cyber-diode

Installation and Configuration
Manual

Version 2.5

Edition September 15, 2023

Revision: fa282a79

This product contains software based on the OpenBSD operating system.

genua GmbH
Domagkstrasse 7
85551 Kirchheim/Munich
Tel.: +49 89-991950-0
Fax : +49 89-991950-999

Please note that in accordance with current legal requirements, all owners of waste electrical and electronic equipment (WEEE) may not dispose of WEEE together with unsorted municipial waste. In addition, the following icon of a crossed out trash bin depicted on WEEE devices denotes the requirement to collect and dispose of all WEEE arising separately:

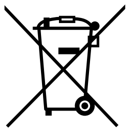


Figure 1: Do not dispose of with municipial waste

You as the end user bear the sole responsibility for deletion of all personal information from WEEE devices before their disposal.

For disposal of WEEE devices, please contact genua as the manufacturer at +49 89-991950-0 with the reference “waste electrical and electronic devices”.

With kind regards,

genua GmbH

Contents

Chapter 1

Basics

Functionality of the cyber-diode

The highly secure cyber-diode is a security appliance that enables one-way data communication.

The two networks connected by the cyber-diode are referred to as the “black network” and the “red network” below. The cyber-diode only allows data to travel from the black network to the red network.

The data packets of a client on the black network are received by the cyber-diode, sent to the red side, and then transmitted to a server connected to the red network.

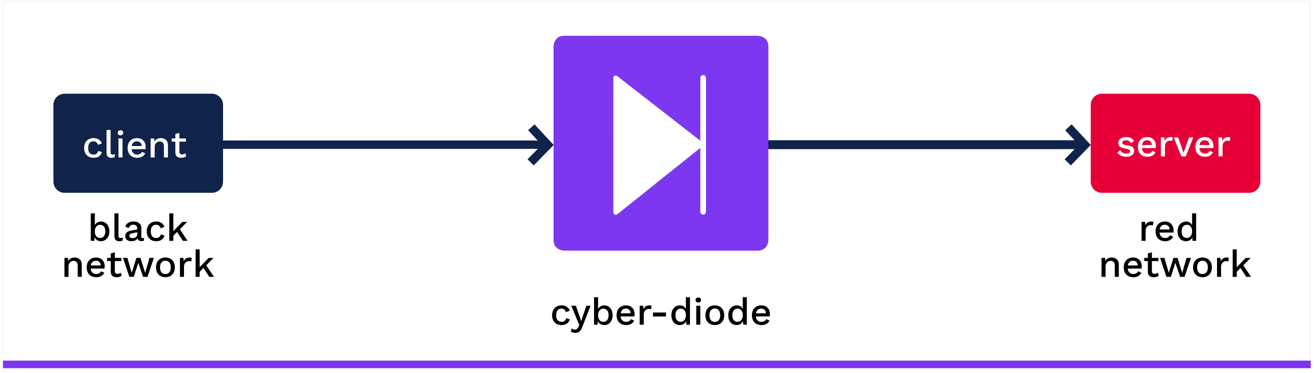


Figure 1.1: Schematic of a cyber-diode

Modes: Proxy and Transparent

Two *modes* are available for the supported protocols TCP, UDP, SMTP, and FTP/FTPS (FTP with SSL/TLS):

- Proxy mode
  The *cyber-diode* operates as a normal proxy in this mode: In proxy mode, the client connects to the black IP address of the cyber-diode. The cyber-diode forwards the connection to an IP address defined in advance by the admin. A new connection to the target system is established in the process, i.e., in the transmitted data, the client’s original source IP address is replaced with the IP address for the red interface of the cyber-diode.
- Transparent mode
  In transparent mode, the client establishes a connection to the server’s IP address on the red network. The cyber-diode forwards the connection transparently like a router, i.e., the source and target IP addresses are not changed.

Please note that the routing in the client and server networks must be configured to forward the data packets via the cyber-diode. To do this, configure the corresponding routes or set the cyber-diode as the default gateway.

Recommendation:
Proxy mode can be used, for example, when networks are initially set up or the IP addresses

of the networks were not previously known reciprocally (connecting previously disconnected networks). Another application of this mode is when the red network is the Internet and private IP addresses (in accordance with RFC1918) are used on the black network.

Transparent mode is used when existing networks (of both the client and server) cannot or should not be reconfigured. The cyber-diode is simply integrated as a new component between the networks. Transparent mode requires that the black IP addresses are known in the red network and vice versa.

