HIRSCHMANN
A BELDEN BRAND

User Manual

Security
BOBCAT Rail Switch
HiOS-2S

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

You find the latest user documentation for your device at: doc.hirschmann.com

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany

Contents

Document History

Version	Finalize date	Finalized by	Relevant content changes
0.21a	2021-08-30	U. Messerle	Prepared draft for review.
0.30b	2021-11-02	U. Messerle	Reworked according to review results: Removed default user credentials "user/public". Added "hardening" to scope. Generalized some descriptions for device security (they also apply to operation and maintenance). Added backup recommendation. Detailed steps for sending a device for repair. Detailed the recommendation to disable L2 loop protection.
0.99a (RC1)	2022-03-18	U. Messerle	Added chapter "Plan a dedicated logging policy". Updated chapter "Operations". Updated configuration details by referring to the respective user manuals. Expanded topics "Defense in depth" and "Hardening" in main chapter "Network security".
0.99b (RC2)	2022-03-30	U. Messerle	Reworked the delivery states of several settings. Added setting for OPC UA Server.
0.99c (RC3)	2022-04-04	U. Messerle	(Internal) Removed misplaced function-related tag.
0.99d (RC4)	2022-04-05	U. Messerle	Review incorporated: Improved description of hardening. Clarified restrictions to physical access. Pointed out forced password change. Removed claims that the external memory function of the USB port can be disabled. Changed delivery state setting of EtherNet/IP management access to disabled. More detailed logging configuration. Added CLI pre-login banner. More detailed backup creation. Added cross references.
0.99e (RC5)	2022-04-05	U. Messerle	(Minor) Improved grammar.
0.99f (RC6)	2022-04-06	U. Messerle	Aligned document to terminology and language rules. Improved description of PoE delivery state settings.
0.99g (RC7)	2022-04-08	U. Messerle	Moved this history to the beginning of the document and updated column headers.
0.99h (RC8)	2022-04-13	U. Messerle	Detailed time synchronization considerations.
0.99i (RC9)	2022-05-17	U. Messerle	Defined responsibility for defense in depth and hardening and recommended how to select security measures.
Rel. 8.7	2022-05-31	U. Messerle	Released for BOBCAT Rail Switch (BRS).

Safety instructions

⚠ WARNING

UNCONTROLLED MACHINE ACTIONS

To avoid uncontrolled machine actions caused by data loss, configure all the data transmission devices individually.

Before you start any machine which is controlled via data transmission, be sure to complete the configuration of all data transmission devices.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

About this Manual

The “Configuration” user manual contains the information you need to start operating the device. It takes you step by step from the first startup operation through to the basic settings for operation in your environment.

The “Installation” user manual contains a device description, safety instructions, a description of the display, and the other information that you need to install the device.

The “Graphical User Interface” reference manual contains detailed information on using the graphical user interface to operate the individual functions of the device.

The “Command Line Interface” reference manual contains detailed information on using the Command Line Interface to operate the individual functions of the device.

The “Security” user manual contains considerations for system security planning, recommendations for the device security over the device lifecycle, and descriptions how the device can help to improve the security of your network.

The Industrial HiVision Network Management software provides you with additional options for smooth configuration and monitoring:

- Auto-topology discovery
- Browser interface
- Client/server structure
- Event handling
- Event log
- Simultaneous configuration of multiple devices
- Graphical user interface with network layout
- SNMP/OPC gateway

Key

The designations used in this manual have the following meanings:

▶	List
☐	Work step
Link	Cross-reference with link
Note:	A note emphasizes a significant fact or draws your attention to a dependency.
`Courier`	Representation of a CLI command or field contents in the graphical user interface

Execution in the Graphical User Interface

Execution in the Command Line Interface

1 Security planning

1.1 Introduction

1.1.1 Subject

The user manual "Security" contains security recommendations for your network device. It deals with the following lifecycle phases of your device:

- Secure installation
- Secure commissioning
- Secure administration and operation
- Secure maintenance
- Secure decommissioning

A secured device in turn can help you to maintain the security and availability of your network.

1.1.2 Audience

This security manual primarily addresses ETHERNET network planners, commissioners, administrators, operators, maintainers, and decommissioners.

Its contents may also be useful for solution providers, sales partners, and system integrators.

1.1.3 Scope

This document deals with the recommended device security measures throughout the device lifecycle. These recommendations include:

- How to achieve defense in depth for the device
- How to harden the device
- How a specifically configured device can help you achieve defense in depth for your system
- How a specifically configured device can help you harden your system

A network device is part of a superordinate system. Therefore, the device and the system are interdependent. The system lifecycle and the requirements of the system for defense in depth are outside the scope of this document. References to the system lifecycle are made only if necessary, and only for information purposes.

For your network, additional planning and implementation steps may be necessary. For example, you may need an L3 network plan in addition to the VLAN plan mentioned in this document. The L3 network plan and the VLAN plan are both outside the scope of this document.

1.1.4 Capability security level

The security requirements, planning steps, and measures in this document deal with the capability security level 1 (SL-C 1) according to the standard IEC 62443-4-2. SL-C 1 means protection against casual or coincidental security violations.

Some security requirements, measures, and steps mentioned in this document may exceed the target security level SL-C 1. They are therefore not strictly required to achieve SL-C 1. They are nevertheless included when these security measures and steps generally mean little effort and reasonable effect.

1.1.5 Document Outline

The following main chapters deal with 2 main subjects:

- The security of the device itself (see on page 23 “Device security”)
- What a secured device can do for the security of your network (see on page 43 “Network security support”)

1.2 Defense in depth

1.2.1 Purpose

Defense in depth is a strategy that employs various independent security measures to guard an asset under consideration against specific attacks.

A system that employs defense in depth first confronts an attacker with a particular barrier. If an attacker overcomes this barrier, the system presents another barrier of a different type. A minimum of 2 barriers of different types shall guard any system asset under consideration. This layered security approach is considered best practice. It potentially demoralizes an attacker while taking the imperfection of real-world security barriers into account.

1.2.2 Defense in depth vs. hardening

In comparison to hardening, defense in depth is a more selective and structured approach. Defense in depth employs a specific subset of all conceivable security measures.

Hardening can be characterized as defense in broad. It aims at closing as many weaknesses in any barriers as possible and reasonable. A strategy for hardening may include the concepts "least necessary functions" for the device and "least necessary privileges" for user accounts.

Develop a strategy for defense in depth first. Then complement it by hardening.

1.2.3 Responsibilities

Defense in depth as well as hardening need planning, implementation and maintenance. It is the responsibility of the system operator to perform these steps.

Hirschmann recommends that you consider all security measures given in this manual, and to select those that are most relevant for the actual situation.

