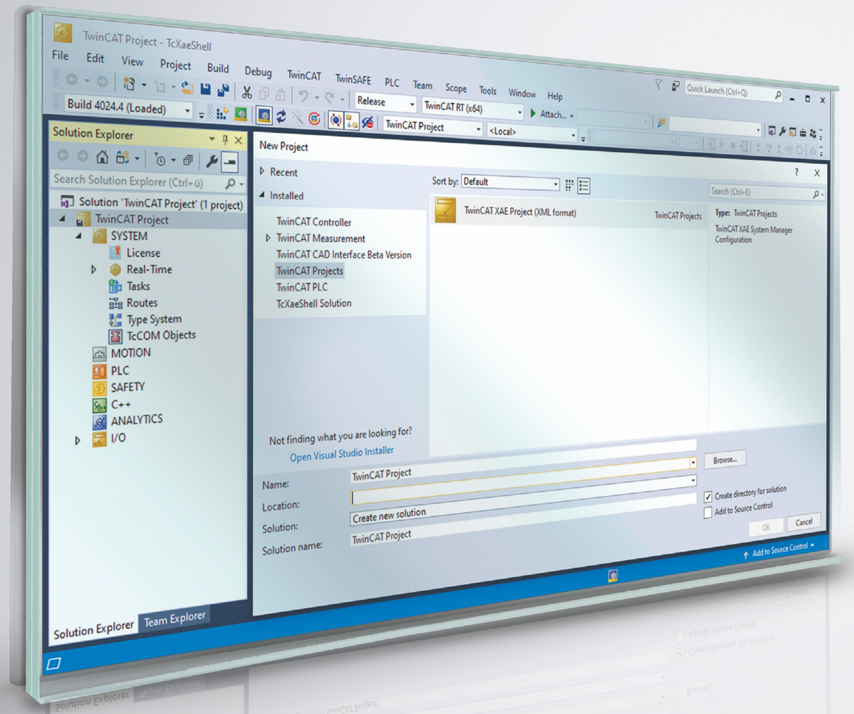
BECKHOFF New Automation Technology

Manual | EN

IPC Security Guideline

for TwinCAT/BSD



2024-03-28 | Version: 1.1

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.
For installation and commissioning of the components, it is absolutely necessary to comply with the documentation and the following notes and explanations.
The qualified personnel is always obliged to use the currently valid documentation.

The responsible staff must ensure that the application or use of the products described satisfies all safety requirements, including all the relevant laws, regulations, guidelines, and standards.

Disclaimer

The documentation has been prepared 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.
No claims to modify products that have already been supplied may be made on the basis of the data, diagrams, and descriptions in this documentation.

Trademarks

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

Patents

The EtherCAT Technology is covered by the following patent applications and patents, without this constituting an exhaustive list:
EP1590927, EP1789857, EP1456722, EP2137893, DE102015105702
and similar applications and registrations in several other countries.

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

Copyright

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 the ID `B4 F4 15 9A` and the 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 the ID `43 7E 2F D4 C5 01 A3 76 7D C2 31 9B` and the fingerprint `EE 3C 29 C3 BA BC 4F D6 43 BE D1 B2 6B 0E 4A FD 22 CF 4E E0`

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

Working hours

The Incident Response Team normally works between 9:00 and 17:00 and not on 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's Industrial PC (IPC) hardware has been designed for general use like a normal PC for office environments but with significant robustness added for use within industrial environments. The complete board has been designed for reliable and highly deterministic operation within such environments. Still the hardware supports general purpose operating systems like Windows® and TwinCAT/BSD which is based on FreeBSD. Consequently, the hardware is designed to support conventional and office-IT grade security mechanisms as provided by the operating systems. It is the duty of the one who integrates the IPC into an operational environment to configure these security features appropriately for the specific environment. Also, that person needs to provide guidance on secure use to the operator. Such configuration and usage guidelines should be the result from or be conformant with a holistic security concept for the specific environment.