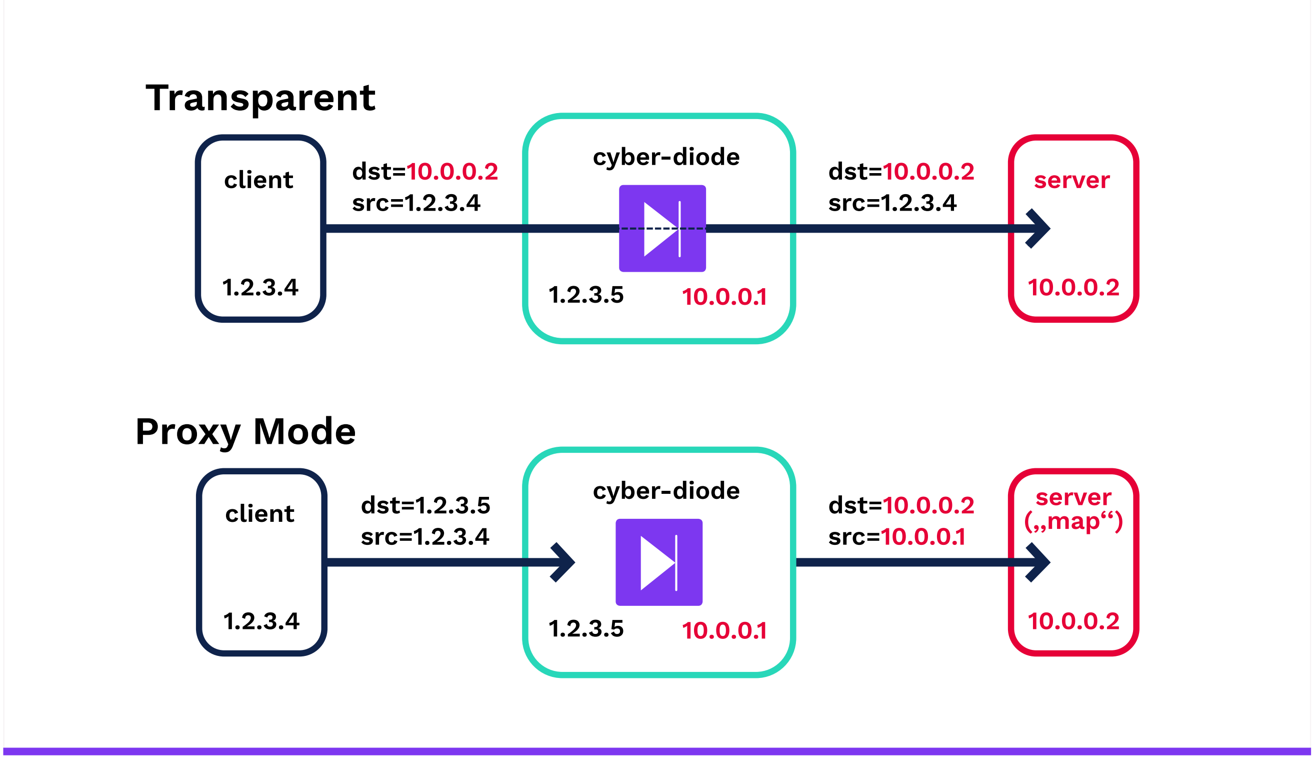


Figure 1.2: Proxy Mode and Transparent Mode

The OPC UA Relay

The OPC UA relay consists of an OPC UA client on the black side of the cyber-diode and an OPC UA server on the red side of the cyber-diode.
The OPC UA client receives data from OPC UA servers out of the black network and forwards them via a one way relay to the OPC UA server on the red side.
The OPC UA server on the red side provides data for OPC UA clients in the red network. The OPC UA clients within the red network access the data from the OPC UA server of the cyber-diode.
The one way relay prevents data from flowing from the red network to the black network.

Chapter 2

Setting Up the Hardware

2.1 cyber-diode Hardware Revision 3

2.1.1 Scope of Delivery

Scope of delivery for the cyber-diode:

- **cyber-diode Hardware Revision 3**
- Phoenix Contact Combicon 3-pin Connector
- DIN rail bracket (pre-installed)
- USB flash drive for configuration updates
  (We recommend using the provided USB flash drive for configuration updates.)
- Installation and Configuration Manual

Please contact your sales partner if anything is missing.

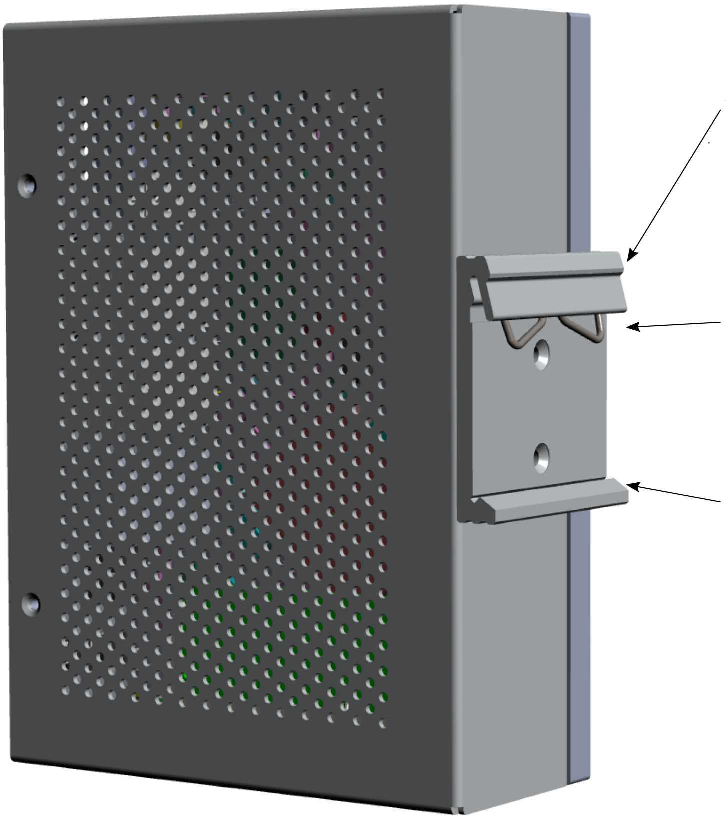
2.1.2 Connecting the Cables and First Boot

The *cyber-diode* is an appliance with two USB interfaces and three network interfaces (1 x red, 1 x black, 1 x not assigned) on its front side. Both USB interfaces support configuration updates via the USB flash drive. The USB flash drive can be connected to either of these interfaces. There are also two status LEDs on the front of the appliance. These LEDs indicate the appliance's operating state.

! **Danger!** Please note that only qualified and trained personnel may install and use cyber-diode hardware. There may be additional requirements for installation and usage of the cyber-diode hardware depending on the operational environment. See section A.3 for mor details.

Mounting on DIN rails

The cyber-diode hardware can be mounted on a DIN rail (also known a cap rail or top hat rail outside of Europe). The DIN rail clamp of the cyber-diode hardware already is assembled on delivery. Refer to the following picture to mount the device on DIN rails:



1. When mounting the hardware on the rail, the rail clamp side with the spring must be on top.
2. Insert the clamp into the rail from above.
3. Then press the lower part of the cyber-diode hardware to the rail until the rail clamp catches in the rail.

Figure 2.1: Cyber-diode hardware montage

Connecting the Cables

Connect the networks to the correct diode interfaces. The network interfaces on the front of the appliance are labeled with **ETH2 (red)** and **ETH3 (black)** (the two interfaces to the right). See figure 2.2.

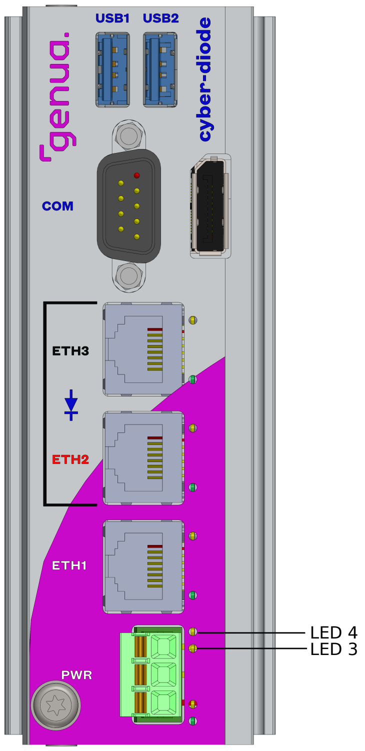


Figure 2.2: cyber-diode hardware

Note: Please use ETH2 and ETH3! ETH1 is not supported.

- **Black**
  Patch the client network to the interface with the black "**ETH3**" label.
- **Red**
  Patch the server network to the interface with the red "**ETH2**" label.

Switching On and Booting

Connect the power cable to a Phoenix Contact Combicon 3 pin connector and then connect the connector to the interface on the front of the appliance. The cyber-diode requires a 24V DC power supply. The sticker on the side of case illustrates how to connect the power supply.
If the connector is wired correctly, the appliance will power up automatically, once supplied with power.
After switching on the cyber-diode, it will boot automatically and operate using the standard configuration.