1.2.4 Example

ID	Barrier	Description
	System level	
1	Internet Firewall	An attacker must overcome the internet firewall between to get access to the company Intranet.
2	Industrial Firewall	An attacker must overcome the industrial firewall to get access to the industrial network. The industrial firewall separates the industrial network from the company Intranet.
3	Dedicated device management VLAN	An attacker must overcome VLAN restrictions to snoop packets like unknown unicast frames of device management traffic.
	Device level	
4	Secure management protocols only	An attacker must overcome encryption to snoop packet contents.

ID	Barrier	Description
5	Non-default user account names[1]	An attacker must guess or find out the real user account names.
6	Non-default passwords[2]	An attacker must guess or find out the real passwords.
7	Specific, restricted account privileges	An attacker must guess or find out the administrator account credentials to read privileged data or manipulate device settings.

1. Dedicated user account names can be device-specific and could be deliberately chosen to be non-descriptive.
2. Passwords can be specific to a certain access protocol (for example HTTPS or SNMPv3) and can be device-specific.

1.3 Impact of the system lifecycle to the device lifecycle

A network device is a component in a superordinate system. Therefore, the system lifecycle determines parts of the device lifecycle. A system lifecycle involves a planning phase. The decisions taken in the planning phase affect the device lifecycle directly or indirectly.

Typical decisions during system planning include:
- The physical position of the device, for example, its installation location and environment
- The logical position of the device, for example, the security zone
- The requirements of the system for defense in depth

1.3.1 VLAN plan

VLANs are a software-configurable concept to segregate a LAN (layer 1) into separate Virtual LANs (VLANs) on layer 2. Advantages include the separation of data packets belonging to different VLANs. The separation also applies to flooded multicast, broadcast, and unknown unicast frames. This helps confidentiality besides helping reduce the network load on layer 1.

A VLAN plan is a prerequisite for a secure configuration of the device itself and in turn for the security and availability of your system. Create a VLAN plan that segregates your network on layer 2. A dedicated management VLAN can be a barrier component in the strategy "Defense in depth".

For simple networks, a VLAN plan and the configuration of VLANs may be considered unnecessary from a functional perspective. However, VLANs are recommended from a security perspective.

Note: The redundancy protocols HIPER Ring and Ring/Network Coupling employ the fixed VLAN ID 1 for their protocol packets. Using the VLAN ID 1 exclusively for these redundancy protocols can help enhance network availability (see on page 21 “VLAN plan considerations depending on redundancy protocols”).

Note: For your network, additional planning and implementation steps may be necessary. For example, you may need an L3 network plan (outside the scope of this document) in addition to the VLAN plan.

1.4 Impact of device requirements on system planning

Some requirements of the device have an impact on the system lifecycle phases, in particular on system planning.

Topics of this interdependence include:
- A secure installation location, including the aspects:
  - Device availability: Power supply, power budget, and data link redundancy
  - Properties of the USB port
  - Properties of the Signal Contact
  - Properties of the Digital Input
  - Device and port LEDs
- The detailed physical device security requirements
- The user account policy parameters the device offers:
  - For the login policy
  - For the password policy
  - For the user name and access role policy
  - For the SNMPv3 authentication and encryption type, and password policy
- VLAN ID restrictions arising from certain redundancy protocols: VLAN IDs ≥2 for payload traffic and device management

Note: These topics are covered in more detail (see on page 23 “Device security”).

1.4.1 Secure installation location

Refer to the user manual "Installation" for a suitable physical installation location.

Select a location that in addition offers appropriate device security by restricting physical access:
- Install the device in a room that can be locked and where only authorized personnel have access.
- Install the device in a cabinet to which only authorized personnel have access.
- Install the device in a cabinet with an opaque door (see on page 19 “Device and port LEDs”).

Device availability

Device availability can be an important base for the security of the superordinate system. Therefore, check that the following device availability requirements are met as needed:
- Provide redundant power supply
- Provide an adequate power budget (device and PoE)
- Provide data link redundancy

Signal Contact

If you plan to use the Signal Contact, consider the following security aspects:
- To help protect the device, connect the Signal Contact only to a circuit that meets the device requirements.
- To help protect your system, connect the Signal Contact only to circuits that do not have explicit security or safety requirements.

Digital Input

If you plan to use the Digital Input, consider the following security aspects:
- To help protect the device, connect the Digital Input only to a circuit that meets the device requirements.
- To help protect your system, connect the Digital Input only to circuits that do not have explicit security or safety requirements.

Device and port LEDs

The device and port LEDs show important information about the device state and the port states.

To prevent information leakage, consider the following security aspects as needed in addition to the secure installation location:
- Install the device in a cabinet with an opaque door.
- Cover or obstruct the LEDs with a removable cover.

1.4.2 Plan a dedicated user account login policy

The device lets you configure a login policy for the user accounts. The login policy applies to all user accounts.

It applies to the following user interfaces and access protocols:
- The Command Line Interface (CLI) using SSH or Telnet
- The Graphical User Interface (GUI) using HTTPS or HTTP

You can configure the following requirements for the user login:
- Maximum number of failed user logins in a row until the device locks the respective user account.
- Waiting time (Login attempts period) before the device auto-unlocks a locked user account.

Access to the CLI using the serial connection is exempt from the login policy. Users accessing the CLI using the serial connection have an unlimited number of login attempts. They are also not required to wait for the next login attempt, that is, the Login attempts period does not apply. This ensures access to the device management in situations where availability may be critical, and for users who already have physical access to the device.

Note: Hirschmann recommends planning an overarching user account login policy and apply it to each device.

1.4.3 Plan a dedicated user account password policy

The device lets you configure a password policy for the user accounts. You can configure the following requirements for the password:
- Minimum password length
- Minimum number of uppercase characters
- Minimum number of lowercase characters
- Minimum number of digits
- Minimum number of special characters

Note: The device asks you to change the default password on the first login. Hirschmann recommends planning an overarching user account password policy and apply it to each device. To deter attackers, consider planning different passwords on different devices.

Table 1: User credentials for the user account in the delivery state

User Name	Default Password	Access Role	Privileges
admin	private	Administrator	Monitor the device and change settings.

Note: Software releases 08.1.00 and higher in the delivery state no longer offer a user account with the name `user` and the associated default password `public`. If you need a user account that has only read access, you can create a user account with the access role `guest` and the user name `user`.

1.4.4 Plan a dedicated user account name and access role policy for device management

Configure dedicated user accounts as needed:
- Assign the login and password policies.
- Create user accounts with:
  - Dedicated names[1]
  - Chosen access roles that offer only the least necessary privileges
- Assign the new user accounts strong, individual passwords and apply the password policy check.
  - Plan strong SNMPv3 authentication and encryption types and strong related passwords for the new user accounts.
- Remove user accounts with standard names.

Note: Hirschmann recommends planning an overarching user account and access role policy and apply it to each device. To deter attackers, consider planning different user account names and different passwords on different devices.

