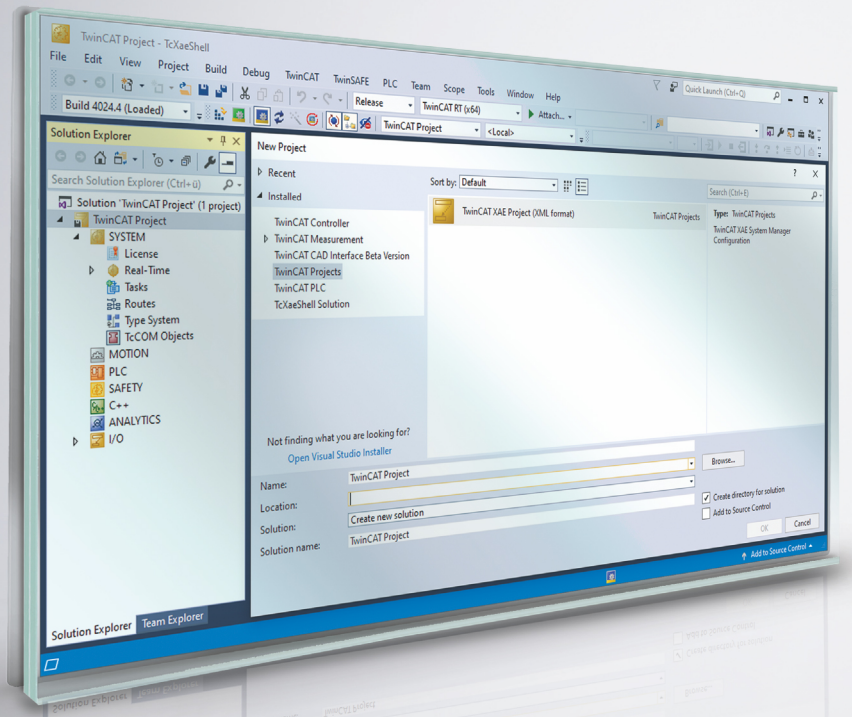
BECKHOFF New Automation Technology

Manual | EN

IPC Security Guideline

for Beckhoff RT Linux®



2026-08-12 | Version: 1.0

Table of contents

1 Notes on the documentation

This description is intended exclusively for trained specialists in control and automation technology who are familiar with the applicable national standards.
The documentation and the following notes and explanations must be complied with when installing and commissioning the components.
The trained specialists must always use the current valid documentation.

The trained specialists must ensure that the application and use of the products described is in line with all safety requirements, including all relevant laws, regulations, guidelines, and standards.

Disclaimer

The documentation has been compiled with care. The products described are, however, constantly under development.
We reserve the right to revise and change the documentation at any time and without notice.
Claims to modify products that have already been supplied may not be made on the basis of the data, diagrams, and descriptions in this documentation.

Trademarks

Beckhoff®, ATRO®, EtherCAT®, EtherCAT G®, EtherCAT G10®, EtherCAT P®, MX-System®, Safety over EtherCAT®, TC/BSD®, TwinCAT®, TwinCAT/BSD®, TwinSAFE®, XFC®, XPlanar® and XTS® are registered and licensed trademarks of Beckhoff Automation GmbH.
If third parties make use of the designations or trademarks contained in this publication for their own purposes, this could infringe upon the rights of the owners of the said designations.

EtherCAT® is a registered trademark and patented technology, licensed by Beckhoff Automation GmbH, Germany.

Copyright

Third-party trademarks

Trademarks of third parties may be used in this documentation. You can find the trademark notices here: https://www.beckhoff.com/trademarks.

1.1 Report vulnerabilities

We kindly request the security analysts to give us sufficient time to develop a solution for closing a security hole before publishing it. The Coordinated Disclosure ensures that customers get an update on the closure of security holes and that they are not unnecessarily endangered during the development of the update. Once customers are protected, the open discussion about the security hole can help the industry as a whole to improve its products and solutions.

If Beckhoff is the supplier of a product that is suspected of being vulnerable, discoverers and coordinators of security holes should contact product-securityincident@beckhoff.com with a vulnerability report, preferably in English or German. Confidentiality is requested. Means of sending encrypted messages are described in Contact Beckhoff Incident Response Team.

Discoverers are requested to provide all necessary contact information in the vulnerability report so that queries are possible. Nevertheless, anonymous vulnerability reports will also be considered. Please provide as much detailed information as possible so that the cases can be reproduced. If the discoverer wishes to publish the discovery, Beckhoff will attempt to coordinate a suitable preliminary release date within 30 days. The discoverer is informed of the availability of solutions prior to the release date and receives the corresponding Beckhoff Advisory. Beckhoff receives the discoverer's planned publication (including requested CVE where applicable). A final release date is then agreed. On this day, both the discoverer's publication and the Beckhoff Advisory are released. If the discoverer so desires and if he adheres to the above procedure, then a note of thanks, a reference to the discoverer's publication and, if helpful, information about the discoverer's publication will be added to the Advisory.

1.2 Contact Beckhoff Incident Response Team

Address

Beckhoff Automation GmbH & Co. KG
Product Management (Security)
Hülshorstweg 20
33415 Verl
Germany

E-mail

<product-securityincident@beckhoff.com>

E-mails to this address are sent to the responsible members of the Beckhoff Incident Response Team.

Public keys

The Beckhoff Incident Response Team has two keys for establishing contact:

- PGP key with ID `B4 F4 15 9A` and fingerprint `C9 6F 56 5C 39 49 43 58 AE B5 07 93 80 95 E1 2D B4 F4 15 9A`
- S/MIME certificate with ID `0a 0e 85 68 56 18 0f 5c 8a 5c 4e 83` and fingerprint `4c b4 d0 99 d4 a0 6c f0 af 69 ee 7a 8f 81 a1 c3 42 eb 17 da`

Key download: https://download.beckhoff.com/download/document/product-security/Keys

Working hours

The Incident Response Team normally works between 9 a.m. and 5 p.m., excluding public holidays, in North Rhine-Westphalia. Time zone: CET (Europe/Berlin).

1.3 Notes on information security

The products of Beckhoff Automation GmbH & Co. KG (Beckhoff), insofar as they can be accessed online, are equipped with security functions that support the secure operation of plants, systems, machines and networks. Despite the security functions, the creation, implementation and constant updating of a holistic

security concept for the operation are necessary to protect the respective plant, system, machine and networks against cyber threats. The products sold by Beckhoff are only part of the overall security concept. The customer is responsible for preventing unauthorized access by third parties to its equipment, systems, machines and networks. The latter should be connected to the corporate network or the Internet only if appropriate protective measures have been set up.

In addition, the recommendations from Beckhoff regarding appropriate protective measures should be observed. Further information regarding information security and industrial security can be found in our https://www.beckhoff.com/secguide.

Beckhoff products and solutions undergo continuous further development. This also applies to security functions. In light of this continuous further development, Beckhoff expressly recommends that the products are kept up to date at all times and that updates are installed for the products once they have been made available. Using outdated or unsupported product versions can increase the risk of cyber threats.

To stay informed about information security for Beckhoff products, subscribe to the RSS feed at https://www.beckhoff.com/secinfo.

1.4 Design goals for security

Beckhoff Industrial PC (IPC) hardware is designed for general use like a consumer PC for office environments, but with considerable additional robustness for use in industrial environments. The complete board is designed for reliable and highly deterministic operation in such environments. Nevertheless, the hardware supports universal operating systems such as Windows®, Beckhoff RT Linux®, and TwinCAT/BSD, which is based on FreeBSD®. As a result, the hardware is designed to support conventional and office IT-compliant security mechanisms as provided by the operating systems. The person who integrates the IPC into an operating environment is responsible for configuring these security functions for the respective environment accordingly. This person must also provide the operator with instructions for secure use. Such configuration and usage guidelines should be the result of a holistic security concept for the respective environment or conform to it.

Beckhoff IPCs can be ordered with or without an operating system. Windows 10, Windows 11, Beckhoff RT Linux®, and TwinCAT/BSD are available under these operating systems. Unless expressly ordered otherwise, these are provided as “Secure by Default”. This means that only certain services are enabled by default so that all access to the device is authenticated and the only preconfigured user has administrative access. For historical reasons, the preconfigured user is “Administrator”. The documented known password is preconfigured for this purpose. Please note the following: This is not “Secure by Default” with regard to the requirements of some environments, while it is well suited for others.

The operating systems listed have been recognized for decades for their security features in office and server environments. They contain and offer advanced security functions. Certain environments and applications have specific requirements for the configuration and use of these security functions. Since Beckhoff provides the operating systems mentioned for general use and does not wish to restrict which applications are implemented with them, Beckhoff cannot foresee the specific security requirements resulting from the respective use or integration. Instructions for secure configuration and use must therefore be created by the person who integrates the operating system into an environment for a specific use. Nevertheless, Beckhoff provides instructions for the secure use of the IPC and its operating system in this guide. These instructions are to be understood as general information and not as a complete and sufficient reference. The developers of the operating systems provide complete documentation for the security functions of the operating systems.