Beckhoff's IPCs can be ordered with and without an operating system. Among these operating systems Windows 10 and TwinCAT/BSD are available. These are provided in a way which is called "secure by default" unless specifically ordered otherwise. This means, that only services are enabled with the default configuration such that all access to the device is authenticated and the only pre-configured user is one for administrative access. For historical reasons, the pre-configured user is "Administrator". Beckhoff offers the named operating system images pre-installed on the IPC in two fashions: One fashion has a random password pre-set for "Administrator" which can be read from a label on the device. The second fashion has the well-known password preconfigured for this as documented. Please note: The latter is not "secure by default" with respect to the requirements of some environments while it serves well for others.

The named operating systems are not developed by Beckhoff. The basis of Beckhoff's Windows 10 images is developed and maintained by Microsoft Corporation. The basis of TwinCAT/BSD is developed and maintained by "The FreeBSD Project". Both bases are well reputed regarding their security features since decades for use in office and server environments. They contain and provide state of the art security features. Specific environments and applications have specific needs for the configuration and use of these security features. Because Beckhoff provides the named operating systems for general purpose use and does not want to restrict which applications are implemented by this, Beckhoff cannot foresee the specific security needs which emerge from specific use or integration. Guidance on the secure configuration and use thus needs to be created by the one who integrates the operating system into an environment for specific use. Nonetheless, Beckhoff provides guidance on how to use the IPC and its operating system securely within this guide. Such guidance is to be considered as general hint and not as a complete and sufficient reference. The developers of the operating systems provide complete documentation for the security features of the operating systems.

Beckhoff created extensions to these operating systems, especially to optimize the deterministic behavior of the operating system for use with real-time applications of the automation industry. The extensions are integrated in operating system images distributed by Beckhoff. For those extensions robustness and determinism for availability is the primary target of their design. Still, Beckhoff cares that these extensions do not compromise the security features of the basis of the operating system unless noted otherwise.

Beckhoff distributes a high variety of software products. One example is the product “TwinCAT 3.1 – eXtended Automation Runtime (XAR)”, which is called TwinCAT 3.1 XAR in short. For some IPCs this can be ordered pre-installed within the operating system. The primary purpose of this specific software is to provide a deterministic and robust but highly customizable runtime for automation applications. When it is installed on an IPC then it turns that device into a Programmable Logic Controller (PLC). Besides availability (through robustness and determinism) the software has been added with perimeter security during its development. This means that it can be configured and used in a way that it securely authenticates access through the protocols which are implemented by TwinCAT 3.1 XAR. The perspective for this perimeter security is that the network interfaces of the IPC mark the boundary. The security risk identified by Beckhoff for this kind of security is that an unauthorized user gets access to the IPC via protocols implemented by TwinCAT 3.1 XAR. For historical reasons and backward compatibility TwinCAT 3.1 XAR still provides protocols which do not authenticate before such access. Some IPCs with TwinCAT 3.1 XAR pre-installed have a configuration for TwinCAT 3.1 XAR which is secure by default. That means that this default configuration enables only secure protocols of TwinCAT 3.1 XAR. Please note that lots of IPCs which are shipped with TwinCAT 3.1 XAR pre-installed do not have a configuration which is secure by default for backward compatibility. This security guide contains a complete list of the protocols which are supported by TwinCAT 3.1 XAR and advises about which are secure, please see: Important TCP/UDP ports [▶ 33]. The other software products come with their own documentation and guides. Please note: The latter is true also for TwinCAT functions which can be added via separate installer to TwinCAT 3.1 XAR.

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.

Category	Description
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 [▸ 30])
- Locked control cabinet [▸ 14]
- Disable interfaces in BIOS (BIOS settings [▸ 16])
- Whitelisting for programs [▸ 28]

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 [▸ 23]
- 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 [▸ 14]

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

Attack type/attacker	Insider	Local	Internal network	Remote
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 [▶ 14]

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 [▶ 22])
- Whitelisting for programs [▶ 28]

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 [▶ 22])
- Network-based detection mechanisms (IDS/IPS)
- Disabling unneeded services
- Removing components that are no longer needed [▶ 28]

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 [▶ 22])
- 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 [▶ 28]

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 Secure data destruction

In the case of scrapped or decommissioned components, it is important to reliably destroy the data. Multiple overwriting of the data carrier is a suitable and reliable method.

