestions help us to further improve the quality of our documentation.

Your assessment of this manual:

	Very good	Good	Satisfactory	Mediocre	Poor
Precise description	O	O	O	O	O
Readability	O	O	O	O	O
Understandability	O	O	O	O	O
Examples	O	O	O	O	O
Structure	O	O	O	O	O
Completeness	O	O	O	O	O
Graphics	O	O	O	O	O
Drawings	O	O	O	O	O
Tables	O	O	O	O	O

Did you discover any errors in this manual?
If so, on what page?

Readers' Comments

Suggestions for improvement and additional information:

General comments:

Sender:

Company / Department:

Name / Telephone no.:

Street:

Zip code / City:

e-mail:

Date / Signature:

Dear User,

Please fill out and return this page

- as a fax to the number +49 (0)7127 14-1600 or
- by post to

  Hirschmann Automation and Control GmbH
  Department 01RD-NT
  Stuttgarter Str. 45-51
  72654 Neckartenzlingen

C Further Support

Technical Questions

For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly.

You will find the addresses of our partners on the Internet at http://www.hirschmann.com

Contact our support at https://hirschmann-support.belden.eu.com

You can contact us

in the EMEA region at
- Tel.: +49 (0)1805 14-1538
- E-mail: hac.support@belden.com

in the America region at
- Tel.: +1 (717) 217-2270
- E-mail: inet-support.us@belden.com

in the Asia-Pacific region at
- Tel.: +65 6854 9860
- E-mail: inet-ap@belden.com

Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors:
- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- Training offers you an introduction to the basics, product briefing and user training with certification.
  The current technology and product training courses can be found at http://www.hicomcenter.com
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you have decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.
Internet:
http://www.hicomcenter.com

HIRSCHMANN
A BELDEN BRAND

www.hirschmann.com

GLOBAL LOCATIONS

For more information, please visit us at:
www.beldensolutions.com

Be certain you stay in touch.

EUROPE/MIDDLE EAST/AFRICA

Germany – Head Office
Phone: +49-7127-14-0
inet-sales@belden.com

France
Phone: +33-1-393-501-00
reseau.france@belden.com

Italy
Phone: +39-039-5965-250
info.milano@belden.com

Russia
Phone: +7-495-287-1391
info@belden.ru

Spain
Phone: +34-91-746-17-30
madrid.salesinfo@belden.com

Sweden
Phone: +46-40-699-88-60
inet-sales@belden.com

The Netherlands
Phone: +31-773-878-555
venlo.salesinfo@belden.com

United Arab Emirates
Phone: +971-4-391-0490
dubai.salesinfo@belden.com

United Kingdom
Phone: +44 161 4983749
manchester.salesinfo@belden.com

AMERICAS

USA
Phone: +1-855-400-9071
inetsalesops@belden.com

ASIA/PACIFIC

Singapore
Phone: +65-6879-9800
singapore.sales@belden.com

China
Phone: +86-21-5445-2353
China.Marketing@belden.com

Contact us

Printed in Germany

ICS-SECURITY-GUIDE-TO-HIRSCHMANN-SWITCHES_INIT_HIR_0915_E_EMEA