Beckhoff has developed extensions for these operating systems, in particular to optimize the deterministic behavior of the operating system for use with real-time applications in the automation industry. The extensions are integrated into the operating system images distributed by Beckhoff. The main objective in the development of these extensions is robustness and determinism for increased availability. Nevertheless, Beckhoff ensures that these extensions do not impair the basic security functions of the operating system, unless otherwise specified.

Beckhoff distributes a wide variety of software products. One example is the product “TwinCAT 3.1– eXtended Automation Runtime (XAR)”, or TwinCAT 3.1 XAR for short. This can be ordered pre-installed as part of the operating system on some IPCs. The main purpose of this special software is to provide a deterministic and robust but highly customizable runtime for automation applications. When installed on an IPC, it turns this device into a programmable logic controller (PLC). In addition to availability (through

robustness and determinism), the software was equipped with perimeter security during its development. This means that it can be configured and used to securely authenticate access via the protocols implemented by TwinCAT 3.1 XAR. With this perimeter security, the IPC's network interfaces mark the boundary. The security risk identified by Beckhoff for this type of security is that an unauthorized user gains access to the IPC via the protocols implemented by TwinCAT 3.1 XAR. For historical reasons and due to backward compatibility, TwinCAT 3.1 XAR still provides protocols that do not perform authentication before such access. Some IPCs with pre-installed TwinCAT 3.1 XAR have a configuration for TwinCAT 3.1 XAR which is secure by default. This means that this standard configuration only activates secure TwinCAT 3.1 XAR protocols. Please note that many IPCs that are delivered with pre-installed TwinCAT 3.1 XAR do not have a secure configuration by default for reasons of backward compatibility. This security guide contains a complete list of the protocols supported by TwinCAT 3.1 XAR and provides information on which protocols are secure, see Important TCP/UDP ports [▶ 28]. Separate documentation and instructions are available for the other software products. Please note the following: The latter also applies to TwinCAT functions that can be added to TwinCAT 3.1 XAR via a separate installer.

2 Hazards and risk assessment

This section provides an overview of the hazards and risk assessment for an automation system. Different attackers and types of attacks as well as typical threat scenarios and protection principles are described.

2.1 Attackers

Classification according to the position of an attacker

Attackers can be divided into four classes according to their access to a system:

Class	Description
Insider attackers	Attackers who want to perform certain actions on the automation system. The intention is to carry out damaging actions for which the attackers are not authorized. In addition, such attackers have access to private information, e.g. passwords, which they need to perform authorized actions.
Local attackers	Attackers who have direct access to components of the automation system. This class also includes local attackers who can access some components directly via hardware interfaces or change the network topology in different places.
Attackers in the internal network	Attackers who control devices on the internal network. Such attackers are generally unable to change the network topology and can only use existing services in the network.
Attackers from an external network	Attackers who can only execute actions through interfaces that are connected to the internet, for example. With successful attacks on internal components, these attackers can escalate to attackers in the internal network.

Assumptions

For all attackers it must be assumed that:

- they can receive public information such as documentation from the internet or via service calls;
- they are able to acquire any products available on the public market and to prepare targeted attacks by analyzing such products;
- they have significant computing power at their disposal, for example by renting computing time from a cloud provider.

The occasionally promoted categorization according to the motivation of an attacker is generally not expedient, as it involves a number of assumptions and speculations.

The classification helps when creating security analyses, but it should be noted that a real attacker has by all means various capabilities in several categories.

2.2 Attack types

Attacks can be categorized according to their execution. The effort involved in the attack plays a key role:

Category	Description
Broad, viral attacks	The attacks exploit widespread vulnerabilities and spread to reachable neighbors. Such "untargeted attacks" are aimed at attacking as many affected systems as possible in order to benefit the attacker. The benefits for the attacker arise, for example, from extortion to decrypt data ("ransomware") or using the resources of the attacked party ("botnet"). These attacks often use unpatched vulnerabilities or common organizational flaws such as weak passwords.
Vendor and integrator-specific attacks	The attacks exploit vulnerabilities in certain products that may be less common. These attacks can spread automatically, but they target special products or configurations as vulnerabilities (e.g. from Beckhoff or, if applicable, integrator configurations/extensions). Attack targets can also be industry-specific, such as spying out know-how or the like.
User-specific attacks	Such attacks are directed against precisely one system installation, hence the term targeted attacks. They are difficult to detect and are elaborately carried out by the attacker. Targeted system configurations are used to achieve the aim of the attack. Attack targets are manifold and are generally difficult to predict.

Only measures against broad viral and vendor-specific attacks are presented in these security guidelines. User-specific attacks necessitate analyses and counter-measures on the part of the user.

2.3 Typical threat scenarios

This section describes typical threats. However, the list is not exhaustive.

Manipulated boot medium

Attack type/attacker	Insider	Local	Internal network	Remote
Broad, viral attacks	not covered	not covered	not covered	not covered
Vendor and integrator-specific attacks	covered	covered	not covered	not covered

A prepared data storage device is connected to a component and the component is booted from it. This is possible if the boot order in UEFI/BIOS is set to boot from external disks or the attacker is able to change the boot order.

Through the attack an attacker can gain read and write access to all data of the component, especially configurations and know-how. After such an access has occurred, the entire component must be considered insecure.

Defensive measures:

- BIOS password (BIOS settings [▶ 16])
- Set boot media (BIOS settings [▶ 16])
- Locked control cabinet [▶ 14]

Unauthorized PXE boot server

Attack type/attacker	Insider	Local	Internal network	Remote
Broad, viral attacks	not covered	not covered	covered	not covered
Vendor and integrator-specific attacks	not covered	not covered	covered	not covered

Boot from an unauthorized PXE boot server in the internal network. The attack involves execution of code controlled by the attacker.

Through the attack an attacker can gain read and write access to all data of the component, especially configurations and know-how. After such an access has occurred, the entire component must be considered insecure.

Defensive measures:

- Disable PXE boot (BIOS settings [▶ 16])

Manipulated USB devices

Attack type/attacker	Insider	Local	Internal network	Remote
Broad, viral attacks	not covered	covered	not covered	not covered
Vendor and integrator-specific attacks	covered	covered	not covered	not covered

If manipulated USB devices are connected, it may be possible for the attacker to execute malicious code on the affected device. In addition, the affected USB device can also be used to steal know-how. For example, any code can be executed by a suitably configured autostart. Unauthorized input can be made or logged by a suitably prepared input device.

Such an attack allows an attacker to gain read and write access to a large number of data relating to the operating system, especially configurations and know-how. After such an access has occurred, the entire component must be considered insecure.

Defensive measures:

- Whitelisting USB devices (USB filter [▶ 25])
- Locked control cabinet [▶ 14]
- Disable interfaces in BIOS (BIOS settings [▶ 16])
- Whitelisting for programs [▶ 24]

Guessing of weak passwords through local interface

Attack type/attacker	Insider	Local	Internal network	Remote
Broad, viral attacks	not covered	not covered	not covered	not covered
Vendor and integrator-specific attacks	covered	covered	not covered	not covered

Weak passwords such as default passwords or easily guessed passwords can be exploited by local attackers. Like authorized local users, attackers can login with unmodified default passwords.

Such an attack allows an attacker to gain read and write access to a large number of data relating to the operating system, especially configurations and know-how. After such an access has occurred, the entire component must be considered insecure.

Defensive measures:

- Secure passwords [▶ 20]
- Set up individual users, no collective accounts
- Minimum rights for users ("Least Privilege"), in particular no administrator rights if not necessary

Theft of data carriers

Attack type/attacker	Insider	Local	Internal network	Remote
Widespread viral attacks	not covered	not covered	not covered	not covered
Vendor and integrator-specific attacks	covered	covered	not covered	not covered

An attacker may gain knowledge of and access information for services in an automation system via unauthorized removal of data carriers.

An attack like this allows an attacker to gain read access to a large amount of data related to the operating system, especially access data, configurations, knowledge and other sensitive private data.

An attacker could also try to gain access to sensitive data by stealing the storage media after it has been disposed of.

Defensive measures:

- Locked control cabinet [▶ 14]
- Secure data destruction

Extraction of sensitive data from discarded material

Attack type/attacker	Insider	Local	Internal network	Remote
Widespread viral attacks	not covered	not covered	not covered	not covered
Vendor and integrator-specific attacks	covered	covered	not covered	not covered

An attacker can gain access to discarded material which contains sensitive data on storage media.

An attack like this allows an attacker to gain read access to a large amount of data related to the operating system, especially access data, configurations, knowledge and other sensitive private data.

Defensive measures:

- Secure data destruction

Handling untrusted emails

Attack type/attacker	Insider	Local	Internal network	Remote
Broad, viral attacks	not covered	not covered	covered	covered
Vendor and integrator-specific attacks	not covered	not covered	covered	covered

Untrusted emails are a typical way to spread malware. In particular, attacks exploit opening of hyperlinks with outdated browsers and email attachments. Sometimes emails are formulated in such a way that they appear to be trustworthy.