For the secure destruction of data on discarded or decommissioned components, it is recommended to overwrite the data carriers. To do this, boot the device from the TwinCAT/BSD installer stick. If the device does not automatically boot from the stick, press F7 during the boot process to select the USB flash drive. In the menu of the installer stick, the TwinCAT/BSD shell of the installer stick can now be accessed via the menu item "Shell". With

```
ls /dev
```

you can display the device nodes found or the data carriers found. Data carriers are usually indicated with ada0 or da0, where "ada" stands for Sata data carriers and "da" for SCSI data carriers. CFast cards are thus listed as "ada", USB flash drives as "da".

If the data on the CFast card of the device is to be irretrievably destroyed, proceed as follows to overwrite the data carrier with zeros:

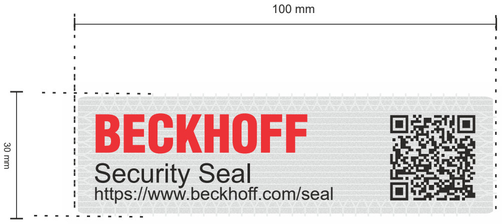
```
dd if=/dev/null of=/dev/ada0 bs=100m
```

Physical destruction

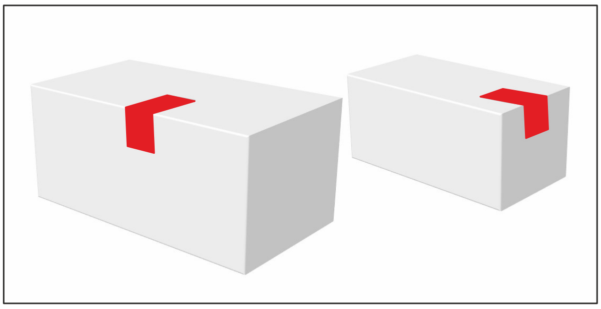
If you don't wish to overwrite a hard disk or cannot do so due to a defect, you should physically damage or destroy the hard disk.

3.4 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 TwinCAT/BSD system in order to restore TwinCAT/BSD 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 stored should be defined.

Beckhoff offers a simple backup solution with the TwinCAT/BSD installer stick. In addition, the `restorepoint` program makes restore points possible with TwinCAT/BSD; these restore points store the current state of the system and restore it if necessary. A variety of implementations are therefore available, with the exact definition of a backup and restore strategy left to the user.

The following scenarios are possible and are intended to help you understand the different modes of operation. However, the scenarios presented should not be considered the only way recommended by Beckhoff.

Scenario 1: Factory settings

An Industrial PC with TwinCAT/BSD is to be reset to the factory settings in case of a problem.

- The user tests and develops on an Industrial PC with TwinCAT/BSD.
- In the test and development phase, there is a problem because, for example, basic settings have been changed.
- The user solves the problem by resetting TwinCAT/BSD to the factory settings (see:Resetting to factory settings [▸ 18]).

Scenario 2: Series production

The test and development phase has been successfully completed. The machine manufacturer wants to start series production:

- The machine manufacturer creates a restore point (delivery state OEM) in order to be able to restore the system in the event of an error (see: Creating a restore point [▸ 18]. The machine manufacturer's end customer can use this restore point in case of problems.
- The machine manufacturer then activates the Write Filter to secure TwinCAT/BSD in the preconfigured state and to prevent a misconfiguration at the end customer (see: Write filter [▸ 29]).
- In the final step, the machine manufacturer creates a backup, which is stored as a master image and used for series production (see: Creating a backup [▸ 20]).