2.1.3 Standard Configuration

For the standard configuration of the cyber-diode, see Chapter 3.
Consult Chapter 4 to discover how to customize the configuration to your individual needs.

2.1.4 BIOS Settings

When initially setting up the cyber-diode, we recommend making some changes to BIOS (system firmware).

2.1.5 Access

1. To start with, attach either a serial console or a USB keyboard and screen via Display Port.

2. Power on the system and wait for the following mesage:

```
Press <DEL> or <ESC> to enter setup
```

3. Follow the instructions and press either DEL to access the BIOS menu.

4. The BIOS menu is displayed. Use the arrow keys to navigate to the desired menu.

2.1.6 BIOS Password

! **Warning!** For security reasons, we strongly recommend setting a BIOS password immediately after receiving the cyber-diode.

Any following access to the BIOS will require this password. This reduces the risk of unauthorized logins to the system, even if physical access is possible.

After accessing the BIOS, use the arrow keys to navigate to the top level menu “Security” and enter a password in the field “Setup Administrator Password” (3-20 characters).

After setting this password, the system still will reboot normally - only access to the BIOS is restricted.

! **Warning!** Do not under any circumstances set a password in the **“User Password”** field!
This password would prevent the cyber-diode from automatically fully booting at system restart. Instead, entering the password would be required to boot. This is not recommended, as it can seriously disrupt functionality.

2.1.7 System Time

If you intend to use logging and modify the configuration to do so (see Chapter 4), the system time needs to be correctly set in the BIOS. In most cases, this should be set in the UTC timezone.

After accessing the BIOS, use the arrow keys to navigate to the top level menu “Main” and set the time in the field “System Date”. Use the + / - to change the values as well as the Enter key to switch between MM/TT/JJJJ.
The time is entered similarly via the “System Time” line.

2.1.8 Save the BIOS settings

If you want to apply your changes, save and exit the BIOS using F4 “Save Configuration & Exit”.

Otherwise, you can exit the BIOS with ESC. Confirm the dialog with “YES” by pressing Enter.

Chapter 3

Standard Configuration Upon Delivery

3.1 Standard Configuration of the cyber-diode

The current software and the standard configuration are already installed on the cyber-diode upon delivery. As long as you can customize your end systems (client and server) to work with this standard configuration, you do not need to configure the cyber-diode.
If you would like to use the OPC UA relay you have to configure your cyber-diode. If this is not possible, consult Chapter 4.

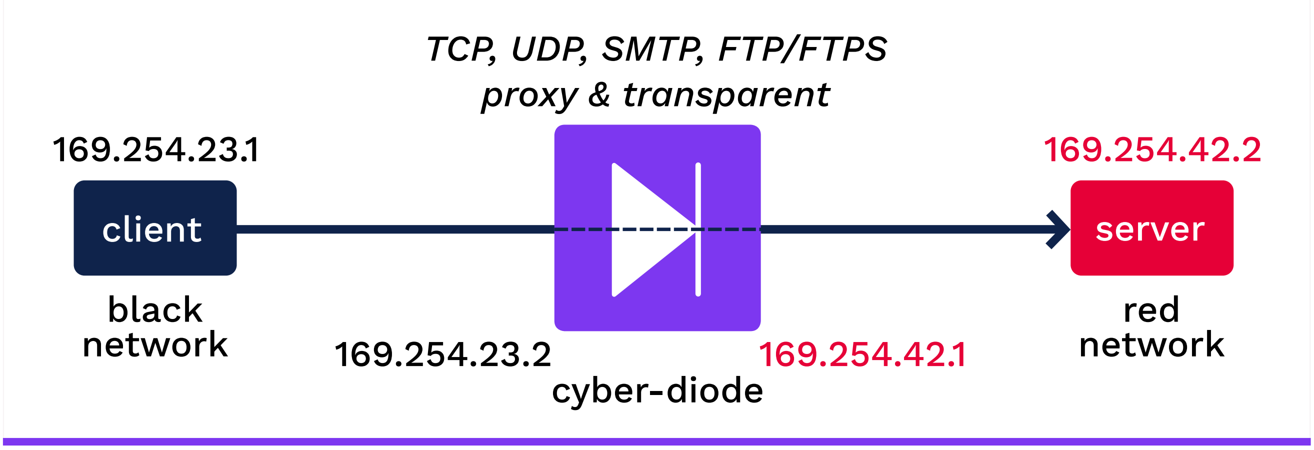


Figure 3.1: Standard Configuration of the *cyber-diode*

3.1.1 IP Addresses

Both interfaces are preconfigured with fixed link local IPv4 addresses that are not routed on the Internet.

- **Input interface**
  (Black interface, receives data from the client): **169.254.23.2/24**
- **Output interface**
  (Red interface, forwards data to the server): **169.254.42.1/24**

3.1.2 Connection Types: Transmitted Protocols

The following protocols and modes are configured on the cyber-diode by default:

- **TCP**: All ports (proxy and transparent)
- **UDP**: All ports (proxy and transparent)
- **SMTP**: Port 25 (proxy and transparent)
- **FTP/FTPS (FTP with SSL/TLS)**: Ports 20 and 21 (proxy and transparent)

! **Attention!** Only the **red / output** side of the cyber-diode is encrypted via FTPS. Data on the black / input side is **not** encrypted.

Data is accepted from any source IP address.

3.2 Configuring the Connected Systems

Since the cyber-diode is delivered to you preconfigured, the end systems to which the cyber-diode will be connected must be configured in the following manner:

- **Client IP**
  In the client network, the IP address for the client (or the router for this network) is configured to **169.254.23.1/24**. This makes the black interface of the cyber-diode reachable (with the IP address 169.254.23.2/24).
- **Client route and gateway**
  If transparent mode is going to be used, a route for the target network must be configured in the client network. This route points to the gateway with the IP address 169.254.23.2.
- **Server IP**
  In the server network, the IP address for the server (or the router for this network) is configured to **169.254.42.2/24**. This makes the red interface of the cyber-diode reachable (with the IP address 169.254.42.1/24).
- **Server route and gateway**
  If transparent mode is going to be used, a route pointing to the gateway with the IP address 169.254.42.1 must be configured in the server network. This makes it possible for the minimal response to reach the client.

Chapter 4

Custom Configuration

You can customize the standard configuration of the **cyber-diode** – the state in which you found it upon delivery – to suit your operating environment. The IP addresses can be configured, as can the forwarded protocols and modes used.

To do this, a separate genua appliance or piece of software must be used to create a new configuration and write this configuration to a USB flash drive.

You can customize the configuration in the following ways:

- **Using the genucenter Management Station**

  A new configuration can be created on a genucenter appliance or a virtual genucenter installation. New releases of the diode software are also available there. They can be installed using a USB flash drive.