A successful attack can execute unauthorized actions that are executed with the privileges of the interacting user.

Defensive measures:

- Do not use control computers for handling emails
- Regular or automatic software updates (Updates [▶ 19])
- Whitelisting for programs [▶ 24]

Exploiting known vulnerabilities in outdated software

Attack type/attacker	Insider	Local	Internal network	Remote
Broad, viral attacks	covered	covered	covered	covered
Vendor and integrator-specific attacks	covered	covered	covered	covered

Manufacturers release software updates to correct known vulnerabilities. If software that is in use is not updated, broadly based viral attacks can be carried out successfully.

A successful attack can execute unauthorized actions that have an impact in the context of the affected software.

Defensive measures:

- Regular or automatic software updates (Updates [▶ 19])

- Network-based detection mechanisms (IDS/IPS)
- Disabling unneeded services
- Removing components that are no longer needed [▶ 25]

Manipulated websites

Attack type/attacker	Insider	Local	Internal network	Remote
Broad, viral attacks	not covered	not covered	not covered	covered
Vendor and integrator-specific attacks	not covered	not covered	not covered	covered

A user is tricked into visiting an untrusted website. A vulnerability in the browser is exploited to execute arbitrary malicious code, or the website is designed in such a way that the user discloses confidential information such as login data.

A successful attack can execute unauthorized actions that are executed with the privileges of the interacting user.

Defensive measures:

- Regular or automatic software updates (Updates [▶ 19])
- Organizational measures for web surfing behavior.

Man-in-the-middle attacks

Attack type/attacker	Insider	Local	Internal network	Remote
Broad, viral attacks	covered	not covered	not covered	not covered
Vendor and integrator-specific attacks	covered	covered	covered	covered

When using an insecure network protocol, an attacker can pretend to be the trusted remote station within the reachable network. This allows the information sent via this protocol to be manipulated or intercepted.

A successful attack can lead to unexpected behavior of the services in the automation system.

Defensive measures:

- Network segmentation
- Use of secure network protocols

Unauthorized use of network services

Attack type/attacker	Insider	Local	Internal network	Remote
Broad, viral attacks	not covered	not covered	covered	covered
Vendor and integrator-specific attacks	not covered	not covered	covered	covered

If network services are provided that an attacker can access, this could result in unauthorized actions.

A successful attack can lead to unexpected behavior of the services in the automation system.

Defensive measures:

- Network segmentation
- Use of authenticating network services
- Disabling unneeded services
- Removing components that are no longer needed [▶ 25]

3 General measures

3.1 Employee training

Trained personnel are an important protection for the system. Employees who have access to the device should know how to operate it. This includes general measures such as the responsible handling of passwords and data carriers such as USB sticks. Every employee should be aware of the possible effects of intervening in the system.

3.2 Physical measures

One of the easiest and safest security measures is physical protection. Make sure that only administrators and technicians have access to the device. Attacks via physical access such as USB flash drives and other data carriers, which represent one of the biggest risks, can be reduced in this way. Physical protection of a device is achieved, for example, by means of a lockable control cabinet.

Locked control cabinet

The standard environment for an industrial controller should be a locked control cabinet. The attack surface is greatly reduced by allowing only individual interfaces to leave the control cabinet. The interfaces led out there should be additionally protected (lockable). Access to the control cabinet should only be given to persons who need it in order to perform their tasks. Electronic locking systems can also be used, for example based on smart cards. As with all key management systems, access to the control cabinet should be revoked when it is no longer required.

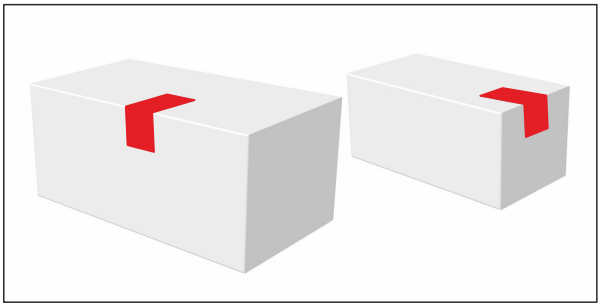
Video surveillance

Video surveillance is suitable for shift working in environments where many people need access to a controller or where facilities are geographically dispersed. However, video surveillance can only detect attacks and not prevent them. This measure is therefore only useful in combination with other measures.

3.3 Security seal on product packaging

From the end of 2021, seals with security features will be affixed in the factory to certain product packaging for Industrial PCs and Embedded PCs:

The position and nature of the seal are such that the removal of the goods from the packaging leads to irreversible and visible changes to the packaging and the seal. The intactness of the product can therefore be checked before opening by means of a visual inspection.



The seal is an aid to an efficient procedure for checking packed products. Because absolute security is impossible, the use of the seal is limited to the following applications: It allows a justified assumption to be made of the intactness, completeness and authenticity of the goods in the packaging without having to open the packaging. If the seal or the packaging is damaged, the recipient should ascertain the correct condition of the goods when accepting or using them. If the goods are intended for applications in which aspects of IT security are relevant, the recipient of the goods can, for example, stipulate that the goods are to be checked for tampering before use if the condition of the seal or packaging gives cause to suspect tampering during dispatch.

The design and stipulation of meaningful processes and rules for the acceptance and use of products from Beckhoff remain the responsibility of the recipient.

Opened seal

Products from Beckhoff often reach the recipient via a multi-step distribution chain. The seal may have been opened during the processing of the product. An opened seal is not grounds for a warranty claim.

4 BIOS settings

It is recommended that you set a password for the BIOS to ensure that critical settings such as boot order, CPU clock or important settings cannot be changed without authorization. It may also be useful to set the boot order and prevent external disks from booting. Settings in the BIOS should only be made by well-versed persons. The changing of unknown parameters can have a negative effect on the function of the system.

5 Operating system

5.1 Restore options

Define a backup and recovery strategy for your Beckhoff RT Linux® system in order to restore Beckhoff RT Linux® in a very short time in the event of data loss or defective storage media. Backups help to minimize downtime and thus to allow work to continue without large production losses. Both a process for creating a backup copy and a process for restoring it should be defined. Security aspects should also be taken into account and, for example, the storage location where the backup is to be saved should be defined. In addition, restore points will be used in the future to save the system's current state and restore it as needed. A variety of implementations will therefore be available, with the exact definition of a backup and recovery strategy left to the user.

5.1.1 Backup and restore

This chapter describes how to create and restore a backup of a Beckhoff RT Linux® image. The backup can be saved and managed on an external storage medium in order to restore the system in the event of a system failure or data loss. Make regular backups of your system.

5.1.1.1 Creating a backup

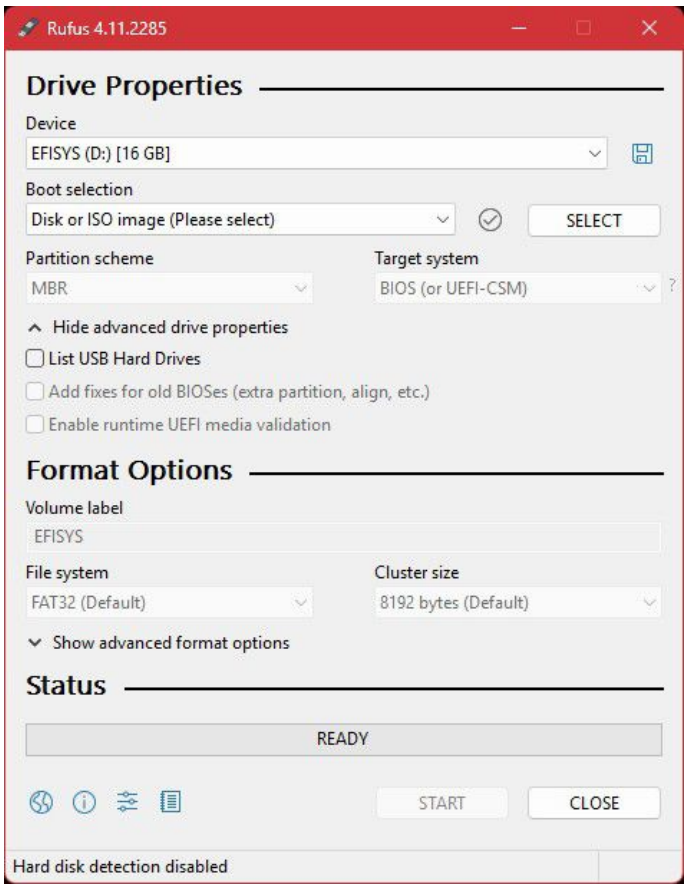
This chapter describes how you can create a backup copy of a Beckhoff RT Linux® image using the Rufus flash tool. The backup copy is created in VHDX format. It does not matter which storage medium is used for the backup. This can be either a microSD card or a CFast card.