Hirschmann also recommends planning an overarching policy for SNMPv3 authentication and encryption types, and the related passwords. To deter attackers, consider planning different SNMPv3 passwords on different devices.

1.4.5 Plan a dedicated logging policy

Configure device logging settings:
- Synchronize the device system clock to a trusted source.
- Assign the logging destinations you require.
- Assign the severity levels you require.

Note: Hirschmann recommends planning an overarching device logging policy and apply it to each device.

1.User account could also be deliberately chosen to be non-descriptive.

1.4.6 VLAN plan considerations depending on redundancy protocols

Network availability can be an important base for the security of the superordinate system. The device offers redundancy protocols for this purpose.

The redundancy protocols HIPER Ring and Ring/Network Coupling employ the fixed VLAN ID 1 for their protocol packets. Using the VLAN ID 1 exclusively for these redundancy protocols can help enhance network availability. A VLAN plan (see on page 17 “VLAN plan”) that takes this peculiarity into account may require the use of VLAN IDs ≥2 for payload traffic and device management.

1.4.7 Network time synchronization considerations

Network time synchronization can be required for several reasons, including secure logging. The protocols NTP and PTP implicitly trust the time source. To make network time synchronization more secure, planning an overarching network time synchronization policy is recommended.

Parameters of this policy may include:

- The choice of the network protocol for time distribution
- The choice of the primary time sources
- The choice of time synchronization paths based on precision, availability and security considerations
- Requirements for controlling or tuning the chosen network time protocol on the nodes in the time synchronization path
- The choice of Multicast or Unicast packets on the network layer

As the protocols NTP and PTP implicitly trust the time source, plan suitable mitigation concepts. E.g., restrict the time sources a given device accepts.

Based on the chosen policy, determine which settings are necessary for the individual devices.

2 Device security

2.1 Security vs. functionality

This chapter deals with the device security throughout lifecycle phases of the device.

For the functional device lifecycle phases, refer to the detailed device documents:
- User manual "Installation", for example, for permissible ambient conditions
- User manual "Configuration", for example, for basic settings and software update
- Reference manual "Graphical User Interface", for example, for specific settings
- Reference manual "Command Line Interface", for example, for specific commands

2.2 Prerequisites for installation and setup

Hirschmann assumes that, when reading this section, you have already performed the system planning steps, including:

- The choice of a suitable physical location for the devices (see on page 26 “Choice of a secure installation location”)
- Creating a dedicated user account login policy (see on page 19 “Plan a dedicated user account login policy”)
- Creating a dedicated user account password policy
- Creating a dedicated user account and access role policy for device management
  - Creating a dedicated policy for SNMPv3 authentication and encryption types, and for the related passwords.
- Traffic segregation on layer 2 by a VLAN plan (see on page 17 “VLAN plan”)
- Use of a network management system like Industrial HiVision (outside the scope of this document)

2.3 Recommended installation work step sequence

The device security lifecycle phases in a practical order are:
- Choice of a secure installation location (see on page 26 “Choice of a secure installation location”)
- Initial software update (see on page 27 “Software update”)
- Initial security configuration (see on page 28 “Security configuration”)
- Possible hardware modification for security (see on page 38 “Possible hardware modifications for security”)
- Initial device installation (see on page 39 “Device installation”)
- Operation (see on page 40 “Operation”)
- Maintenance (see on page 41 “Maintenance”)
- Decommissioning (see on page 42 “Decommissioning”)

Note: Depending on your needs, you can perform the work steps in a different sequence.

2.3.1 Reasons for the recommended installation work step sequence

Performing the initial configuration and the initial software update before the initial device installation can have the following benefits:
- The required resources, for example, prepared configuration files and device labels, may be more conveniently available in an office location.
- Time-consuming steps like software updates can be performed in parallel.
- Associated devices, for example, devices participating in a ring redundancy, can be configured contiguously.
- For certain hardware measures like physically securing a USB port, you may need the USB port for the initial configuration and software update before you can lock the USB port.
- The remaining work steps in the field require less time.

2.3.2 Recommended preparation for installation

The following recommendations can help reduce the initial effort and save time:
- Check the available device software release on the Hirschmann product pages on the Internet at www.hirschmann.com.
- Decide which device software release you want to run on your devices.
- Download the selected software files.
- Prepare device configuration files based on your network plan.
- Prepare device labels.

Note: Hirschmann recommends that you use the latest available release of the device software.

2.4 Choice of a secure installation location

Refer to the user manual "Installation" for a suitable physical installation location. Select an installation location that in addition offers appropriate device security by restricting physical access.

Check that the following device security requirements are fulfilled if needed:
- Install the device in a room that can be locked and where only authorized personnel have access.
- Install the device in a cabinet to which only authorized personnel have access.
- Install the device in a cabinet with an opaque door (see on page 38 “Restrict physical (visual) access to the device and port LEDs”).

2.4.1 Device availability requirements

Device availability can be an important base for the security of the superordinate system. Therefore, also consider implementing measures that increase device availability.

Check that the following device availability requirements are fulfilled if needed:
- Provide redundant power supply (see on page 26 “Power supply redundancy requirements”)
- Provide an adequate power budget (see on page 26 “Power supply power budget requirements”)
- Provide data link redundancy (see on page 26 “Data link redundancy requirements”)

Power supply redundancy requirements

Check that the power supply redundancy requirements are fulfilled if needed:
- The device is powered by 2 redundant power sources.
- The power supply cables to the device run along different paths as far as possible.
- The power supplies themselves are powered in a redundant way, for example, by 2 separate mains cables.
- The mains cables to the redundant power supplies run along different paths.

Power supply power budget requirements

Refer to the user manual "Installation" for the power requirements of the device. Check that the power requirements are fulfilled if needed:
- One single power supply is able to deliver power for all the connected devices.
- One single power supply is also able to deliver the configured PoE or PoE+ power.

Data link redundancy requirements

Check that the data link redundancy requirements are fulfilled if needed:
- The device has redundant data links where needed (typically for uplinks).
- The cabinet or room has redundant data links when needed.
- The redundant data links of the cabinet or the room run along different paths.

2.5 Software update

The following description applies to:
- The initial software update for a device out-of-the-box
- A software update as part of operation or maintenance

Check if an updated release of the device software is available. You find information and software downloads on the Hirschmann product pages on the Internet at www.hirschmann.com. Then decide which software release you want to run on your device.

Note: To check the running software release on a device that does not yet have an IP configuration, Hirschmann recommends using HiView.

To update the software on the device, you need management access to the device, which requires at least a preliminary IP configuration. Hirschmann recommends using HiView to assign an IP configuration to the device. HiView then offers you to open the device management.

At the first login with the default password, the device asks you to change the password. Use a dedicated password according to your password policy (see on page 19 “Plan a dedicated user account password policy”).