  For more information on this, see Chapter 4.2

  The software for the virtual genucenter can be purchased separately or together with the *cyber-diode*.

- **Using the online configurator**

  If the only items in the standard configuration that you want to customize are the IP addresses or the OPC UA relay, you can use the online configurator. The online configurator can be used to create a configuration that you can download directly from there.

  For more information on this, see Chapter 4.1.

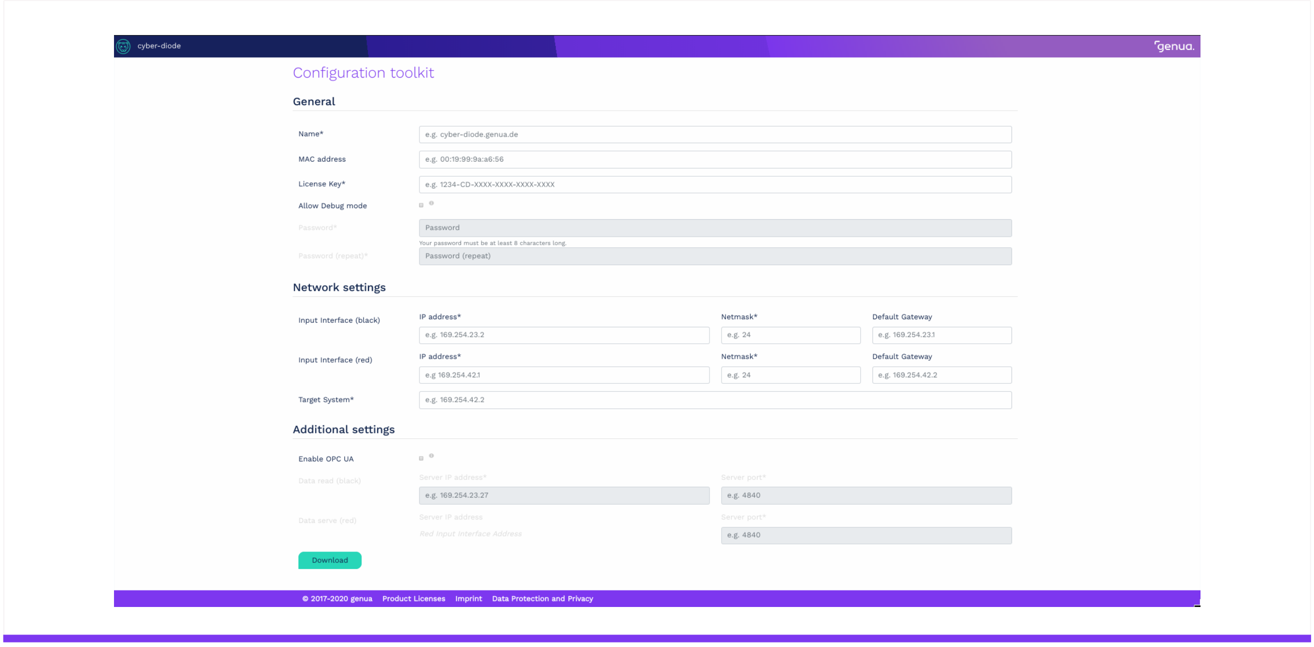
- **As a service provided by genua**

  Upon request, genua can also configure the cyber-diode for you on-site or create a configuration file for you that you then simply have to apply.
  Contact genua for an offer on these or other individual services such as a support agreement. To be able to use IPSec service an offer for provided services is required from genua.

4.1 Creating a Configuration Using the Online Configurator

genua provides a web-based form that you can use to prepare a configuration for your cyber-diode yourself, and download it as a file.

The online configurator is available at the following URL:
https://support.genua.de/cyber-diode/config/



Configuration toolkit

General

Name* e.g. cyber-diode.genua.de

MAC address e.g. 00:19:99:9a:a6:56

License Key* e.g. 1234-CD-XXXX-XXXX-XXXX-XXXX

Allow Debug mode □

Password* Password

Your password must be at least 8 characters long.

Password (repeat)* Password (repeat)

Network settings

	IP address*	Netmask*	Default Gateway
Input Interface (black)	e.g. 169.254.23.2	e.g. 24	e.g. 169.254.23.1
Input Interface (red)	e.g 169.254.42.1	e.g. 24	e.g. 169.254.42.2

Target System* e.g. 169.254.42.2

Additional settings

Enable OPC UA □

	Server IP address*	Server port*
Data read (black)	e.g. 169.254.23.27	e.g. 4840

	Server IP address	Server port*
Data serve (red)	Red Input Interface Address	e.g. 4840

Download
© 2017-2020 genua Product Licenses Imprint Data Protection and Privacy

Figure 4.1: Online Configurator

Note: The online configurator does not save any data! As soon as you have completed the configuration and downloaded the configuration file, or as soon as you leave the page, all data entered into the fields is deleted.

You can create a configuration using the online configurator as follows:

1. Enter a fully qualified domain name for your **cyber-diode**.

2. Enter your cyber-diode's MAC address into the following field. If you set up several cyber-diodes via the online configurator, the `.hdf` configuration file is stored within the `update.tgz` archive named according to the configured MAC address.

   Note: With the online configurator you can configure one cyber-diode after the other, unpack the respective configuration files and as soon as you have configured all cyber-diodes, pack the individual configuration files into a `update.tgz`. This allows you to install multiple cyber-diodes with a single USB drive. The various cyber-diodes will use the configurations appropriate to their MAC addresses during installation.

   If you do not specify a MAC address, the configuration file will receive a generic name and is accepted by every cyber-diode.

3. Enter the license key that genua provided you in the license document.

4. If applicable, enable the Debug Mode and define a corresponding password. For further information about the Debug Mode, please read appendix A.1.

5. Enter an IP address and the prefix length for the input interface (black).

6. Enter an IP address and the prefix length for the output interface (red).

7. Enter the IP address of the target system within the server network (red network).

8. Within **Additional Settings** you can configure the OPC UA relay. Enable the checkbox **Enable OPC UA**, configure the corresponding IP address and the OPC UA server port on the black side as well as the port on the red side. This port is used by the OPC UA server to serve data to the OPC UA client within the red network.

9. Click on Download.
   Save the `update.tgz` file to your workstation.

10. Copy the file to a FAT32-formatted USB flash drive and apply the configuration to the **cyber-diode** as described in Chapter 4.3.

Note: The configuration of the transmitted protocols remains unchanged when using the online configurator. The following configuration is used:

- **TCP**: All ports (proxy and transparent)
- **UDP**: All ports (proxy and transparent)
- **SMTP**: Port 25 (proxy and transparent)
- **FTP/FTPS (FTP with SSL/TLS)**: Ports 20 and 21 (proxy and transparent)

> ! **Attention!** Only the **red / output** side of the cyber-diode is encrypted via FTPS. Data on the black / input side is **not** encrypted.