Prerequisites:

- Memory card reader
- Download Rufus from: https://rufus.ie/

Proceed as follows:

1. Start Rufus on a PC with Windows operating system. The storage medium (MicroSD, CFast) should already be integrated under Windows.
2. The storage medium from which a backup copy is to be created appears under **Device**.
3. Click on **Show advanced drive properties** to enable advanced settings.
4. Click on the **floppy disk icon** to open the save function.



5. The file type **Compressed VHDX Image (*.vhdx)** is already chosen. Then choose the appropriate storage location and click **START** to create the backup copy.

⇨ You can then manage the backup copy created in VHDX format as you wish or restore the backup copy and thus the Beckhoff RT Linux® image (see: Restoring a backup [▶ 18]).

5.1.1.2 Restoring a backup

Use a suitable backup for the restore

Avoid incompatibilities and use the right backup for your device.

The backup of a Beckhoff RT Linux® image can in principle be restored to any storage medium. However, make sure that the backup is only used on a device of the same series, e.g. CX51x0, CX20x3, C6015 etc., as otherwise incompatibilities may occur.

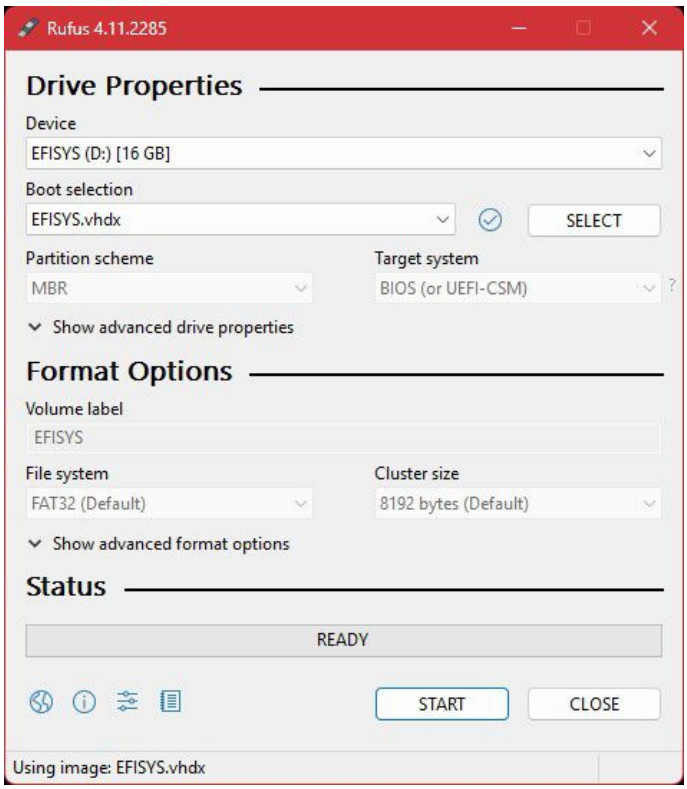
Use a flash tool such as Rufus to do this. The backup is copied directly to the storage medium, in this example in VHDX format.

Prerequisites:

- Existing backup of a Beckhoff RT Linux® image (see also: Creating a backup [▶ 17]).

Proceed as follows:

1. Start Rufus on a PC with Windows operating system. The storage medium (MicroSD, CFast) should already be integrated under Windows.



2. Click on **Select** and select the image you want to copy to the storage medium.
3. Select the microSD card as the target drive under **Device**.
4. Click on **Start** to start the copying process.

⇨ The process may take a few minutes. Do not cancel the process until the **Ready** message appears. Then boot the industrial PC from the storage medium used and start Beckhoff RT Linux®.

5.2 Updates

Regular updates are important because they primarily close known security vulnerabilities. You should review security updates promptly and install them in the system once they have been successfully validated. Beckhoff provides updates for the basic system and all other software components via the public package servers that are preset in each system.

For a system update, you should proceed as follows:

1. If possible, first test the update on test hardware to ensure it works properly with your own programs and the hardware you are using.
2. Back up the system so that you can restore it to its previous state in the event of unexpected behavior (see Recovery Options).
3. First, update the package information, and then view the packages that can be updated. Next, update the desired package or the entire system.

You can update the package information using the following command:

```
sudo apt update
```

You can view the packages for which updates are available using the following command:

```
apt list --upgradable
```

You can then update a single package using the following command:

```
sudo apt install
```

If you want to update the entire system, you can use the following command:

```
sudo apt upgrade
```

5.3 User and rights management

5.3.1 Secure passwords

Secure passwords are an important prerequisite for ensuring the security of a system. Beckhoff delivers the images with standard user names and standard passwords for the operating system. These must be changed by the customer. Otherwise, your device is vulnerable to attack via the network and access by unauthorized personnel.

Controllers are delivered without password in the UEFI/BIOS. Here, too, it is recommended to assign a password.

A Security Wizard is integrated in the system. This is started directly after booting up the device during local access. This wizard requests the user to change the password. However, the password can also be changed locally using operating system tools.

The following applies:

- Passwords should be unique for each user and service.
- Password complexity: the password should contain capital and lower-case letters, numbers, punctuation marks and special characters.
- Password length: the password should be at least 10 characters long.
- Contrary to some previous recommendations, it is recommended that passwords are no longer changed regularly, but only after an incident in which passwords have become known to unauthorized persons. See also https://arstechnica.com/information-technology/2016/08/frequent-password-changes-are-the-enemy-of-security-ftc-technologist-says/
- It may be useful to schedule a mandatory waiting time after unsuccessful logon attempt.

Generate secure password

There are many ways to create a secure password. The following table describes a method of generating passwords. The procedure can also help to remember complex passwords:

Procedure	Example
1. Start with one or two sentences.	Complex passwords are more secure
2. Remove the spaces.	Complexpasswordsaremoresecure
3. Abbreviate words or add spelling mistakes.	Complxpasswordsarmorescure
4. Insert numbers and special characters to extend the password.	Complxpasswordsarmorescure#529954#

Problematic passwords

Cyber criminals use sophisticated tools that enable high-performance attacks on passwords. Therefore, it is advisable to avoid:

- Words contained in dictionaries
- Words written backwards, common spelling mistakes, and abbreviations
- Repetitive sequences, e.g. 12345678 or abcdefgh
- Personal information, e.g. birthdays, ID numbers, telephone numbers

5.3.1.1 Change password

You can change the password of the currently logged-in user with the command `passwd`. Note that if you use `sudo passwd`, you run the command with root rights, changing the password of the superuser account (`root`) and not that of the logged-in user. Do not run `passwd` with root rights.

When Beckhoff RT Linux® is delivered, a user (`Administrator`) is available by default that you can use to login to the console. This user does not have conventional administrator rights as on Windows systems but has the authority to obtain `sudo` root rights for certain purposes.

Login data:

- Login: Administrator
- Password: 1

Proceed as follows:

1. Start the Industrial PC.
2. Log in with the user name `Administrator` and the password `1`.
3. After successful login, the user and the host name of the industrial PC are displayed. For example: CX-1D7BD4.
4. Enter the command `passwd` to set a new password. Follow the instructions.

⇨ You have successfully set a new password.

5.3.1.2 Password policies

Having your own password policy protects the system from the use of weak passwords. Determine the length and complexity of the user passwords used and follow the recommendations below:

To define a password policy, edit the file `/etc/pam.d/passwd` as follows:

```
sudo nano /etc/pam.d/passwd
```

Depending on your needs, add an entry for the pam_passwdqc module or modify an existing entry accordingly. One possible configuration, for example, is:

```
password requisite pam_passwdqc.so min=disabled,disabled,disabled,disabled,10 similar=deny retry=3
en-force=users
```

```
@include common password
```

If an entry for `pam_passwdqc` is already present, update it; do not add a second entry. Existing PAM lines related to actual password processing must not be removed.

For the parameter `pam_passwdqc.so`, at least five values can be set. These five values represent predefined password categories. Each position can either be disabled using “disabled” or assigned a number representing the required minimum length. The positions represent the following password categories:

- Passwords consisting of a single character set–that is, passwords consisting only of numbers or only of lowercase or uppercase letters;
- Passwords consisting of two character classes are allowed, i.e. passwords that consist of lowercase and uppercase letters, for example;
- Passphrases are allowed, i.e. strings of characters that can be separated by spaces;
- Passwords consisting of three character classes, such as lowercase and uppercase letters and numbers;
- Passwords consisting of four character classes: lowercase and uppercase letters, numbers, and special characters.

The example shown therefore only allows passwords that consist of all four character classes and are at least 10 characters long.

The `similar=deny` parameter specifies that the new password must not be similar to the previous one. The `retry=3` parameter determines how often a user is prompted to enter a new password if the chosen password does not meet the requirements of the password policy. With `enforce=users`, the user account policy is enforced.

5.3.2 Automatic logout

With autologout configured, a user is automatically logged out after a certain time without interacting with the command line. This is to prevent unauthorized access to the command line when the IPC is unattended and a logout by the user has been forgotten. By default, the autologout is not active, but should be switched on for commissioning.