Scenario 3: Commissioning at the end customer

The machine arrives at the end customer and is to be backed up after commissioning:

- After parameterizing the machine, the end customer creates a restore point called "Commissioning" (see: Creating a restore point [▸ 18]).
- The end customer then activates the Write Filter in order to avoid accidental misconfiguration (see: Write filter [▸ 29]).
- The end customer creates his own backup (see: Creating a backup [▸ 20]) in order to be able to restore the system, for example, in the event of a defective data carrier (see: Restoring a backup [▸ 21]).

5.1.1 Restore point

Restore points are used to restore an old system state if TwinCAT/BSD exhibits undesirable behavior after a major system change or misconfiguration, and this behavior is not easy to rectify. The advantage of restore points is that these configuration errors are easily and quickly undone without reinstalling TwinCAT/BSD.

You define the time to create a restore point, for example, when you make a larger system change or install third-party programs. However, restore points are not a substitute for a full backup and do not protect against data loss. Regular backups are another protection measure that allows you to protect yourself from data loss due to defective storage media, for example (see: Creating a backup [▶ 20]).

The restore points are created and managed in the console using the `restorepoint` program. The following modes are supported by the program:

- `status`: Lists all available restore points. On delivery, a restore point named `factoryreset`, the Beckhoff factory settings, is available.
- `create`: Creates a new restore point. The name of the restore point can be set as an argument. If no name is specified, an automatically generated name is used.
- `rollback`: Return to a specific restore point. Note that all data created after the restore point will be destroyed. If no restore point is specified as an argument, the user is asked with an interactive dialog.
- `destroy`: The specified restore point is destroyed. In this mode, all existing data is preserved, but the restore point itself is deleted.

Restore points under TwinCAT/BSD are based on ZFS snapshots. As a result, they consume very little memory when they are created. Any change in the saved restore point for the current live system the user is working with is reflected in the memory space used by the restore point. Use `zfs list -t snap` to display all system snapshots.

The USED column shows the actual space used by the snapshot; the REFER column shows the space referenced by the snapshot but actually stored in other datasets. It is therefore always advisable to create a restore point before making any changes in the system, since this hardly uses any system resources. After some time and many changes between the restore point and the live system, it is recommended to delete restore points that are no longer needed in order to free up the increasing memory space used by the restore points.

5.1.1.1 Resetting to factory settings

You can reset TwinCAT/BSD to the factory settings at any time and restore the delivery status if, for example, the system no longer works properly after a misconfiguration.

The restore points are created and managed in the console using the `restorepoint` program. This section shows you how to reset TwinCAT/BSD to the factory settings.

Proceed as follows:

1. Enter the command `doas restorepoint rollback factoryreset` on the console.
2. All snapshots to which the system is reset are displayed.
3. Confirm the restoration with **[y]**.

⇨ The system is reset to the factory settings. After a restart, TwinCAT/BSD is in the delivery state again.

5.1.1.2 Creating a restore point

Memory consumption due to restore points

A restore point consumes storage space because the entire system is backed up, including kernel dumps at /`var/crash`. Clean up the system before creating a restore point or delete old restore points.

Restore points are used to restore an old system state if TwinCAT/BSD no longer works properly after a major system change or misconfiguration. Create restore points when you want to make major system changes, install programs or run tests.

The restore points are created and managed in the console using the `restorepoint` program. This section shows you how to create restore points in TwinCAT/BSD.

Proceed as follows:

1. Enter the command `doas restorepoint create` in the console.

2. The restore point is created with an automatically generated name.
3. Check the creation of the restore point with the command `restorepoint status` and have all restore points displayed.

```
Administrator@CX-4FAA38$ restorepoint status
last BE: zroot/ROOT/default
factoryreset
2020-08-28T08:56:14Z
2020-08-28T09:03:05Z
```

4. Alternatively, use the command `doas restorepoint create your-restorepoint` in order to define your own name for the restore point.