Refer to the user manual "Configuration" for details on how to:
- Determine the currently running software release
- Determine the stored software release
- Check for newer available software release

If you decide to update the device software:
- Save the configuration profile in the volatile memory (*RAM*) to the non-volatile memory (*NVM*); see the user manual "Configuration", chapter "Managing configuration profiles".
- Back up the device configuration.
- Update the device software; see the user manual "Configuration", chapter "Loading software updates".
- Reboot the device for the new software to take effect.

Note: Hirschmann recommends checking for device software updates regularly and using the latest available release. A newer release of the device software could provide you with security improvements or benefits like new functions, including new security-related device functions.

2.6 Security configuration

The following description applies to:
- The initial security configuration for a device out-of-the-box
- Changes in the security configuration as part of operation or maintenance

Refer to the user manual "Configuration" for the functional device configuration.

Note: To configure the device, you need management access to the device, which requires at least a preliminary IP configuration. If the device does not yet have an IP configuration, Hirschmann recommends using HiView to assign an IP configuration to the device. HiView then offers you to open the device management.

The "Security Status" function in the device GUI can help you gain a first overview of the device security status. The "Security Status" function monitors the most essential security configuration settings. Depending on your needs, additional security configuration steps may be necessary even if the "Security Status" function reports *ok*.

To save time and effort, you can perform the following security configuration steps by loading a prepared configuration profile into the device.

At the first login with the default password, the device asks you to change the password. Use a dedicated password according to your password policy (see on page 19 “Plan a dedicated user account password policy”).

Overview and recommended sequence:

Perform the following steps as needed:
- Assign a static IP address for the device management.
- Configure a VLAN dedicated to management access.
- Disable HiDiscovery access.
- Disable logical access to unused ports and SFP slots.
- Disable logical access to the Signal Contact.
- Disable logical access to the Digital Input.
- Configure Power over Ethernet
- Disable booting from an external memory.
- Disable automatic software update from an external memory.
- Disable writing a configuration profile to an external memory.
- Disable loading a configuration profile from an external memory.
- Disable insecure management protocols.
- Enable IP access restrictions.
- Configure a dedicated HTTPS certificate.
- Configure a dedicated SSH host key pair.
- Configure a dedicated user account login policy.
- Configure a dedicated user account password policy.
- Configure dedicated user accounts.
- Remove user accounts with standard names.
- Adapt session timeouts.
- Configure the time synchronization.
- Configure logging.
- Configure dedicated login banners.

You can elect to configure the following advanced device security as needed (see on page 36 “Configure advanced device security”):
- Disable access to the System monitor 1 via V.24.
- Disable access to the CLI service shell.

You can also elect to configure the following advanced user authentication measures as needed (see on page 36 “Configure advanced user authentication”):

- Use 802.1X for user authentication.
- Use a dedicated authentication policy list.
- Configure RADIUS access instead of or in addition to the local IAS (Integrated Authentication Server).

When the device configuration is complete:

- Create a backup copy of the configuration.
- Include other device-related data like private keys.

2.6.1 Assign a static IP address for the device management

Note: At the first login with the default password, the device asks you to change the password. Use a dedicated password according to your password policy (see on page 19 “Plan a dedicated user account password policy”).

The device offers you the following options of assigning a management IP address: Local, DHCP (delivery state), and BOOTP.

Selecting the setting "Local" (that is: static) helps make the device more immune to potential attacks via the DHCP or BOOTP protocols.

2.6.2 Disable HiDiscovery access

The HiDiscovery protocol is enabled in the delivery state.

Setting the HiDiscovery protocol to `Off` helps make the device more immune to potential attacks via the HiDiscovery protocol.

2.6.3 Configure a VLAN dedicated to management access.

Note: Hirschmann assumes that, when reading this section, you have already performed the general and security-related configuration planning for the device (see on page 21 “VLAN plan considerations depending on redundancy protocols”).

The delivery state VLAN ID for management access is 1.

Configure a VLAN dedicated to management access only. This helps make the device more immune to potential attacks via the network. It may also help improve the reachability of the device management when there is heavy network traffic.

Note: If you use the redundancy protocols HIPER Ring or Ring/Network Coupling, use a VLAN ID ≥2 for management access. Else you are free to use any VLAN ID you like.

2.6.4 Disable logical access to the Signal Contact

If you do not need the Signal Contact, disable the Signal Contact in the device configuration. In the delivery state, the Signal Contact is disabled.

If you do need the Signal Contact (see on page 39 “Signal Contact considerations”).

2.6.5 Disable logical access to the Digital Input

If you do not need the Digital Input, disable the Digital Input in the device configuration. In the delivery state, the Digital Input is disabled.

If you do need the Digital Input (see on page 39 “Digital Input considerations”)

2.6.6 Disable logical access to unused ports and SFP slots

In the delivery state, all ports and SFP slots are enabled.

Disable network access for unused ports and empty SFP slots: See the user manual "Configuration", chapter "Configuring the ports". This helps prevent potential attacks that connect a rogue network device to an unused port.

Note: Treat inserted SFPs without a data cable the same way as unused ports.

2.6.7 Configure Power over Ethernet

Delivery state:
- The device-global setting `PoE Global Operation` is *`On`*.
- Port-related settings:
  - The setting `PoE Port Enable` is *`PoE enable`*.
  - The allowed classes ,*`Class 0`*..*`Class 4`*, are all enabled.
  - The `Power limit [W]` is `0.0` — the device will not enforce a specific power limit.
  - The power PoE `Priority` is *`low`*.

Device security aspects:
- If you do not need PoE or PoE+, disable PoE and PoE+ globally in the device.
- If you need PoE or PoE+:
  - Disable PoE or PoE+ on those ports that shall not deliver power.
  - For each port with PoE or PoE+ enabled, configure the minimal necessary reserved power according to the class (*`Class 0`*..*`Class 4`*) of the powered device (PD).
  - If you know the exact power consumption of a PD, additionally set the power limit for the given port to the known value.

Network availability aspects: Assign a PoE priority (*`critical`*, *`high`*, or *`low`*) to each PoE port. This helps delivering power to the most important PDs even if the power supply of the device is unable to deliver its nominal power, for example, if there is a failure.

Energy conservation aspects:

- If you set the power limit for a given port to the known power consumption of the PD, this may help in powering more PDs in certain cases.
- If you know the power consumption needs of a PD on a time-of-day or day-of-week basis, you can activate the *Auto-shutdown power* function and configure the associated values *Disable power at [hh:mm]* and *Re-enable power at [hh:mm]*. The prerequisite is that the device system clock is synchronized to a reliable, trustworthy source.

2.6.8 Disable booting from an external memory

Disable the booting from an external memory. This helps secure the device against rogue device software placed on an external memory and plugged into the device with the intention that the rogue device software will take effect after a reboot.