Data is accepted from any source IP address.

4.2 Creating a Configuration Using genucenter

Just like other genua appliances, the *cyber-diode* can be administered remotely by the **genucenter Management Station.**

An existing **genucenter Management Station** can be used for this. It must be running version 8.3 or later to support *cyber-diode* version 2.5.

As an alternative, you can also use a *virtual genucenter Management Station*. The virtual genucenter requires an appropriate license. This software is available for download in the Support section on the genua web server.

The operation of genucenter and its various menus are described in the *genucenter Installation and Configuration Manual*. The genucenter manual can be downloaded from the Support section of the genua website.

Note: The following section describes the process on the genucenter GUI. This requires that you have an account with the appropriate privileges on the genucenter and that you have experience using genucenter.

Customizing the Configuration

Administering the cyber-diode over the network is not supported. Configuration changes can only be transferred to a cyber-diode via a file created within genucenter and a USB flash drive.
The configuration is changed as follows:

1. Create new connection
2. Create appliance
3. (Optionally): Configure logging
4. (Optionally): Add local file extensions
5. Download file and save file to a USB flash drive
6. Update cyber-diode with the USB flash drive

These steps are described below.

Creating the New Connection for a cyber-diode

In order for the cyber-diode to permit connections from a black network to a red network, such a connection must be created as an individual object in genucenter.
You can choose one of the following protocols for a new connection:

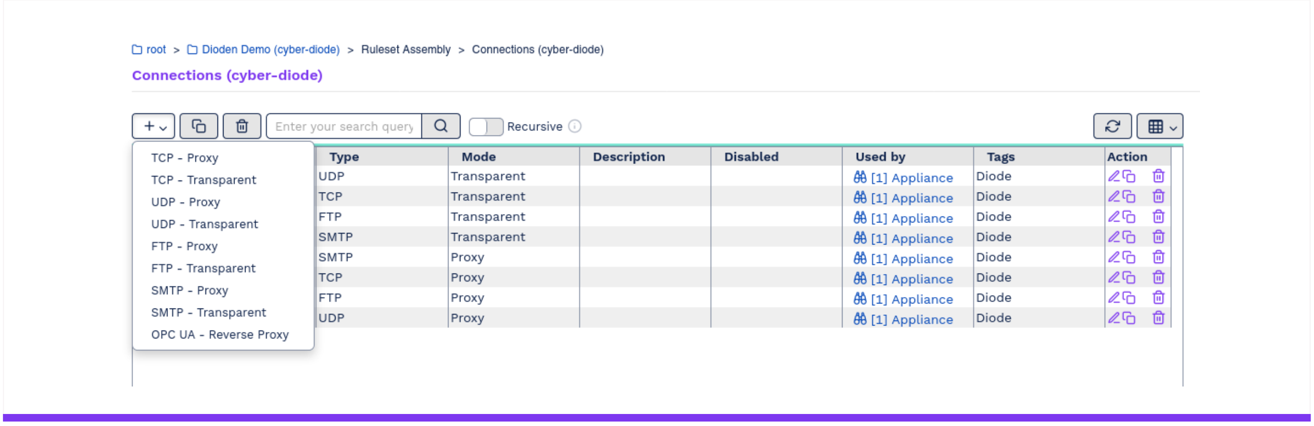
- TCP
- UDP
- FTP/FTPS (FTP with SSL/TLS, only on the red side)
- SMTP

- OPC UA Reverse proxy

You can choose between the modes “transparent” and “proxy” for every supported protocol (except OPC UA).

To create a new connection, follow these steps:

1. Select a domain and go to the menu Ruleset Assembly → Connections (cyber-diode).
2. You can create a new connection by clicking the “+” icon.



root > Dioden Demo (cyber-diode) > Ruleset Assembly > Connections (cyber-diode)

Connections (cyber-diode)

Type	Mode	Description	Disabled	Used by	Tags	Action
UDP	Transparent			[1] Appliance	Diode	
TCP	Transparent			[1] Appliance	Diode	
FTP	Transparent			[1] Appliance	Diode	
SMTP	Transparent			[1] Appliance	Diode	
SMTP	Proxy			[1] Appliance	Diode	
TCP	Proxy			[1] Appliance	Diode	
FTP	Proxy			[1] Appliance	Diode	
UDP	Proxy			[1] Appliance	Diode	

Figure 4.2: Creating a New Connection

3. Select a protocol and mode and enter the necessary information into the fields.

   You have to configure the server IP address and the destination port for the red and the black side. All other parameters can be configured for optimization purposes. Changing these parameters is usually not mandatory.
4. Click “Save” to finish.

A new connection for a cyber-diode has been created.
You can now proceed by adding a cyber-diode as a new appliance.