⇨ The restore point is created and can be used at any time to reset the system (see: Resetting to the restore point [▶ 19]).

```
Administrator@CX-4FAA38$ restorepoint status
last BE: zroot/ROOT/default
factoryreset
2020-08-28T08:56:14Z
2020-08-28T09:03:05Z
your-restorepoint
```

5.1.1.3 Resetting to the restore point

NOTICE

Loss of data

Data and restore points created after a certain restore point are deleted when resetting to a previous restore point.

If TwinCAT/BSD no longer works properly after a misconfiguration, you can easily undo these configuration errors with the help of restore points without reinstalling TwinCAT/BSD.

Proceed as follows:

1. Enter the command `restorepoint status` on the console to display all the restore points that can be used.

```
Administrator@CX-4FAA38$ restorepoint status
last BE: zroot/ROOT/default
factoryreset
2020-08-28T08:56:14Z
2020-08-28T09:03:05Z
your-restorepoint
```

2. Enter the command `doas restorepoint rollback` in the console to see all existing restore points.
3. Select a menu item to reset the system to a specific restore point.

```
Administrator@CX-4FAA38~ $ doas restorepoint rollback
Password:
    1 factoryreset
    2 2020-08-28T08:56:14Z
    3 2020-08-28T09:03:05Z
    4 your-restorepoint
```

4. All snapshots to which the system is reset are displayed.
5. Confirm the restoration with **[y]**.

⇨ TwinCAT/BSD is reset to the restore point and restarted. Note that data and restore points created after the selected restore point are deleted during the reset.

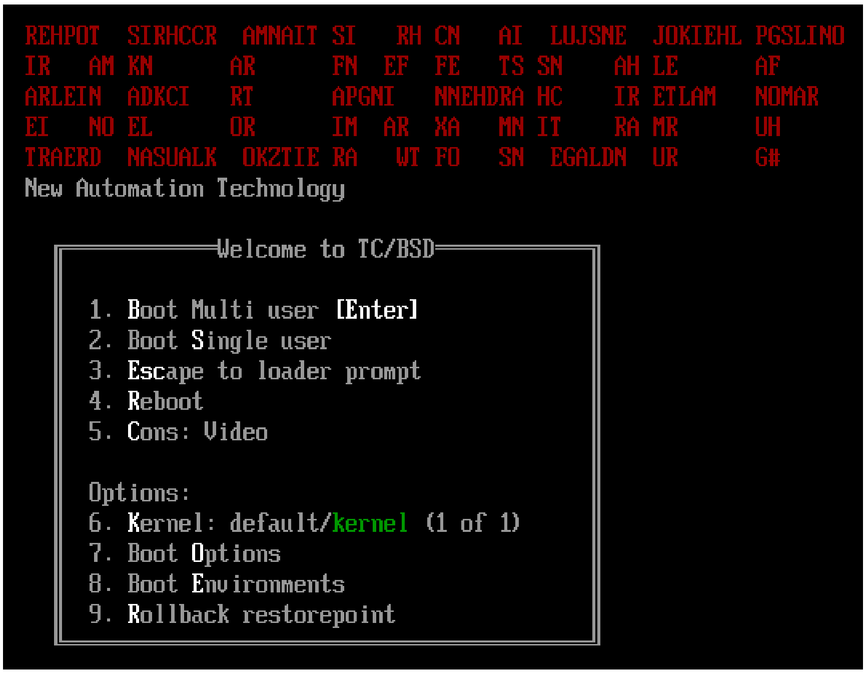
5.1.1.4 Using the restore boot environment

You can restore a restore point from the restore boot environment when TwinCAT/BSD no longer boots and the console is inaccessible as a result. To do this, start the boot menu during the boot process in order to switch to the restore boot environment.