See the user manual "Configuration" on how to disable booting from an external memory.

2.6.9 Disable automatic device software update from an external memory

Disable the automatic device software update from an external memory. This helps secure the device against rogue device software placed on an external memory and plugged into the device with the intention that the rogue device software will be copied to the device and take effect after a reboot.

See the user manual "Configuration" on how to disable automatic device software update from an external memory.

2.6.10 Disable writing a configuration profile to an external memory

Disable the writing of a configuration profile to an external memory. This helps secure the device against leaking its configuration onto a rogue external memory plugged into the device.

See the user manual "Configuration" on how to disable writing a configuration profile to an external memory.

2.6.11 Disable loading a configuration profile from an external memory

Disable the loading of a configuration profile from an external memory. This helps secure the device against loading a rogue configuration profile placed on an external memory and plugged into the device with the intention that the rogue configuration profile will take effect after a reboot.

See the user manual "Configuration" on how to disable loading a configuration profile from an external memory.

2.6.12 Disable loading a configuration profile that lacks a valid fingerprint

Disable the loading of a configuration profile that lacks a valid fingerprint. This helps secure the device against loading an unsigned configuration profile placed on an external memory and plugged into the device with the intention that the unsigned configuration profile will take effect after a reboot.

See the user manual "Configuration" on how to disable loading an unsigned configuration profile from an external memory.

2.6.13 Disable insecure management protocols

Disable insecure management protocols:
- Disable SNMPv1 (delivery state: disabled).
- Disable SNMPv2 (delivery state: disabled).
- Disable Telnet (delivery state: disabled).
- Disable HTTP (delivery state: **enabled** (redirects to HTTPS)).

2.6.14 Configure management IP access restrictions

The device allows restricting the management access to the device to a source IP address range. You specify the address range by giving an IP address and a netmask.

You can configure the management access IP restrictions individually for each protocol or for a group of protocols.

Table 2: Management access protocol overview

Protocol	Recommendation for production	Delivery state
HTTP	Disabled	**Enabled** (redirects to HTTPS)
HTTPS	Enabled	Enabled
SNMPv1	Disabled	Disabled
SNMPv2	Disabled	Disabled
SNMPv3	Enabled	Enabled
Telnet	Disabled	Disabled
SSH	Enabled	Enabled
IEC 61850-MMS	Disabled	Disabled
Modbus TCP	Disabled	Disabled
EtherNet/IP	Disabled	Disabled
PROFINET	Disabled	Disabled

Note: Protocols with the delivery state **Enabled** (bolded) may be useful for the initial configuration of the device. However, they may be considered insecure for production. Disable these protocols as soon as you no longer need them.

Confirm that at least one of the configured management access IP restrictions is active. If no restriction is active, this leads to unrestricted management access for all enabled protocols.

Excluding a protocol from all management access IP restrictions while the protocol itself is enabled leads to unrestricted management access for the respective protocol.

2.6.15 Configure a dedicated HTTPS certificate

In the state of delivery, the device contains a self-signed HTTPS certificate.

You have the option of:
- Replacing the existing HTTPS certificate with a new, self-signed HTTPS certificate on the device
- Loading a dedicated HTTPS certificate onto the device

Note: When you create new, self-signed HTTPS certificate on the device, use the HTTPS certificate fingerprint algorithm *sha256* (delivery state: *sha256*).

If you have an established public key infrastructure (PKI), then loading a dedicated HTTPS certificate onto the device is generally considered more secure and also more convenient.

Choose the option that meets your needs. For details, refer to the user manual "Configuration", appendix chapter "HTTPS certificate".

2.6.16 Configure a dedicated SSH host key pair

In the state of delivery, the device contains a self-signed SSH host key pair.

You have the option of:
- Replacing the existing SSH host key pair with a new, self-signed SSH host key pair on the device
- Loading a dedicated SSH host key pair onto the device

Note: When you create a new, self-signed SSH host key pair on the device, use the SSH host key fingerprint algorithm *sha256* (delivery state: *sha256*).

If you have control over the entropy used for key generation, then loading a dedicated SSH host key onto the device is probably more secure.

If you have an established PKI, then loading an SSH host key signed by a Certification Authority onto the device is generally considered more secure and also more convenient.

Choose the option that meets your needs. For details, refer to the user manual "Configuration", appendix chapter "Preparing access via SSH".

2.6.17 Configure a dedicated user account login policy

Note: Hirschmann assumes that, when reading this section, you have already created a dedicated user account login policy (see on page 19 “Plan a dedicated user account login policy”).

The login policy applies to the following user interfaces and access protocols:
- The Command Line Interface (CLI) using SSH or Telnet
- The Graphical User Interface (GUI) using HTTPS or HTTP

Maximum number of failed user logins in a row: For security reasons, configure the value as low as possible. For availability reasons, configure it as high as practical. practical. Use a value >0. Chose a value that corresponds to your situation.

Waiting time before the device auto-unlocks a locked user account: For security reasons, configure the value as high as possible. For availability reasons, configure it as low as practical. Use a value >0. Chose a value that corresponds to your situation.

These steps helps ensure that the device will lock out a user after the maximum number of failed user logins in a row and then enforces a waiting period.

Configure a dedicated user account login policy as needed:
- Configure a maximum number of failed user logins in a row until the device locks the respective user account (**delivery state: 0 (no limit)**).
- Configure a waiting time (Login attempts period in minutes) before the device auto-unlocks a locked user account (**delivery state: 0 (no waiting time)**).

Note: Access to the CLI using the serial connection is exempt from the login policy. Users accessing the CLI using the serial connection have an unlimited number of login attempts. They are also not required to wait for the next login attempt, that is, the Login attempts period does not apply. This ensures access to the device management in situations where availability may be critical, and for users who already have physical access to the device.

2.6.18 Configure a dedicated user account password policy

Note: Hirschmann assumes that, when reading this section, you have already created a dedicated user account password policy (see on page 19 “Plan a dedicated user account password policy”).

Configure a dedicated user account password policy as needed:
- Minimum required number of uppercase characters (delivery state: 1)
- Minimum required number of lowercase characters (delivery state: 1)
- Minimum required number of digits in a password (delivery state: 1)
- Minimum required number of special characters (delivery state: 1)

Note: To deter attackers, consider using different passwords on different devices, even for user accounts with the same name.

2.6.19 Configure dedicated user account names and access roles for device management

Note: Hirschmann assumes that, when reading this section, you have already created a dedicated user account name and access role policy (see on page 20 “Plan a dedicated user account name and access role policy for device management”).

Hirschmann also assumes that you have created a dedicated policy for SNMPv3 authentication and encryption types, and for the related passwords.

For details on the privileges of the individual access roles, see the user manual "Configuration", chapter "Access roles".