To enable autologout, edit the file */etc/profile.d/autologout.sh* with root privileges, for example as follows:

```
sudo nano /etc/profile.d/autologout.sh
```

Add the following lines:

```
export TMOUT=300
```

```
readonly TMOUT
```

Log in again so that the user is automatically logged out after 300 seconds (5 minutes).

5.3.3 Group and file permissions

Beckhoff RT Linux® TwinCAT/BSD uses the access control list that is also used by other Unix®-like systems. There are generally three types of users for whom you can define permissions: owner of the files, owner's group, and all other users (Owner / Group / Other). For each user type, you can set write, read, and execute permissions for a file.

View the permissions of files and directories in one place with `ls -l`

```
Administrator@CX-0C8440$ ls -l
total 10
-rw-r--r--  1 root           Administrator   5 Dec  4 12:31 file
-rw-r--r--  2 Administrator  Administrator  10 Dec  4 15:29 test
drwxr-xr-x  3 Administrator  Administrator   6 Dec  7 10:44 testdir
```

The first column contains the permission scheme, followed by the owner of the file and the owner's group. The permission scheme is divided into four parts. The first icon indicates the type of file, whether it is a file (-) or a directory (d). The next three icons show the owner's rights, the next three icons show the group's rights, and the last three icons show the rights for all other users. The first of these three icons indicates whether read permissions have been granted (r), the second whether write permissions have been granted (w), and the third icon indicates whether the file can be executed or a directory can be accessed (x). The permission scheme of the above output from `ls -l` can be read as follows:

Type	Owner	Group	Other
- file	rw- read write	r-- read	r-- read
- file	rw- read write	r-- read	r-- read
d directory	rwx read write execute	r-x read execute	r-x read execute

By default, a new file is given the rights `-rw-r--r--`, which means that new scripts must first be made executable. With the default permissions, even the superuser root cannot run the script.

To change the permissions remotely via your development computer, you can use WinSCP, described in the TwinCAT/BSD documentation in chapter “Managing files with WinSCP client”. Locally, the permissions can be changed via the program `chmod`. Enter `man chmod` for the local manual.

Create unprivileged users

It is advisable to use different users for different tasks, such as an “HMI user” or a “maintenance” user. Give each user the rights they need to perform their tasks, and make sure that only the responsible users can be given root rights. To create a user account, use the following command:

```
sudo adduser benutzername
```

This will launch a wizard that will guide you through the user creation process. To edit a user account, use `sudo usermood [Optionen] <Benutzer>`

Groups

Users are divided into one or more groups. When a new user is created, a group with the same name is created by default. Additionally, users with similar tasks can be assigned to a common group to have similar permissions. These permissions can be access to specific folders and files, as well as running programs.

Users assigned to the “sudo” group can be granted root rights. The preconfigured user “Administrator” is a “sudo” member and obtains root rights by placing the command `sudo` in front of programs and authenticating again with their password.

Create new groups by running `sudo addgroup <Gruppenname>`, then use `sudo usermod -aG <Gruppenname> <Benutzer>` and to add a user to a group.

In addition, the command `sudo cat /etc/group` displays all available groups. Most of the groups shown are default groups and originate historically from Unix®. For security reasons, these groups are assigned to system users who have a specific task. Otherwise, these programs would run with root rights without restrictions.

5.3.4 Audit policy

As part of a security concept for the integration of a device into a network, it should be specified which level of security audit is suitable for detecting potential attacks. Security audit means that an industrial PC creates audit logs of events as soon as an interaction with the device takes place. For example, file and folder accesses can be logged each time a user accesses the selected files or folders.

These logs are intended for review to detect deviations from normal use that could indicate an attack, or for forensic purposes to reconstruct details about an attack. The check can be carried out immediately or at regular intervals by automated mechanisms or manually. It depends on the environment and the application as to which deviations are relevant. Therefore, rules that describe which actions are logged are usually configured using audit policies.

However, configuring too many rules can lead to a kind of blindness. The logs can become overloaded with irrelevant entries, with the relevant entries easily overlooked by humans or not processed quickly enough by automatic monitoring mechanisms. Sometimes it is good practice to forward logs to a central location for automatic review and/or archiving, among other things to avoid exhausting limited log capacity.

File and folder access, as well as security-relevant user inputs, can be logged in Beckhoff RT Linux®. Each time a user performs a specific action, the event is logged. These event logs are especially important for monitoring the system, detecting unauthorized access, and for subsequent analysis after a security incident.

Install and activate the audit daemon:

```
sudo apt update
sudo apt install auditd audispd-plugins
sudo systemctl enable auditd
```

Starting the audit daemon:

```
sudo systemctl start auditd
```

Checking the status:

```
sudo systemctl status auditd
```

If you also want to audit the early system startup, you can set the kernel parameter `audit=1` .

In `/etc/audit` you will find the configuration files of the audit daemon, which can be used to fine-tune the audit. Two areas in particular are important here:

`/etc/audit/auditd.conf` which is used for general, system-wide audit settings, and `/etc/audit/rules.d/*.rules` , where the actual audit rules are defined.

For a Beckhoff RT Linux® system, it is recommended to start with a conservative set of rules that logs changes to security-relevant configuration files, identity data, mount operations, kernel modules, and permissions without placing an unnecessarily heavy load on high-frequency runtime paths.

An obvious example configuration is:

```
# /etc/audit/rules.d/30-rt-security.rules

-b 8192
-f 1

# Audit-Konfiguration selbst überwachen
-w /etc/audit/ -p wa -k audit-config

# Benutzer-, Gruppen- und Authentisierungskonfiguration
-w /etc/passwd -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/group -p wa -k identity
```

```
-w /etc/gshadow -p wa -k identity
-w /etc/sudoers -p wa -k privilege
-w /etc/sudoers.d/ -p wa -k privilege
-w /etc/pam.d/ -p wa -k pam-config
```

```
# Zeitänderungen
-a always,exit -F arch=b64 -S adjtimex,settimeofday,clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
```

```
# Host- und Netzwerkkonfiguration
-w /etc/hostname -p wa -k network-config
-w /etc/hosts -p wa -k network-config
-w /etc/resolv.conf -p wa -k network-config
-w /etc/network/ -p wa -k network-config
```

```
# Persistenzmechanismen
-w /etc/crontab -p wa -k cron
```

On 64-bit systems that also allow 32-bit applications, the corresponding `arch=b32` rules should be supplemented accordingly.

Run `sudo augenrules –load` to load the rules and `sudo auditctl -l`, to view the loaded rules. You can then view the audit logs using commands such as `sudo aureport -k -i` or `sudo ausearch -k identity -i`.

As a general rule, you should avoid rules that extensively monitor high-traffic directories or heavily used system calls–for example, global rules on `/tmp, /run, /var/tmp` or complete monitoring of all `execve-`, open or read accesses. Such rules can quickly lead to large amounts of log data and compromise real-time performance. Instead, it is recommended to focus on:

- Changes to user, group, and authentication data
- Changes to network and host configuration
- Changes to startup mechanisms and services
- Mount and kernel module activities
- Changes to permissions, ownership, and attributes
- optional, targeted monitoring of critical application directories

5.4 Programs

5.4.1 Whitelisting for programs

Application whitelisting, as available on Windows with, for example, AppLocker or Software Restriction Policies (SRP), does not exist in exactly the same form onLinux® systems. However, there are various approaches to restricting the execution of programs to defined applications, files, services, or integrity states. However, these approaches are less uniform and generally more complex to configure and operate than under Windows.

The reason for this is the increased complexity associated with the command line, scripts, interpreters, and flexible toolchains in Linux® systems, as opposed to the mostly graphical user interface in Windows. Strictly enforced application whitelisting is therefore possible in principle, but in practice it often involves increased maintenance and testing efforts. Particularly with Beckhoff RT Linux® systems, it is also important to note that, depending on their configuration, additional security-related mechanisms can affect runtime behavior, maintainability, and real-time characteristics.

Instead, you should pay close attention to the sources from which packages are obtained and which packages are installed on the system. It is recommended that you use only trusted and verified package sources and install only the software that is actually necessary for the intended operation. Programs, services, interpreters, compilers, and administration tools that are not needed should be removed or not installed in the first place (see Removing components that are no longer needed [▶ 25]).

In addition, the execution of unwanted programs can be made more difficult by implementing appropriate system hardening measures. These include, for example, restrictive service configurations, integrity checks, the restriction of writable areas, and appropriate file system options. In practice, however, for Beckhoff RT Linux® systems, a reduced, controlled, and regularly reviewed software inventory is often the most obvious and low-maintenance approach.

5.4.2 Removing components that are no longer needed

To reduce the size of the attack surface, unneeded programs, services, and operating system components should be removed.

The deletion of system components should only be done by experienced users. Negative side effects may occur, and programs or services can no longer be run correctly.

Particularly with Beckhoff RT Linux® systems, changes should be reviewed and tested in advance, as even indirect dependencies can affect proper operation.