Proceed as follows:

1. Start the Industrial PC.

2. During the bootup, press and hold the **[Space bar]**. The boot menu appears.



```
REHPOT  SIRHCCR  AMNAIT SI   RH CN   AI  LUJSNE  JOKIEHL PGSLINO
IR   AM KN       AR     FN  EF  FE   TS SN    AH LE      AF
ARLEIN  ADKCI    RT     APGNI   NNEHDRA HC    IR ETLAM   NOMAR
EI   NO EL       OR     IM  AR  XA   MN IT    RA MR      UH
TRAERD  NASUALK  OKZTIE RA   WT FO   SN  EGALDN  UR      G#
New Automation Technology

    ╔════════════Welcome to TC/BSD═════════════╗
    ║                                          ║
    ║  1. Boot Multi user [Enter]              ║
    ║  2. Boot Single user                     ║
    ║  3. Escape to loader prompt              ║
    ║  4. Reboot                               ║
    ║  5. Cons: Video                          ║
    ║                                          ║
    ║  Options:                                ║
    ║  6. Kernel: default/kernel (1 of 1)      ║
    ║  7. Boot Options                         ║
    ║  8. Boot Environments                    ║
    ║  9. Rollback restorepoint                ║
    ╚══════════════════════════════════════════╝
```

3. Select the option **Rollback restorepoint**.

⇨ TwinCAT/BSD starts in the restore boot environment. Now you can restore the factory settings with the command `restorepoint rollback factoryreset` or use a specially created restore point (see: Resetting to the restore point [▶ 19]).

5.1.2 Backup and restore

Unlike a restore point, TwinCAT/BSD can be saved and managed as a backup copy on an external storage device by means of a backup.

This backup copy can be used to restore the system in the event of a system failure or data loss. Make regular backups from your system in order to restore your industrial PC to the state it was at the time of the backup.

5.1.2.1 Creating a backup

You can create and restore a backup using the TwinCAT/BSD installer stick. All backups are stored on a FAT32 partition on the USB stick. FAT32 is interoperable with Windows and FreeBSD. This allows the backups created to be managed both with a TwinCAT/BSD system and with a Windows system.

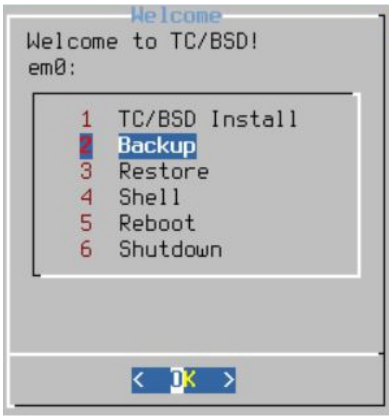
Requirements:

- TwinCAT/BSD installer stick (see: Create bootable USB stick).

Create a backup as follows:

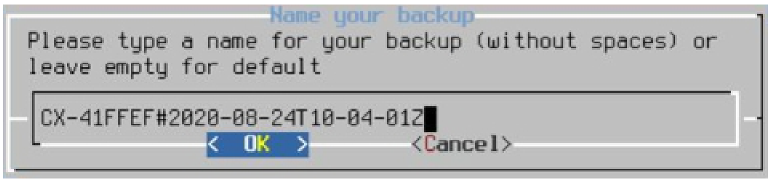
1. Connect the TwinCAT/BSD installer stick to the Industrial PC.
2. Boot the Industrial PC from the TwinCAT/BSD installer stick.
3. Open the boot menu with **[F7]** if the Industrial PC doesn't boot automatically from the USB stick.
4. Select the UEFI entry for the USB stick and confirm with **[Enter]**. The Industrial PC boots from the USB stick and the Beckhoff TwinCAT/BSD installer is run.

5. Select the option **Backup**.



```
Welcome
Welcome to TC/BSD!
em0:
```

6. Assign a file name to the backup or accept the default name made up of host name and timestamp.



```
Name your backup
Please type a name for your backup (without spaces) or
leave empty for default
CX-41FFEF#2020-08-24T10-04-01Z
```

7. Select the option **Reboot** for a reboot once the backup is complete.

⇨ The backups are stored on the USB stick with the respective file name. Archive the backups on the USB stick. You can also copy the backups to an external storage medium or archive them on the network.