Configure dedicated user accounts as needed:
- Assign the device login policy.
- Assign the device password policy.

- Create user accounts. For each new user account, perform the following steps:
  - Create a user account with a dedicated name.
  - Assign the new user account an access role that offers only the least necessary privileges.
  - Assign the new user account a strong, individual password.
  - Apply the password policy check to the new user account.
- For each new user account, configure a SNMPv3 policy as needed:
  - Set the SNMPv3 authentication type to `hmacsha` (delivery state: `hmacmd5`).
  - Set a SNMPv3 authentication password according to your policy.
  - Set the SNMPv3 encryption type to `aesCfb128` (delivery state: `des`).
  - Set a SNMPv3 encryption password according to your policy.
- Remove user accounts with standard names.

Note: To deter attackers, consider using different user account names and different passwords on different devices.

Also consider using different SNMPv3 passwords on different devices.

2.6.20 Adapt session timeouts

Adapt session timeouts for the:
- Graphical User Interface using HTTPS or HTTP
- Command Line Interface using SSH
- Command Line Interface using Telnet
- Command Line Interface using the serial connection

Note: Configure the session timeouts as short as possible and as long as practical. Set each timeout to a value >0. This helps ensure that the device terminates the respective session automatically when idle.

2.6.21 Configure time synchronization

The protocols NTP and PTP implicitly trust the time source. Configure the network time synchronization protocol according to the requirements from the overarching network time synchronization policy (see on page 21 “Network time synchronization considerations”).

To receive time information from an upstream time server, the device has the role of a time synchronization client. To redistribute the time information to other devices, the device has the role of a time synchronization server. Thus, the client role is normally required, e.g., for synchronizing the device system clock while the necessity of the server role depends on your network.

Parameters to be configured may include:
- Enable only the client functions for the network protocols allowed by the policy.
- Configure only trusted next-hop upstream time servers.
- Tune the client functions of the chosen network time protocol on the device.
- Enable the server functions of the device only if necessary.
- Tune the server functions of the chosen network time protocol on the device.

2.6.22 Configure logging

Configure logging:

- Configure synchronization of the device system clock to a trusted source.
  See the user manual "Configuration" on how to synchronize the device system clock to a trusted source. If you use PTP (IEEE 1588), refer to the PTP chapters.
- Configure logging severity levels.
  The necessary settings depend on our security requirements. See the user manual "Configuration" on how to configure logging severity levels.
- Configure logging destinations:
  - The necessary settings depend on our security requirements. See the user manual "Configuration" on how to configure logging destinations.
  - For log availability reasons, a remote destination, different from the location of the device, may be preferable.
  - For log confidentiality reasons, an appropriately secured remote destination may be preferable.

Note: The audit trail function is always active and cannot be disabled. Neither can the audit trail be deleted by resetting the device to the delivery state.

2.6.23 Configure dedicated login banners

Configure dedicated login banners:

- Configure the GUI pre-login banner with only the minimal information necessary. If possible, avoid any information that may help an attacker.
- Configure the CLI pre-login banner with only the minimal information necessary. If possible, avoid any information that may help an attacker.
- Configure the CLI post-login banner with only the minimal information necessary.

2.6.24 Configure advanced device security

You can elect to configure the following advanced device security:

- Disable access to the CLI service shell.
  See the user manual "Configuration", chapter "User Interfaces" on how to disable access to the CLI service shell

2.6.25 Configure advanced user authentication

You can also elect to configure the following advanced user authentication measures as needed:

- Use 802.1X for user authentication.
  See the user manual "Graphical User Interface" on how to configure 802.1X port security.
- Use a dedicated authentication policy list
  See the user manual "Graphical User Interface" on how to configure authentication policy of the local IAS (Integrated Authentication Server).
- Configure LDAP or RADIUS access instead of or in addition to the local IAS.
  See the user manual "Graphical User Interface" on how to configure the authentication policy of the device.

2.6.26 Create a backup of device-specific data

When the device configuration is complete:

- Consider creating a backup copy of the configuration. For example, place the backup file in a device-specific folder.
- Include other device-specific data. For example, copy device-specific private keys or certificates to the same device-specific folder.
- Keep the backup files separate from the device in a secure location.

This minimizes your effort to replace a device should the hardware become inoperable.

2.7 Possible hardware modifications for security

The following descriptions apply to:
- The possible hardware modifications for a device out-of-the-box
- Possible hardware modifications as part of operation or maintenance

Perform the following hardware modification steps, like covering or obstructing a slot or a port, as needed:
- Restrict physical access to the USB port.
- Restrict physical access to network ports or SFP slots.
- Restrict physical (visual) access to the device and port LEDs.
- Restrict physical access to the Signal Contact.
- Restrict physical access to the Digital Input.

2.7.1 Restrict physical access to the USB port

If you have high security requirements and you are sure you will not need the USB port after commissioning, consider covering or obstructing the USB port.

2.7.2 Restrict physical access to network ports or SFP slots

If you have high security requirements and you are sure you will not need certain network ports or SFP slots after commissioning, consider covering or obstructing these network ports and SFP slots.

2.7.3 Restrict physical (visual) access to the device and port LEDs

If you have high security requirements, perform the following steps as needed:
- Install the device in a cabinet with an opaque door.
- Cover or obstruct the LEDs with a removable cover.

2.7.4 Restrict physical access to the Signal Contact

If you do not need the Signal Contact and have high security requirements, consider covering or obstructing the Signal Contact terminals.

If you use the Signal Contact (see on page 39 “Signal Contact considerations”).

2.7.5 Restrict physical access to the Digital Input

If you do not need the Digital Input and have high security requirements, consider covering or obstructing the Digital Input terminals.

If you use the Digital Input (see on page 39 “Digital Input considerations”).

2.8 Device installation

The following description applies to:
- The installation of a device in a new system
- Changes to the device as part of operation or maintenance

Perform the device installation according to the user manual "Installation" for the device.

2.8.1 Data connections

Perform the data connections according to the user manual "Installation" for the device. If you have high device availability requirements, use redundant data uplinks.

2.8.2 Signal Contact considerations

If you use the Signal Contact, consider the following security and safety aspects:
- **To help protect the device**, connect the Signal Contact only to a circuit that meets the device requirements. For details, see the user manual "Installation".
- **To help protect your system**, connect the Signal Contact only to circuits that do not have explicit security or safety requirements. This means:
  - The circuit controlled by the Signal Contact does not have any security or safety function.
  - The controlled circuit does not rely on the secure or safe operation of the Signal Contact.

2.8.3 Digital Input considerations

If you use the Digital Input, consider the following security and safety aspects:
- **To help protect the device**, connect the Digital Input only to a circuit that meets the device requirements. For details, see the user manual "Installation".
- **To help protect your system**, connect the Digital Input only to circuits that do not have explicit security or safety requirements. This means:
  - The circuit that controls the Digital Input does not have any security or safety function.
  - The controlling circuit does not rely on the secure or safe operation of the Digital Input.