Creating the Appliance and Downloading the Configuration Update

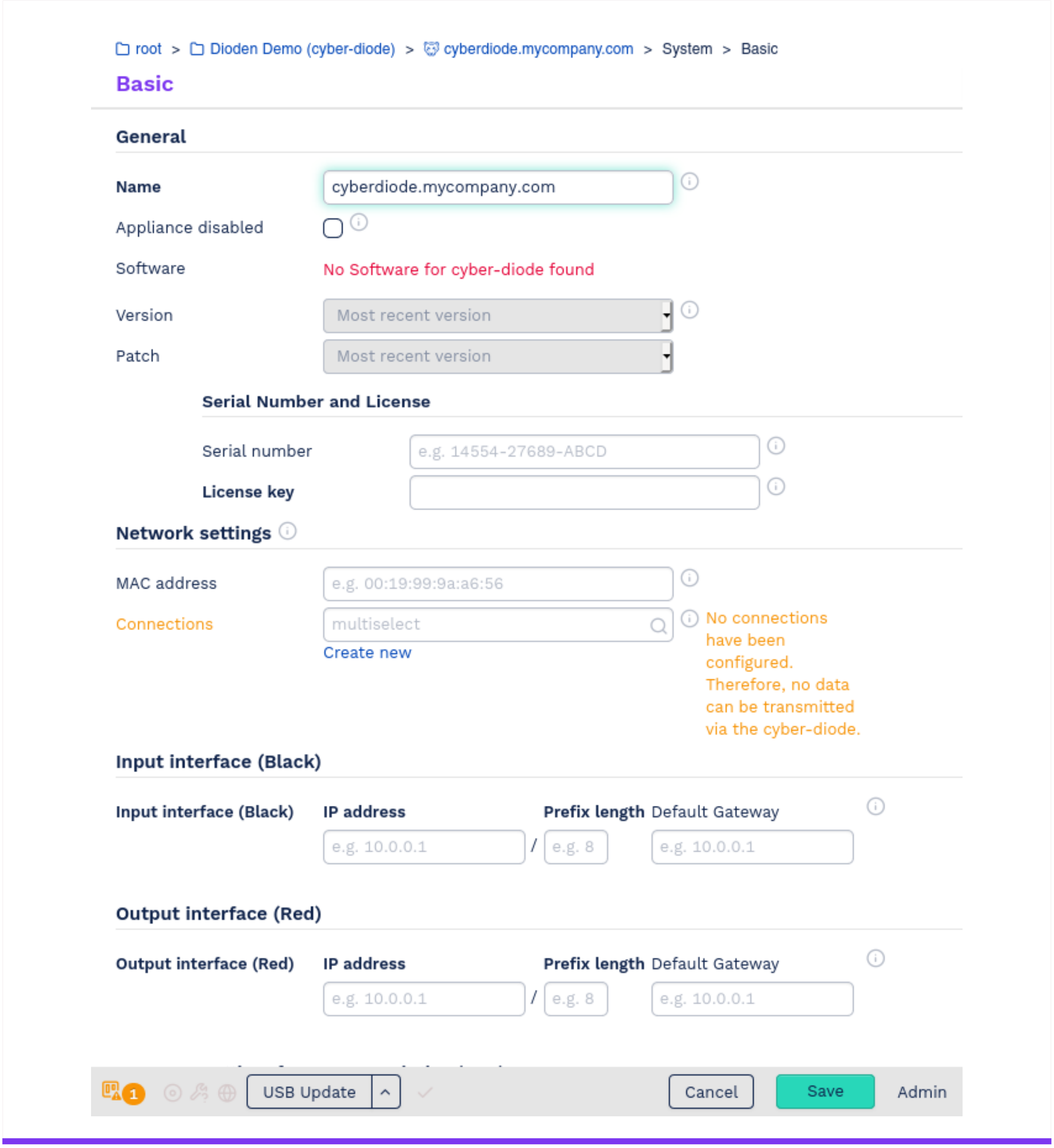
Have the following information available before adding a cyber-diode to genucenter:

- Hostname of the appliance
- License key from the genua license document
- IP address for the black interface
- IP address for the red interface
- **Optional:** IP addresses of DNS servers resolving addresses on the red side (when transferring files via FTP(S))

- **Optional:** Debug Mode password. You can find more information about the Debug Mode in appendix A.1.
- **Optionally:** Local file extensions

To add a cyber-diode as a new appliance, follow these steps:

1. Select a domain, click the “+” icon and choose “cyber-diode”.
2. Change the desired settings by filling the fields with their corresponding values.



root > Dioden Demo (cyber-diode) > cyberdiode.mycompany.com > System > Basic

Basic

General

Name: cyberdiode.mycompany.com

Appliance disabled: □

Software: No Software for cyber-diode found

Version: Most recent version

Patch: Most recent version

Serial Number and License

Serial number: e.g. 14554-27689-ABCD

License key:

Network settings

MAC address: e.g. 00:19:99:9a:a6:56

Connections: multiselect

Create new

No connections have been configured. Therefore, no data can be transmitted via the cyber-diode.

Input interface (Black)

Input interface (Black)	IP address		Prefix length	Default Gateway
	e.g. 10.0.0.1	/	e.g. 8	e.g. 10.0.0.1

Output interface (Red)

Output interface (Red)	IP address		Prefix length	Default Gateway
	e.g. 10.0.0.1	/	e.g. 8	e.g. 10.0.0.1

Figure 4.3: Configuring the cyber-diode

3. Click Save to finish.

Now, you can optionally configure syslog servers for the black and the red side of the cyber-diode.

1. Select the cyber-diode from the explorer view and navigate to the menu `System → Logging Settings`.
2. Configure syslog servers for the black and/or red side of the cyber-diode, if applicable.

3. Once the configuration has been completed, click Save at the bottom of the GUI.

The changes are now saved in the genucenter database.

Optionally, you may add local file extensions for HDF configuration changes via `<appliance>` → `Advanced` → `Files`. See the genucenter Installation and Configuration Manual for more information. Only changes to the HDF configuration are possible, other local file extensions will be ignored.
Local file extensions for the cyber-diode have to be created in the `hdf` subfolder. Add the subfolder when saving the local file extension to have it automatically created, e.g., `hdf/customizations.hdf`

To transfer the configuration changes to the appliance, you need to create an update file on genucenter and then transfer it to the cyber-diode using a USB flash drive.

Follow these steps to create an update file.

1. After having made the desired configuration changes, select the appliance (if necessary) within the explorer view and click USB Update at the bottom of the GUI. Set the check box **Update configuration** and click Execute. This starts a job that generates the update file.

2. After the job has finished a green check mark appears to the right of the button. Once you click it, you are forwarded to the job details page.

3. At the bottom of the GUI click the Download button. Save the update file to your workstation.

4. Copy the downloaded file to the USB flash drive included for configuration updates without unpacking the file. Configuration files already stored on the flash drive must be deleted beforehand or overwritten.

Note: If you want to install multiple cyber-diodes with a single USB stick, configure MAC addresses for each cyber-diode. The corresponding configuration files are then created according to the MAC addresses in the update file and the cyber-diodes use their respective configurations during installation.
Note, however, that the genucenter will only accept jobs where either **all** cyber-diodes have configured MAC addresses or jobs which contain only one appliance.
This means that with one job you can either configure a generic cyber-diode or configure several appliances individualized by their MAC addresses.

4.3 Applying the Custom Configuration

Insert the USB flash drive containing the new configuration into one of the two USB ports on the front of the appliance. The configuration is applied automatically. This process is indicated by the corresponding signals of the status LEDs.

Wait until both LED 3 and LED 4 (cyber-diode Rev 3) remain illuminated. Then, remove the USB flash drive and LED 4 will turn off. This means that the cyber-diode is operating properly, and a connection between the client and the server is enabled.

Upon applying the configuration log files from the cyber-diode are copied onto the USB stick. The log files are named according to the MAC address of the cyber-diode, so that log files of multiple cyber-diodes can be collected at once.

The Status LEDs

Since the *cyber-diode* operates without a monitor, operating states (normal, boot, error, etc.) cannot be displayed on a screen.

Therefore, the cyber-diode uses the LEDs on its front side to indicate various operating states.

cyber-diode Rev 3

Depending on the operating state, the LEDs light up or blink. Whenever LED 3 and LED 4 are illuminated you can remove the USB drive. In the normal operating state (verified software version, valid configuration, hard disk OK), only LED 3 is illuminated.