5.1.2.2 Restoring a backup

Use suitable backups to restore

A backup can only be restored to one device within the same series, e.g. CX51x0, CX20x3, C6015 etc., otherwise incompatibilities may occur if the backup is restored to a device from a different series.

You can restore a backup with the aid of the TwinCAT/BSD installer stick. To do this, the industrial PC must be booted from the TwinCAT/BSD installer stick.

Requirements:

- TwinCAT/BSD installer stick (see: Create bootable USB stick).

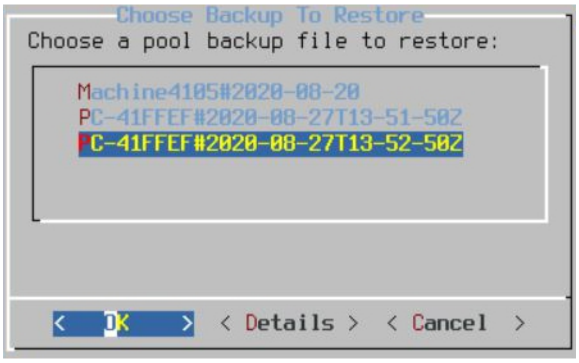
Proceed as follows:

1. Connect the TwinCAT/BSD installer stick to the industrial PC.
2. Boot the industrial PC from the TwinCAT/BSD installer stick.

Open the boot menu with [F7] if the industrial PC doesn't boot automatically from the USB stick.

3. Select the UEFI entry for the USB stick and confirm with **[Enter]**. The industrial PC boots from the USB stick and the Beckhoff TwinCAT/BSD installer is run.
   Select the **Restore** option.

4. Select the backup to be restored to the industrial PC.



Choose Backup To Restore

Choose a pool backup file to restore:

```
Machine4105#2020-08-20
PC-41FFEF#2020-08-27T13-51-50Z
PC-41FFEF#2020-08-27T13-52-50Z
```

⇨ Restart the industrial PC after restoring. The industrial PC is now in the state it was at the time of the backup.

5.1.2.3 Creating and restoring a backup from the live system

If required by your application, backups can also be created and restored from the live system, without a TwinCAT/BSD installer stick. Use the scripts TcBackup and TcRestore for this purpose.

Do not create a backup from the running system if the system is writing to the disk at the time of the backup. A backup can become corrupted if the system has write access to the disk during the backup. In other words, make sure that there are no processes running that persistently back up data and that the disk you want to restore your backup to has enough space.

Running TcBackup and TcRestore and writing to and from the file where the backup is saved must be done with root rights. In other words, execute a shell with root rights beforehand, in which you then work, or execute the single command as a string with a shell with root rights. The latter option is illustrated in the following examples.

Proceed as follows:

1. Enter the command `doas sh -c "TcBackup.sh --disk /dev/ada0 > backup.tcbkp00"` to create a backup from the ada0 disk to the Backup.tcbkp00 file.
2. Enter the command `doas sh -c "TcRestore.sh --disk /dev/ada1 < backup.tcbkp00"` to restore a backup from the Backup.tcbkp00 file on the ada1 disk.

⇨ The two commands can be combined, as follows. The command `doas sh -c "TcBackup.sh --disk /dev/ada0 | TcRestore.sh --disk /dev/ada1"` creates a backup from the ada0 disk and immediately restores it to the ada1 disk.

5.2 Updates

Regular updates are important because they close dangerous security holes in particular. The open source community usually closes known security holes very quickly. This advantage should be used and patches should be applied to the system promptly. Beckhoff provides updates for the basic system and for many programs via the public Package Server that is preset in each system.

For a system update, you should proceed as follows:

1. If possible, first test the update in interaction with your own programs on test hardware.
2. Perform a backup of the system or create a restore point to restore the old system state in case of unforeseen behavior (See: Restore options [▶ 17]).
3. First display the packages that can be updated with `doas pkg upgrade -n` and then execute the update with `doas pkg upgrade <packagename>`.