2.9 Operation

In the operation phase of the device, Hirschmann assumes you have already taken the appropriate physical and logical steps to set up the device and operate it properly regarding the functional and security aspects of the device. This essentially reduces the required security steps during the operation phase to the considerations already described in this security manual, the user manual "Installation" and the user manuals "Configuration", "Graphical User Interface" and "Command Line Interface".

The most essential parts are repeated below.

2.9.1 Environmental conditions

Obey the environmental conditions given in the user manual "Installation".

Do not open the device.

2.9.2 Connectivity

Obey instructions for connecting the Signal Contact.

Obey instructions for connecting the Digital Input.

Obey instructions for connecting the Ethernet ports.

2.10 Maintenance

2.10.1 Software update

If necessary, perform a software update:
- For the security aspects (see on page 27 “Software update”).
- For the detailed worksteps, see the user manual "Configuration", chapter "Loading software updates".

2.10.2 Hardware enhancement

Typical application cases include:
- Connecting a new end device to an existing Ethernet port
- Connecting a new PoE- or PoE+-powered end device to an existing Ethernet port
- Replacing a PoE- or PoE+-powered end device at an existing Ethernet port
- Switching PoE or PoE+ power on or off for an existing end device
- Modifying the PoE or PoE+ parameters for an existing end device

Use redundant power supplies.

Plan power supply for worst case device power budget, even in case one of the redundant power supplies fails.

Configure PoE or PoE+ power budget. Take the worst case PoE or PoE+ power budget into account.

Provide redundant data uplinks.

2.10.3 Hardware replacement

Note: Do not open the device.

Perform the following steps:
- Perform an initial software update (see on page 27 “Software update”).
- Perform the software configuration, for example, by transferring the existing configuration of the old device to the new device (see on page 28 “Security configuration”).

2.10.4 Hardware repair

Should your device need repair, consider the following recommendations:
- Do not open the device.
- Send the device to the manufacturer for repair.
- Keep a backup copy of the device configuration (see on page 37 “Create a backup of device-specific data”).
- If necessary and possible, delete the configuration and other data you consider confidential (see on page 42 “Destruction of confidential data and secrets”).

2.11 Decommissioning

If you have high security requirements, consider physical destruction (see on page 42 “Secure physical destruction of device and components”). Secure physical destruction addresses the possible reading-out of memory blocks from the flash memory and makes deletion and wiping (see on page 42 “Destruction of confidential data and secrets”) redundant.

Note: If you plan to continue using the device, consider leaving the device and its software intact and deleting or wiping only the data on the device and on the external memory.

2.11.1 Destruction of confidential data and secrets

Note: Resetting the device to the delivery state performs normal file deletion operations on the device and the external memory which may leave some of the file contents or blocks in the flash memory intact. Also, the audit trail persists after a reset to the delivery state.

If you have high security requirements, consider the physical destruction of the device and the external memory.

Reset to the delivery state

For the deletion of data, perform the following steps as needed:

- Reset the device to the delivery state. This performs the following operations:
  - Deletes the current HTTPS certificate in the device and creates a new, self-signed HTTPS certificate.
  - Deletes the current SSH host key pair in the device and creates a new, self-signed SSH host key pair.
  - Deletes the configuration profiles and configuration scripts in the device.
  - Resets the boot parameters.
  - If the external memory is plugged in, the device deletes configuration profiles on the external memory.
- If necessary, manually delete the configuration profiles on the external memory and/or any other files on it.

Note: The audit trail persists after a reset to the delivery state.

2.11.2 Secure physical destruction of device and components

For the secure physical destruction of physical components, perform the following steps as needed:

- Physically destroy the external memory. This addresses:
  - The configuration profiles on the external memory
  - The software files on the external memory
  - Any other files on the external memory
- Physically destroy the device, including the flash memory chips. This addresses:
  - The HTTPS certificate in the device
  - The SSH host key pair in the device
  - The configuration profiles in the device
  - Any other files in the device

3 Network security support

This chapter lists what the device can do for the security of your network, including enhancing the availability of your network. The chapter deals with **device functionality** in the operation and maintenance lifecycle phases that can affect the security of your network. The prerequisite is that you have secured the device itself (see on page 23 “Device security”).

For the general device functions, refer to the detailed manuals.

3.1 Introduction

Aside from the basic task of transmitting data packets in your network, the device also can help you:

- Employ defense in depth for your network infrastructure
- Harden your network infrastructure
- Enhance and maintain the availability of your network infrastructure

3.2 Prerequisites for setting up network security

A securely configured device can help you make your network more secure and available. Hirschmann assumes that, when reading this section, you have taken the necessary steps to securing the device itself (see on page 23 “Device security”).

3.3 Employ defense in depth for your network infrastructure

Defense in creates uses several barriers that a potential attacker has to overcome one after the other. Hirschmann assumes that, when reading this section, you have already set up a dedicated plan for defending your system in depth (see on page 15 “Defense in depth”).

From a system view, there are 2 aspects how defense in depth is realized — that is, how they translate into specific device setups:

- Measures to secure the device itself, and in turn to secure the network. These measures are described in the chapter "Device security" (see on page 28 “Security configuration”).
- Measures to secure the network by using specific device functions. These measures are described in the remainder of this main chapter.

The suggested measures for defense in depth are collected in the chapter (see on page 47 “Measures to secure the network infrastructure”). Pick the measures suitable for defense in depth first. Then complement them by selecting from the remaining hardening possibilities.

3.4 Hardening the network infrastructure

The suggested hardening measures are collected in the chapter (see on page 47 “Measures to secure the network infrastructure”). Pick the measures suitable for defense in depth first. Then complement them by selecting from the remaining hardening possibilities.

3.5 Measures to secure the network infrastructure

The collection of suggested measures can be used for hardening and for defense in depth. Pick the measures suitable for defense in depth first. Then complement them by selecting from the remaining hardening possibilities.