With `apt list –installed` you can view all packages installed on the system. On delivery, all packages listed here are relevant for the basic system or for Beckhoff software. Alternatively, you can query the package database directly using `dpkg -l`. In addition to packages for the actual application, diagnostic, or administrative functions, the list also includes packages required by other programs.

If a package that is required by another installed package is removed, the package manager will indicate which other packages are affected or would need to be removed as well. This allows you to determine whether a package is still a dependency of other installed components. Packages that are known to no longer be needed can be removed using `sudo apt remove <Paketname>`.

If you also want to remove the associated configuration files, you can use *sudo apt purge <package name>* instead. After that, you can use `sudo apt autoremove` to automatically delete dependencies that were installed but are no longer needed. This ensures that no packages that are no longer needed remain on the system. In addition, any services that are not needed should be disabled, unless they are already removed by uninstalling the corresponding packages.

5.4.3 Package audit

Beckhoff RT Linux® provides a tool called `debsecan` that allows you to check installed software for known vulnerabilities. The command `debsecan --suite trixie` compares information about known vulnerabilities with the locally installed packages. You will receive the **CVE** (*Common Vulnerabilities and Exposures*) number as well as information about the affected packages.

5.4.4 Antivirus programs

Antivirus programs do not appear to be necessary for Beckhoff RT Linux® and Linux® systems in general, because malicious software for Linux® systems tends to be rare. Viruses for Linux® systems are still very rare. The main reason for this is the less widespread use of the systems compared to Windows and Mac OS.

In addition, there is a clear separation of user accounts and their rights. Under Beckhoff RT Linux®, even the Administrator user must obtain root rights for changing system-relevant files and executing programs by entering a password. Scripts must be made executable before they can be run at all. An accidentally downloaded virus can initially only infect the files of the logged-in user. Propagation throughout the system is not easily possible due to the strict permissions management.

However, security vulnerabilities must be closed through regular updates. Due to the large open-source community, security holes are usually quickly identified and closed. The updates are then available via the Beckhoff Package Server preset in each system.

There are antivirus programs for Linux® systems, but they are mainly useful for mail or file servers that can also be used by Windows clients. Of course, an antivirus program can also be used to add another security layer to the system. For Beckhoff RT Linux®, the free Linux® antivirus program Clam Antivirus is available in addition to some proprietary applications. Note that this program falls under the GPL license and is subject to its terms.

5.5 USB filter

For security reasons, USB storage devices are not mounted automatically. You must implement them manually for each session or configure automatic implementation.

6 Network communication

At this point an overview will be provided of some relevant measures with regard to communication. Topics outside of the actual IPC – such as network segmenting – are not dealt with.

A list of the ports used for TwinCAT products can be found here: Important TCP/UDP ports [▶ 28] .

6.1 Remote maintenance

Remote maintenance plays an important role in industrial facilities. It enables service technicians and programmers to carry out maintenance work remotely in the event of a malfunction.

Since remote maintenance access routes are generally always available for maintenance purposes and security measures are often neglected in order to be able to react quickly in the event of a malfunction, such access routes are often used for attacks.

Measures at this point are absolutely necessary to prevent attacks that could disrupt system operation.

See also:

- VPN [▶ 27]

6.2 Firewall

Firewall settings are a means of protecting the system from network attacks. Incoming ports that are not needed should be blocked. Even better than that, however, is not to start any services that open these ports. The necessary settings require an overview of the ports used that is coordinated with everyone involved.

A firewall can be used to filter the network packets that are passing through. Depending on the firewall technology, filter rules can be formulated on the basis of address, port, state of communication relationship, content of the packet, and much more. Firewalls are thus a tool to reduce the attack surface.

A firewall can be implemented as additionally installed software, as part of the operating system, or as a self-contained device. Each of these forms has advantages and disadvantages. A host-based firewall provides protection directly on the system, while an external firewall can filter network traffic centrally.

Firewalls with deep-packet inspection, which also evaluate the user data of the data packets, are not able to see the contents of encrypted connections. In order to be able to process the content (e.g. web applications), encryption is often terminated at the firewall and the data for the client is re-encrypted. As a result of this, the contents are visible to the firewall, but the end-to-end encryption is interrupted.

Restrictive, explicit settings for communication via a firewall are an important measure to allow network access only to the necessary extent.

Important TCP/UDP ports [▶ 28] contains a list of TCP/UDP ports that typically need to be considered in order to configure a firewall.

In Beckhoff RT Linux®, packet filtering is performed using `netfilter` with `nftables`. This allows you to define rules for incoming, outgoing, and forwarded network connections.

You can view the currently active firewall configuration by running `sudo nft list ruleset`. Even if the standard file `/etc/nftables.conf` exists on the system, it is not used as the primary configuration file on that system. The file `nftables`, loaded by the `/etc/nftables-bhf.conf` service, is the key file; it includes additional rule files from `/etc/nftables.conf.d/`. This enables a modular and more maintainable structure for the firewall rules.

When configuring the system, you must ensure that only the connections actually required for operation are enabled. You should disable any ports and services that are not needed, or block them using appropriate filter rules. If both secure and insecure communication options are available, you should, whenever possible, enable only the secure options.

You should review changes to the firewall configuration after commissioning and after software updates to avoid unintentional openings or blocked communication paths.

6.3 Network technologies

This section describes the security-relevant features of some protocols.

6.3.1 Modbus

The Modbus protocol was originally developed in the late 1970s as a serial communication protocol. The main objectives were to provide a communication protocol for industrial applications that was easy to set up and maintain and transfers data without the need to develop an information model. Because of this simplicity, it has been very popular for 30 years. But this simplicity makes it difficult to use Modbus in modern industrial plants that place more complex demands on a communication protocol, such as security and information models. The original Modbus protocol does not include security measures such as encryption or authentication.

Even though Beckhoff provides two TwinCAT functions for Modbus RTU and Modbus TCP, it is advisable to use more advanced protocols such as OPC UA, which inherently implement security mechanisms.

6.3.2 ADS

The Automation Device Specification (ADS) is a proprietary communication protocol developed by Beckhoff. It is designed for high throughput and portability over different transport protocols (e.g. TCP or serial). ADS was not designed with security in mind and does not include cryptographic operations because of their negative effect on performance and throughput.

It is recommended to use ADS only in secured environments or to use appropriately secured transport channels.

For ADS there are currently two TCP transport channels that support encryption:

- ADS-over-MQTT
- Secure ADS

6.3.3 OPC UA

OPC Unified Architecture (IEC 62541) is the new technology generation of the OPC Foundation for the secure, reliable and manufacturer-neutral transport of raw data and pre-processed information from the manufacturing level into the production planning or ERP system. With OPC UA, all desired information is available to every authorized application and every authorized person at any time and in any place.

Further information can be found in the documentation: TF6100 TC3 OPC UA

6.3.4 VPN

A Virtual Private Network (VPN) makes it possible to establish a virtual LAN between different devices via public networks. In most cases, the data traffic transmitted over the public network is encrypted. VPN solutions can be used, for example, to temporarily tunnel insecure protocols until secure alternatives are operational.

6.4 Security Gateway

A further option to protect the system from network influences is the use of a security gateway. This hardware solution can be installed in a network in front of an IPC. This way, certain network segments or every single PC can be protected.

In addition to the network protection function, the devices also offer the option, for example, to run antivirus software and thus to monitor a file transfer that is implemented via a local clipboard – without limiting the real-time capability of the actual control computer.

6.5 Important TCP/UDP ports

Depending on the use case, unsecured protocols must be disabled or secured by a lower-level layer, for example by a physically secured network or VPN.

In the case of secured protocols, the security must be commissioned in accordance with the product documentation.

Standard services

The table below provides an overview of the incoming ports that are opened in the normal case in the delivered images

Service	Ports (incoming)
SSH	22 / tcp
HTTPS/Device Manager	443 / tcp
ADS Secure	8016 / tcp
ADS Broadcast	48899/udp
mDNS/local name resolution via IPv4 and IPv6	5353/udp

TwinCAT services

The table below provides an overview of the ports typically used with TwinCAT products:

Service	Port (default setting)
TF1810 TwinCAT PLC HMI Web	80 / tcp (incoming) See also: Documentation on TF1810
TF2000 TwinCAT HMI	1010 (versions ≤ 1.12), 2010 (versions ≥ 1.14) / tcp (local) 1020 (versions ≤ 1.12), 2020 (versions ≥ 1.14) / tcp (incoming) See also: Documentation on TF2000
TF6100 OPC UA	4840 / tcp (UA Server, incoming), changeable 48050/tcp (UA Gateway, incoming), changeable See also: Documentation on TF6100
TF6100 OPC DA	Dynamic (depending on DCOM) between 1024 and 65535 (incoming) See also: Documentation on TF6120
TF6250 Modbus TCP	502 / tcp (incoming), changeable See also: Documentation on TF6250
TF6310 TCP-IP	changeable / tcp (incoming, outgoing) See also: Documentation on TF6310
TF6311 TCP/UDP Realtime	changeable / tcp (incoming, outgoing) The communication cannot be influenced by an operating system firewall. See also: Documentation on TF6311
TF6300 FTP	20 / tcp (outgoing) 21 / tcp (outgoing) See also: Documentation on TF6300
TF6420 Database Server	changeable depending on the database / tcp (outgoing) See also: Documentation on TF6420
TF67xx IoT TF35xx Analytics	changeable depending on the broker / tcp (outgoing) See also: Documentation on TF670x and TF35xx
TwinCAT EAP	34980 / udp (incoming), if EAP is used via UDP. The communication cannot be influenced by an operating system firewall. See also: Documentation of EAP
TwinCAT ADS-over-MQTT	changeable depending on the broker / tcp (outgoing) See also: Documentation on ADS-over-MQTT

6.6 Nginx web server

The Nginx web server is active by default on Beckhoff RT Linux® and is used, among other things, for the Beckhoff Device Manager.