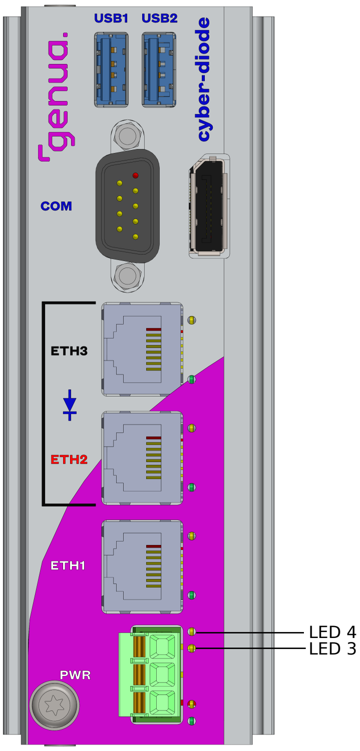


Figure 4.4: cyber-diode LEDs

Brief Overview of the Possible LED States

State	Meaning	Action
LED 3 on, LED 4 off	OK	X
LED 3 on, LED 4 blinking	USB drive detected, update in progress	Do not remove USB flash drive
LED 3 on, LED 4 on	Update finished successfully	Remove USB flash drive
LED 3 off, LED 4 on	Performing a reboot	Wait until LED 3 is on and LED 4 is off
LED 3 off, LED 4 blinking	Error	Repeat the configuration process and the configuration update, remove USB drive, log messages have been written to the USB stick

Chapter 5

Updating the cyber-diode Software

5.1 Updating the Software via genucenter

> **Note:** The software can only be updated to a higher or the same major version.

Due to storage space concerns, *cyber-diode* software images are no longer automatically supplied by genucenter starting with **genucenter Version 5.4**. As a result, these images first have to be manually transferred from the genua support server to the genucenter before a cyber-diode appliance's software can be updated.
To do so, follow these steps:

1. Select the genucenter from the explorer view and navigate to `Advanced → Software Management`.
2. Here you can configure some options such as proxy servers or an alternative patch server.
3. In the section **Download Software for Appliances** click the Save and Execute button. The bar to the right of the button shows the download progress.

Now, the *cyber-diode* software is available in genucenter. It is time to update the cyber-diode software:

1. Select the domain of your cyber-diode and navigate to `Maintenance → Create jobs`.
2. Select the cyber-diode from the table and choose the job `Configuration/Software → Update configuration and software with file`. Click the Execute button.
3. Set the check box **Update software/firmware** in the new window and click on Execute. After the job has finished the link **Download** appears in the "Status" column of the appliance table.
4. Click the and link and then on Download at the bottom of the GUI.

The cyber-diode configuration remains unchanged when updating the software.

5.2 Downloading software updates from the genua Web Server (without genucenter)

New versions of the *cyber-diode* software are available for download in the Support section on the genua web server:

`https://kunde.genua.de/en/overview/cyber-diode.html`

> **Note:** You have to log in using your customer credentials and enter your license key before you can download a software version from the "(Recovery) Releases" or "Software updates (Patches)" link.

Verifying the Checksum

The integrity of new *cyber-diode* software versions can be verified using the checksum as follows:

- View the checksums on the genua web server.
  1. Using your web browser, go to the URL above.
  2. Click on the “Checksums” link.
  3. Click on the “cyber-diode Patch Images Checksums” link.
     This page lists all of the available image files and their corresponding SHA256 checksums.
- Generate checksums for the new software version:
  The local checksum can be generated using the appropriate command for the checksum.
  - **Linux:** `$ sha256sum <File Name>`
  - **Windows:** `certUtil -hashfile <File Name> SHA256` (in the Command Prompt)
- Verifying the checksums:
  Next, compare the local checksum that you get for the software with the checksum on the genua server. If the checksums are the same, the integrity of the package is ensured. If they are different, please contact genua Support for assistance.

5.3 Installing the Software Update

Copy the new software (`.tgz` file) to a FAT32-formatted USB flash drive. Insert the flash drive into an open USB port on the front of the cyber-diode.

The cyber-diode automatically reboots (once or twice) and the new software is installed. The status LEDs indicate the progress with the corresponding signals. While this is happening, the connection between the client and the server is interrupted. See Chapter 4.3.

Wait until both LED 3 and LED 4 (cyber-diode Rev 3) remain illuminated. You can then remove the USB flash drive and test the communication connection.

Upon applying the configuration log files from the cyber-diode are copied onto the USB stick. The log files are named according to the MAC address of the cyber-diode, so that log files of multiple cyber-diodes can be collected at once.

Chapter 6

Recovering the cyber-diode Software

6.1 Recovery of the cyber-diode Software

In the rare case that the cyber-diode update fails and causes the system to lock up, a reset to the **original** version can be performed.

This is an emergency procedure and should only be performed if the cyber-diode cannot be reached either by genucenter or via a serial console/keyboard and monitor.

Note: After resetting the cyber-diode software, the configuration must be restored.

6.1.1 Downloading the software from the genua Webserver

Previous versions of the *cyber-diode* software are available for download in the customer portal on the genua web server:

`https://kunde.genua.de/en/overview/cyber-diode.html`

Note: You have to log in using your customer credentials and enter your license key before you can download a software version from the “(Recovery) Releases” link.

Download the software image and save it to your local workstation. Apply th recovery image to the cyber-diode. Please see section 6.2.

6.1.2 Downloading from genucenter

Starting with version 2.0, the required image can be downloaded from genucenter. See Chapter 5.1. After you have downloaded the desired software version via the software management, configure the software version in `<cyber-diode>` → `System` → `Basic`. Execute the job `Configuration/Software` → `Install appliance with file` from the maintenance menu. This job creates an `.img` file which you can transfer to a USB drive and onto the cyber-diode. This is described in the following sections.

6.1.3 Verifying the Checksum

The integrity of the software versions can be verified using the checksum. See Section 5.2.

6.2 Setting up the Software

Copy the software to a FAT32-formatted USB flash drive by one of the following methods:

6.2.1 Write the USB Flash Drive on Linux/Unix

The dd command is available on Unix and Linux systems. It is called as follows:

```
user@machine:~# dd if=/path/to/image of=/dev/usb-stick bs=1m
```

Modify the paths to your environment.

6.2.2 Write the USB Flash Drive on Linux/Unix

The USB flash drive can be written on a Windows workstation using the open source application “Rufus”.

Rufus can be downloaded from the page https://rufus.ie. The application can be run by double clicking it. No installation is required. The workflow is as follows:

1. Insert the flash drive in the workstation
2. Start Rufus
3. Select the USB flash drive
4. Check the box **Create bootable drive**
5. Select **DD Image**
6. Click on the CD symbol and and select the downloaded image
7. Click **Start** to write the image

6.2.3 Select Boot Device

Note: The USB drive supplied by genua is internally labeled as ATP NANODURA 1100.

Special system operations (for example software recovery) may require booting the cyber-diode from a different data medium (usually USB flash drive).