To help you secure your network infrastructure, perform the following steps on the respective devices as needed:

- Restrict logical access to your network (see on page 48 “Restrict logical access to your network”):
  - Configure a dedicated management VLAN. If you use certain redundancy protocols, use only VLAN IDs ≥2 for payload traffic and device management (see on page 21 “VLAN plan considerations depending on redundancy protocols”).
  - Configure VLAN segregation
  - Disable GVRP and MVRP
  - Configure Port Security
  - Configure ACLs
- Secure the network protocols used (see on page 49 “Secure the network protocols used”):
  - Disable GMRP and MMRP
- Secure the redundancy protocols used (see on page 50 “Secure the redundancy protocols used”):
  - Configure RSTP guards and helper protocols
  - Configure MRP (MRP VLAN ID ≥2, tagged packets)
  - Configure HIPER Ring (VLAN ID 1: tagged packets)
  - Configure Ring/Network Coupling (VLAN ID 1: tagged packets)
- Configure attack protection functions
  - Configure Denial of Service (DoS) protection (see on page 51 “Configure Denial of Service (DoS) protection”)
  - Configure rate limiters (see on page 51 “Configure rate limiters”)
- Configure network time synchronization (see on page 52 “Configure network time synchronization”)
- Configure logging (see on page 53 “Configure logging”)

Note: Securing the redundancy protocols used can also help you enhance and maintain the availability of your network infrastructure.

Routing protocols like HiVVRP, VRRP, OSPF or RIP are outside the scope of this document.

3.6 Restrict logical access to your network

3.6.1 Configure a dedicated management VLAN

If you have already set up a dedicated management VLAN, you can skip this chapter. Else follow the description (see on page 29 “Configure a VLAN dedicated to management access.”).

Note: If you use certain redundancy protocols, use only VLAN IDs ≥2 for payload traffic and device management (see on page 21 “VLAN plan considerations depending on redundancy protocols”).

3.6.2 Configure VLAN segregation

Prerequisite for setting up VLANs in the device is that you have created a VLAN plan for your network (see on page 17 “VLAN plan”).

For details on how to configure VLANs, see the reference manual "Graphical User Interface" and the user manual "Configuration".

Note: If you use certain redundancy protocols, use only VLAN IDs ≥2 for payload traffic and device management (see on page 21 “VLAN plan considerations depending on redundancy protocols”).

3.6.3 Disable GVRP and MVRP

The GARP VLAN Registration Protocol (GVRP) and its successor, the Multiple VLAN Registration Protocol (MVRP) can be used to dynamically set up VLANs in a device. This also creates a potential attack surface.

It is generally considered more secure to disable GVRP and MVRP. In the delivery state, GVRP and MVRP are both globally disabled on the device.

3.6.4 Configure Port Security

Port Security is a concept to restrict which frames the network device accepts on a specific port. Port Security distinguishes frames by their MAC source address. This restriction typically translates to which source device the network device accepts on the port. The device drops frames with a disallowed MAC source address. This can be helpful in securing your network.

To configure Port Security, create a list of allowed MAC source addresses. If the device receives a frame with a MAC source address that is not on the allow list, the device can take a configurable action like sending an SNMP trap to the network management station and/or disable the port.

For details, refer to the reference manual "Graphical User Interface", chapter "Port Security".

3.6.5 Configure ACLs

Configure ACLs

3.7 Secure the network protocols used

3.7.1 Disable GMRP and MMRP

The GARP Multicast Registration Protocol (GMRP) and its successor, the Multiple MAC Registration Protocol (MMRP) can be used to register group MAC addresses dynamically and automatically setup multicast forwarding in a device. This also creates a potential attack surface.

It is generally considered more secure to disable GMRP and MMRP. In the delivery state, GMRP and MMRP are both globally disabled on the device.

3.8 Secure the redundancy protocols used

Note: Securing the redundancy protocols used can also help you enhance and maintain the availability of your network infrastructure.

3.8.1 Secure RSTP guards and helper protocols

Secure RSTP guards. See the user manual "Graphical User Interface" on how to configure RSTP guards.

Secure RSTP helper protocols:

- Consider disabling the L2 loop protection. This helps protecting against a Denial-of-Service attack if malicious loop protection frames are sent to the device with the intention to trick it into disabling its respective port.

Note: The delivery state for the L2 loop protection is disabled.

3.8.2 Secure MRP

Secure MRP (MRP VLAN ID ≥2, tagged packets). This may require an existing VLAN plan.

See the user manual "Graphical User Interface" on how to configure MRP.

3.8.3 Secure HIPER Ring

Secure HIPER Ring (VLAN ID 1: tagged packets). This may require an existing VLAN plan with a device management VLAN ID ≥2.

See the user manual "Graphical User Interface" on how to configure the HIPER Ring and VLANs.

3.8.4 Secure Ring/Network Coupling

Secure Ring/Network Coupling (VLAN ID 1: tagged packets) This may require an existing VLAN plan with a device management VLAN ID ≥2.

See the user manual "Graphical User Interface" on how to configure Ring/Network Coupling and VLANs.

3.9 Configure attack protection functions

3.9.1 Configure Denial of Service (DoS) protection

Configure DoS protection. See the user manual "Graphical User Interface" on how to configure DoS protection.

3.9.2 Configure rate limiters

Configure rate limiters. See the user manual "Graphical User Interface" on how to configure rate limiters.

3.10 Configure network time synchronization

Hirschmann assumes that, when reading this section, you have taken the necessary steps to securing the device itself (see on page 35 “Configure time synchronization”).

To help synchronize the time in the network, the device may act as a time server.

Configure the server function of the device. Parameters to be configured may include:
- Enable the server function of the device only if necessary.
- Enable only the servers for the network protocols allowed by the policy.
- Tune the server functions of the chosen network time protocol on the device.

3.11 Configure logging

Configure logging severity levels and destinations.

The necessary settings depend on our security requirements. See the user manual "Configuration" on how to configure logging severity levels and destinations.

Note: Secure logging also relies on the synchronization of the device system clock to a trustworthy source (see on page 35 “Configure time synchronization”).

The audit trail function is always active and cannot be disabled. Neither can the audit trail be deleted by resetting the device to the delivery state.

3.11.1 Configure an audit trail

Note: The audit trail function is always active and cannot be disabled. Neither can the audit trail be deleted by resetting the device to the delivery state.

A Index

C

D

E

F

N

O

P

R

S

T

U

V

W

B Further support

Technical questions

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

You find the addresses of our partners on the Internet at www.hirschmann.com.

A list of local telephone numbers and email addresses for technical support directly from Hirschmann is available at hirschmann-support.belden.com. This site also includes a free of charge knowledge base and a software download section.

Technical Documents

The current manuals and operating instructions for Hirschmann products are available at doc.hirschmann.com.

Customer Innovation Center

The Customer Innovation Center is ahead of its competitors on three counts with its complete range of innovative services:

- 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.
  You find the training courses on technology and products currently available at www.belden.com/solutions/customer-innovation-center.
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Customer Innovation Center, you decide against any compromise in any case. Our client-customized package leaves you free to choose the service components you want to use.

C Readers' Comments

What is your opinion of this manual? We are constantly striving to provide as comprehensive a description of our product as possible, as well as important information to assist you in the operation of this product. 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
Comprehensive	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?

Suggestions for improvement and additional information:

General comments:

Sender:

Company / Department:

Name / Telephone number:

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

HIRSCHMANN

A BELDEN BRAND