To further secure the system and restrict access via the web server, you can disable forwarding in the Nginx configuration. In Beckhoff RT Linux®, the relevant entries are configured via the file `mdpwebservice-bhf.conf` and the included `location` files.

1. Open the file `mdpwebservice-bhf.conf` at `/etc/nginx/sites-enabled/` and check the linked `location` files at `/usr/share/mdpwebservice-bhf/locations/`.. The files should be named `00-root.conf, 10-config.conf` and `20-console.conf`.
2. Completely comment out the entries under `location /,location /config/` and `location /console/` .

```
# location / {
# add_header ServerHostname $hostname;
# root /usr/local/www/default;
# index index.html index.htm;
# }
```

```
# location /config/ {
# include /usr/share/mdpwebservice-bhf/errorpages.conf;
# include /usr/share/mdpwebservice-bhf/auth.conf;
# include /usr/share/mdpwebservice-bhf/proxy.conf;
# proxy_pass http://unix:/var/run/mdpwebservice-bhf/web0;
# }

# location /console/ {
# include /usr/share/mdpwebservice-bhf/errorpages.conf;
# include /usr/share/mdpwebservice-bhf/auth.conf;
# include /usr/share/mdpwebservice-bhf/proxy.conf;
# proxy_set_header Upgrade $http_upgrade;
# proxy_set_header Connection "upgrade";
# proxy_pass "http://127.0.0.1:7681/";
# }
```

3. Save the modifications.
4. Check your configuration with `sudo /usr/sbin/nginx -t.`
5. Then restart the Nginx service using `sudo systemctl restart nginx .`

⇨ From now on, no requests will be forwarded to the Beckhoff Device Manager.

6.7 HTTPS certificates

This chapter describes how you can create and import your own HTTPS certificates if the certificates provided by Beckhoff by default for the web interface (Device Manager) are not suitable for your application.

Certificates are used in information technology to securely prove identities. This allows messages or documents to be encrypted so that only the intended recipient can decrypt the content again. Among other things, this technique is used by every web browser when retrieving a page via the HTTPS protocol.

A network subscriber requests the certificate of another subscriber when establishing a communication connection. The certificate and whether the other party authenticates itself using the associated key are checked. Once the identity has been proven, the subsequent message exchange over the connection can be protected against unauthorized manipulation and, optionally, against unauthorized viewing.

In order to use specially generated HTTPS certificates:

- the automatic generation of a certificate for industrial PCs must be disabled,
- a certificate must be requested from a certificate authority (CA)
- and then the HTTPS certificate must be imported.

The exact procedure and the necessary steps are described in this chapter.

6.7.1 Disabling automatic certificate creation

In some use cases it does not make sense for the user to reuse the certificates generated automatically for the web server. In this case, you can disable automatic synchronization and use your own certificate for the web server (nginx).

To do this, you must first disable automatic certificate creation so that your own certificates are installed and not overwritten by the default Beckhoff certificate.

Proceed as follows:

1. Disable the service `TcSeldSigned` so that the certificate is not overwritten by the default Beckhoff certificate.
2. To do this, enter the command `sudo systemctl disable –now TcSelfSigned.service` in the console.

⇨ You have disabled the automatic generation of certificates.

Also see about this

Requesting or creating an HTTPS certificate [▶ 31]

6.7.2 Requesting or creating an HTTPS certificate

A certificate authority (CA) typically provides installation instructions on how to install a certificate it has issued. The certificate authority even provides instructions on how to apply for the certificate. Please primarily follow the instructions of the certificate authority.

First, you must create a certificate signing request (CSR) and forward the certificate request to the certificate authority in accordance with its instructions. The certificate authority will then provide you with the server certificate and the intermediate certificates in response to the certificate signing request

If you do not have a certificate from an official certificate authority (CA), you can create a self-signed certificate for test purposes.

Proceed as follows:

1. Generate a self-signed certificate for test purposes with the following command:

```
Openssl req -new -newkey rsa:4096 -nodes -sha256 \
                -keyout IPCDiagnostics.key \
                -out IPCDiagnostics.csr \
                -subj '/CN=<hostname>' \
                -addext 'subjectAltName=DNS:<hostname>,IP:<ipaddress>'
```

2. The command creates a private key `IPCDiagnostics.key` and a self-signed certificate `IPCDiagnostics.crt`.

   `openssl req`: The command-line tool `req` creates and edits certificate signing requests (CSR). Instead, `-x509` is used to generate a self-signed certificate directly.

   `-newkey rsa:4096`: Creates a new key pair using the RSA algorithm with a key length of 4096 bits.

   `-nodes`: Means “no DES.” The private key is saved unencrypted, which means no password is required to use the key.

   `-sha256`: Uses the SHA-256 secure hash algorithm to generate the certificate signature.

   `-keyout IPCDiagnostics.key`: Saves the private key to the IPCDiagnostics.key file.

   `-out IPCDiagnostics.crt`: Saves the created certificate to the file IPCDiagnostics.crt.

   `-subj '/CN=<hostname>'`: Specifies the data for the certificate without an interactive query. `/CN=<hostname>` specifies the common name (CN), which is usually the host name or domain that is protected by the certificate.

   `-addext 'subjectAltName=DNS:<hostname>,IP:<ipaddress>'`: Adds an extension to the certificate. `subjectAltName` (SAN) allows additional names and IP addresses to be covered by the certificate.
3. Replace `<hostname>` with the host name and with the IP address of your Linux® device.

⇨ In the next step, the certificate can be imported (see Importing the certificate [▶ 31]).

Also see about this

Importing the certificate [▶ 31]

6.7.3 Importing the certificate

As soon as you have received a certificate from an official certificate authority (CA), you can import it into your Beckhoff RT Linux® system. Alternatively, you can also use the self-signed certificate that you have created for test purposes.

Proceed as follows:

1. Replace the existing private key for nginx with your private key:

```
sudo cp IPCDiagnostics.key /etc/TwinCAT/3.1/Target/PrivateKeys/IPCDiagnostics.key
```

2. Replace the existing certificate for nginx with your certificate:

```
sudo cp IPCDiagnostics.csr /etc/TwinCAT/3.1/Target/Certificates/IPCDiagnostics.csr
```

3. Restart the nginx web server:

```
sudo systemctl restrt nginx
```

4. The certificate is ready for use after restarting the service.

⇨ If you are not using a certificate from an official certificate authority (CA), your browser will display a security warning. You can configure your browser to accept the certificate automatically by importing the server certificate into your browser's certificate store. For more information on this topic, see Self-Signed Certificates for HTTPS connections

Since some browsers (e.g., Mozilla Firefox) use their own certificate stores, it may be necessary to import the certificate directly into the browser.

7 TwinCAT

What is considered a threat for eXtended Automation Engineering (XAE) and eXtended Automation Runtime (XAR) must emerge from a security concept for the plant. The IEC 62433 standard, which explains, among other things, the necessary threat analysis, provides assistance in creating a security concept. In addition, the VDMA guide can be consulted to help with security in operating processes and the resilience of products against cyberattacks: https://www.vdma.org/viewer/-/v2article/render/16110956

This chapter lists some example threats related to XAE and XAR without claiming to be complete.

7.1 eXtended Automation Engineering (XAE)

Table 1: Unauthorized manipulation of the source code.

Countermeasures	Description
Technical	• Define authorizations and implement them with software protection • Use version control system to make changes traceable • Use individual access control for version control system
Organizational	• Use IT security management system (e.g. according to ISO 27001) • Use version control system (see: Source-Control): • Use "Staging": ◦ Check-in first in development source control repository ◦ Use separate (pre-)release build repository to build alpha, beta, RC and release versions from there ◦ Transfer development repository -> (pre-)release build repository only after review, for example via Project Compare Tool (see: Project Compare Tool)

Table 2: Unauthorized access to the source code.

Countermeasures	Description
Technical	• Store source code encrypted using software protection (see: Software protection)
Organizational	• Use IT security management system (e.g. according to ISO 27001). • Secure access to the storage locations. • Use encrypted storage.

7.2 eXtended Automation Runtime (XAR)

Table 3: Unauthorized access via ADS or Secure ADS.