First determine the technical label of the data medium to help identify it in the BIOS.

To do so, insert the USB drive ino a USB port on your workstation and check for the label (Linux/Unix: use command dmesg, Windows: check in File Explorer).

Under Linux, a message similar to the following example will be displayed:

```
update  | sd1 at scsibus2 targ 1 lun 0: <ATP, NANODURA, 1100>
removable serial.111111122222233333
```

Revision 3

Disconnect the flash drive from your workstation and insert the flash drive into an open USB port on the front of the cyber-diode. Power on the cyber-diode.

After accessing the BIOS (by pressing Del during boot) select the entry **Boot Override - UEFI <Name of USB device>** from the `Save & Exit` menu. Confirm by pressing Enter.
This is how you can perform a one-time boot from your flash drive.

6.2.4 Setup

After booting from the flash drive the software setup will start. The cyber-diode will automatically reboot once or twice during setup. The status LEDs indicate the progress with the corresponding signals. While this is happening, the connection between the client and the server is interrupted.

Wait until both LED 3 and LED 4 (cyber-diode Rev 3) remain illuminated. You can then remove the USB flash drive and test the communication connection.

Upon applying the configuration log files from the cyber-diode are copied onto the USB stick. The log files are named according to the MAC address of the cyber-diode, so that log files of multiple cyber-diodes can be collected at once.

6.2.5 Restore the Configuration

After recovery, the system already is running with the standard configuration. See Chapter 3.

A modified configuration needs to be generated with the online configurator or downloaded from genucenter, and copied to the system. See Chapter 4.

Appendix A

Appendix

A.1 Debug Mode

A.1.1 General

Starting with cyber-diode version 1.3 it is possible to access a so-called Debug Mode. If activated, the administrator can connect to the internal compartments of the cyber-diode to diagnose configuration and communication problems.
Logging in to the internal compartment is only possible via a serial console, so a physical connection to the hardware is required.
The unidirectional data flow is still enforced in Debug Mode.

A.1.2 Configuring the password

In order to access the Debug Mode you have to configure the password during the installation.
This configuration can be done either with genucenter or the online configuration tool.

To configure the password of the Debug Mode, please read chapter 4.2 for configuration using genucenter or 4.1 for configuration with the configuration tool.

A.1.3 Using the Debug Mode

To use the Debug Mode, follow these steps:

1. Define a password for the Debug Mode using genucenter or the online configuration tool, enable the Debug Mode by activating the check box **Allow debug mode** and update the cyber-diode configuration.
   See chapters 4.2 or 4.1.

2. Connect a serial console to the **COM0** connector of the cyber-diode.

3. Reboot the cyber-diode.

4. Login with the user name `root` and the configured password.

5. Use the keyboard combination Ctrl b and the number of the desired compartment to log in to one of the compartments.

   - 1 for the black compartment
   - 2 for the red compartment

   Note: Use Ctrl b and h to display additional help.

6. Enter the configured login credentials.

7. You are now connected to the desired compartment and you can start debugging. Standard Unix tools for network debugging such as `ping`, `netstat`, or `tcpdump` are available. The corresponding man pages can be consulted over the internet.

A.2 Important Terminology

- **cyber-diode** Product name of the appliance.
- **Red Network** Network which receives data coming from the cyber-diode.
- **Black Network** Network from which data is sent to the cyber-diode.
- **Client** Sends data to the cyber-diode or the server.
- **Server** Receives data from the cyber-diode or the client.
- **OPC UA Client** Operates on the black side of the cyber-diode and receives data from the OPC UA server from the black network
- **OPC UA Server** Operates on the red side of the cyber-diode and offers data to OPC UA clients within the red network
- **Input Interface** Black network interface. The cyber-diode listens for data on this interface.
- **Output Interface** Red network interface. The cyber-diode transmits data from here.
- **Target System** Server inside the red network to which data is transmitted using proxy mode.

A.3 Technical Data and Safety Notices

A.3.1 Technical Data

- Supply voltage: 24 V DC; min. 0.5 A, max. 0.9 A
  (optionally: 100 – 240 V AC; 0,7 – 0,4 A; 50/60 Hz)
- Temperature (operation): 0 – 60 °C
- Temperature (storage): -40 – 80 °C
- Humidity: +55 °C and +25 °C, 90 – 100 % RH
- Measurements (w×d×h): 42×144×132 mm
- Weight: 790 g

A.3.2 Safety notices

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

! **Danger!** Please note that only qualified and trained personnel may install and use cyber-diode hardware.

! **Danger!** If used within an environment classified as VS-NUR FÜR DEN DIENSTGEBRAUCH/VS-NfD (approved/restricted operation), the security operating procedures (SecOPs) requirements have to be met.

! **Danger!** This device is not a toy. This equipment is not suitable for use in locations where children are likely to be present.

! **Danger!** The device must be operated with a certified power supply according to IEC/UL 62368-1 with the following output ratings: 16 – 60 V DC, max. 1.7 A.

! **Danger!** The device must not be mounted outdoors at a height of 2 m or higher.

! **Danger!** The device must be mounted on a DIN rail in a fire protection enclosure according to IEC/UL 62368-1, e.g., completely of metal, non-combustible or UL94-V0 material. If openings are present, the following max. dimensions apply to these openings.

- **For top openings**
  5 mm in each direction or
  1 mm width, regardless of length

- **For bottom openings**
  3 mm in each direction or
  1 mm width, regardless of length

! **Danger!** Cet équipement doit être installé hors de portée des enfants.

! **Danger!** L’appareil ne doit être utilisé qu’avec une alimentation certifiée selon la norme IEC/UL 62368-1 avec les valeurs de sortie suivantes: 16 – 60 V DC, max. 1.7A.

! **Danger!** En extérieur, l’appareil ne doit pas être monté à une hauteur supérieure à deux mètres.

!

Danger! Le dispositif ne peut être monté que sur un rail DIN dans un boitier résistant au feu (par exemple, entièrement en métal, en matériau non inflammable ou UL94-V0) conformément à la norme IEC/UL 62368-1. Si le boitier possède des ouvertures, celles-ci ne doivent pas dépasser les dimensions suivantes.

- **Pour les ouvertures supérieures**
  5 mm dans chaque direction ou
  1 mm de largeur, peu importe la longueur
- **Pour les ouvertures inférieures**
  3 mm dans chaque direction ou
  1 mm de largeur, peu importe la longueur

A.4 Support

You can send support request to:

support@genua.de

For individual solutions genua is available as a competent development partner to implement special configurations according to customer requirements.

You can also reach genua via the following contact information:

genua gmbh
Domagkstraße 7
85551 Kirchheim (near Munich)
Germany

tel +49 (89) 99 19 50-0

fax +49 (89) 99 19 50-999

https://www.genua.de

info@genua.de

Index