Countermeasures	Description
Technical	Use Secure ADS (see: Secure ADS): • Open only for defined remote stations • Firewall restriction • Static routes • Secure remote stations against manipulation
Organizational	• Replace accesses via Secure ADS with accesses via OPC UA.

Table 4: Influencing the real time via ADS / Secure ADS.

Countermeasures	Description
Technical	Use Secure ADS (see: Secure ADS): • Open only for defined remote stations • Firewall restriction • Static routes • Secure remote stations against manipulation
Organizational	• Replace accesses via Secure ADS with accesses via OPC UA.

7.3 Further technical information

This chapter summarizes further topics in a link collection, which concern the security of TwinCAT. Links are provided to further Beckhoff documentation that describes the respective topics in detail. The selection is a guide. It is intended as the first place to look and does not claim to be complete.

TwinCAT general	Further information
TwinCAT 3 Software Protection	https://infosys.beckhoff.com/english.php?content=../content/1033/tc3_security_management/index.html&id=355557539833111233
ADS	https://infosys.beckhoff.com/english.php?content=../content/1033/tc3_ads_intro/index.html&id=7262890787652929099
Disable ADS	https://infosys.beckhoff.com/english.php?content=../content/1033/secure_ads/6917981195.html&id=5745105416081707706
Secure ADS	https://infosys.beckhoff.com/english.php?content=../content/1033/secure_ads/index.html&id=2501949194726739202
ADS over MQTT	https://infosys.beckhoff.com/english.php?content=../content/1033/tc3_ads_over_mqtt/index.html&id=120186874503837909

OPC UA	Further information
Server-Security	https://infosys.beckhoff.com/content/1033/tf6100_tc3_opcua_server/15563113227.html?id=1035811638453978802
IO Client-Security	https://infosys.beckhoff.com/content/1033/tf6100_tc3_opcua_client/16622176779.html?id=5022570264195624057
Gateway Security	https://infosys.beckhoff.com/content/1033/tf6100_tc3_opcua_gateway/15626711307.html?id=1826922088201458894

8 Appendix

8.1 Further reading

IEC 62443 is a series of international standards for security in automation systems. Some individual sections are still under development. The parts that have already been published describe the organizational and technical concepts and measures for systems and components. URL: https://webstore.iec.ch/publication/7029

NIST SP800-82 Guide to Industrial Control Systems Security specifically describes the analysis of and measures against security threats to industrial facilities. URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

BSI IT Basic Protection Compendium offers structured function blocks for the analysis of risks and the application of measures. The compendium also contains function blocks relating to industrial IT. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

8.2 Advisories

Our Security Advisories are intended to help our customers protect their Beckhoff Industrial PCs and Embedded PCs against certain effects. The following table provides an overview of the available advisories regarding weak points in security and includes a link to download the document.

These Security Advisories are also provided as an RSS feed. In addition, Beckhoff publishes these advisories as part of CERT@VDE together with other manufacturers: https://cert.vde.com/de/advisories/vendor/beckhoff/.

If you suspect security weak points in one of our products, please inform us via the procedure described in the Coordinated Disclosure.

Number	Title	Version	Language	Download	External CNA
2025-003	Vulnerabilities in Beckhoff Device Manager	1.0	EN	PDF	HTML, CSAF
2025-002	XSS Vulnerability in TwinCAT 3 HMI Server	1.0	EN	PDF	HTML, CSAF
2025-001	Deserialization of untrusted data by TwinCAT 3 Engineering	1.0	EN	PDF	HTML, CSAF
2024-005	Local command injection via TwinCAT Package Manager	1.0	EN	PDF	HTML, CSAF
2024-004	Local Denial of Service issue in TwinCAT/BSD "MDP" package	1.0	EN	PDF	HTML, CSAF
2024-003	Local Denial of Service issue in TwinCAT/BSD package "IPC-Diagnostics"	1.0	EN	PDF	HTML, CSAF
2024-002	Improper neutralization of input in TwinCAT/BSD package "IPC-Diagnostics-www"	1.0	EN	PDF	HTML, CSAF
2024-001	Local authentication bypass in TwinCAT/BSD package "IPC-Diagnostics"	1.0	EN	PDF	HTML, CSAF
2023-001	Open redirect in TwinCAT/BSD package "authelia-bhf"	1.0	EN	PDF	HTML
2022-001	Null Pointer Dereference vulnerability in products with OPC UA technology	1.0	EN	PDF	HTML
2021-003	Relative path traversal vulnerability through TwinCAT OPC UA Server	1.0	EN	PDF	HTML
2021-002	Stack Overflow and XXE vulnerability in various OPC UA products	1.0	EN	PDF	HTML
2021-001	DoS Vulnerability for TwinCAT OPC UA Server and IPC Diagnostics UA Server	1.2	EN	PDF	HTML
2020-003	Privilege Escalation through TwinCAT System Tray (TcSysUI.exe)	1.1	EN	PDF	HTML
2020-002	EtherLeak in TwinCAT RT network driver	1.1	EN	PDF	HTML
2020-01	BK9000 couplers – Denial of service inhibits function	1.0	EN	PDF	HTML
2019-07	Denial-of-Service on TwinCAT using Profinet protocol	1.1	EN	PDF	HTML
2019-06	CE Remote Display behaves incorrectly with wrong credentials	1.2	EN	PDF	
2019-05	Remote Code Execution in Remote Desktop Service ("Dejablue")	1.0	EN	PDF	
2019-04	ADS Discovery	1.1	EN	PDF	
2019-03	Remote Code Execution in Remote Desktop Service	1.4	EN	PDF	
2019-02	Microarchitectural Data Sampling (MDS) vulnerabilities	1.2	EN	PDF	
2019-01	Spectre-V2 and impact on application performance as well as TwinCAT compatibility	1.4	EN	PDF	
2018-02	Updates for OPC-UA components (Several Vulnerabilities)	1.0	EN	PDF	
2018-01	TwinCAT 2 and 3.1 Kernel Driver Privilege Escalation	1.1	EN	PDF	

Number	Title	Version	Language	Download	External CNA
2017-02	Add Route using "Encrypted Password" bases on fixed key	1.3	EN	PDF	
2017-01	ADS is only designed for use in protected environments	1.4	EN	PDF	
2015-001	Potential misuse of IPC Diagnostics version < 1.8 backend	1.1	EN	PDF	
2014-003	Recommendation to change default passwords	1.1	EN	PDF	
2014-002	ADS communication port allows password bruteforce	1.1	EN	PDF	
2014-001	Potential misuse of several administrative services	1.1	EN	PDF	

8.3 Support and Service

Beckhoff Support and Service provides assistance with questions regarding Beckhoff products and system solutions, as well as with their planning, commissioning, and operation.

Beckhoff subsidiaries and representative offices

Please contact your Beckhoff subsidiary or your representative office for local support and service for Beckhoff products. You can find the addresses of Beckhoff subsidiaries and representative offices at: www.beckhoff.com/worldwide.

For Beckhoff products and technologies, we offer Training programs, tutorials, and webinars.

Beckhoff Support

Beckhoff Support provides assistance with technical questions regarding the use, planning, programming, and commissioning of Beckhoff products.

☎ Hotline: +49 5246 963-157
✉ Email: support@beckhoff.com, Support form
Web page: www.beckhoff.com/support

Beckhoff Service

Our service specialists are here to assist you with any questions you may have regarding after-sales service processes, such as replacement parts, repairs, etc.

☎ Hotline: +49 5246 963-460
✉ Email: service@beckhoff.com, Service form
Web page: www.beckhoff.com/service

Download finder

The Download finder serves as a central source for downloadable documents and files related to Beckhoff products, such as application reports, technical documentation, drawings, and configuration files.

Beckhoff Information System

The Beckhoff Information System is the central online documentation resource for Beckhoff products and contains documentation on products and automation topics, as well as sample code.

Beckhoff Headquarters

Beckhoff Automation GmbH & Co. KG
Hülshorstweg 20
33415 Verl, Germany

☎ Phone: +49 5246 963-0
✉ Email: info@beckhoff.com
Web page: www.beckhoff.com

List of tables

List of figures

Trademark statements

Beckhoff®, ATRO®, EtherCAT®, EtherCAT G®, EtherCAT G10®, EtherCAT P®, MX-System®, Safety over EtherCAT®, TC/BSD®, TwinCAT®, TwinCAT/BSD®, TwinSAFE®, XFC®, XPlanar® and XTS® are registered and licensed trademarks of Beckhoff Automation GmbH.

Third-party trademark statements

CFast is a registered trademark of CompactFlash Association.

Excel, IntelliSense, Microsoft, Microsoft Azure, Microsoft Edge, PowerShell, Visual Studio, Windows and Xbox are trademarks of the Microsoft group of companies.

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Modbus is a registered trademark of Schneider Electric USA, Inc.

OPC UA is a registered trademark of the OPC Foundation.

Beckhoff Automation GmbH & Co. KG
Hülshorstweg 20
33415 Verl
Germany
Phone: +49 5246 9630
info@beckhoff.com
www.beckhoff.com