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 `doas passwd`, you run the command with root rights, changing the password of the superuser account (`root`) and not those of the logged-in user. Do not run `passwd` with root rights.

When TwinCAT/BSD is delivered, a user (`Administrator`) is available by default, with which you can log in to the console. This user does not have conventional administrator rights like under Windows systems but has the authority to obtain 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 is displayed. For example: CX-1D7BD4.
4. Enter the command `passwd` in order to set a new password for TwinCAT/BSD. Follow the instructions.

⇨ You have successfully set a new password for TwinCAT/BSD.

5.3.1.2 Password policies

A separate password policy protects the system against 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 `/etc/pam.d/passwd` as follows:

```
doas ee /etc/pam.d/passwd
```

Remove the "#" at the beginning of the line

```
password requisite pam_passwdqc.so enforce=users
```

and add entries for the pam_passwdqc module as required:

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

Five values can be set behind `pam_passwdqc`, since five password categories are predefined for this module. Categories include password complexity requirements, such as combinations of special characters, lowercase and uppercase letters, and numbers. Each digit after `pam_passwdqc.s` can either be disabled or given a number for the required password length and represents one of the following password categories:

- Passwords of one character class are allowed, i.e. passwords consisting only of numbers or 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 password categories, e.g. lowercase and uppercase letters and numbers.
- Passwords consisting of four password categories, i.e. lowercase and uppercase letters as well as numbers and characters.

So the example shown only allows passwords consisting of four password categories and 10 characters. The "similiar" also defines whether a new password may be similar to the old password. "retry" describes how often `pam_passwdqc` prompts for a new password when the user fails to choose a new password according to the password policy.

For more information on configuring password policies, visit https://www.freebsd.org/cgi/man.cgi?query=pam_passwdqc

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, change the user's shell from sh to tcsh. The tcsh shell has already implemented an autologout, which can be defined afterwards:

```
chsh -s tcsh
```

```
ee ~/.login
```

Add the following line and specify the desired idle time until the auto-logout should be executed:

```
set -r autologout=1
```

Re-login with `login` for the changes to take effect.

5.3.3 Group and file permissions

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 Twin-CAT/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:

```
doas adduser
```

This will launch a wizard that will guide you through the user creation process. To edit a user, use `doas chpass <Benutzer>`

There are already some users that are shipped with the base system. In addition to the Administrator user, there are so-called system accounts. These accounts are not set up as interactive accounts and are only used to manage and run integrated programs.

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 "wheel" group can be granted root rights. The preconfigured user "Administrator" is a "Wheel" member and obtains root rights by placing the command `doas` in front of programs and authenticating again with his password.

Change the group memberships and create new groups by editing `/etc/group` with `doas ee /etc/group` accordingly.

This file shows 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.

Restricting the use of the system

You can use so-called logon classes to define system resources and information that are made available to users.

5.3.4 File flags

In addition to basic file permissions, FreeBSD provides file flags that add another security level to file control. Depending on the security level, which is explained in the chapter Securelevel [▶ 26], file flags have different effects. Below are some common file flags that help secure your system. A complete list of file flags can be found in the respective manual.

sappnd: Files marked with this flag cannot be edited or deleted, but it is allowed to append the content. This is useful, for example, for log files that can grow in this way but cannot be deleted by an attacker to make their intrusion more difficult. Sappnd can only be set with root rights and cannot be removed with Securelevel 1 or higher.

uppnd: Like sappnd, but besides root, the file owner can also set and remove this flag. Useful to prevent accidental deletion or modification of a file.

schg: Files marked with this flag cannot be edited, deleted or moved to another location. Schg can only be set with root rights and cannot be removed with security level 1 or higher.

uchg: Like schg, but besides root, the file owner can also set and remove this flag.

Set file flags with the command `chflags`, followed by the respective file flag and the file you want to protect: `doas chflags sappnd /pfad/zu/datei`

Delete file flags by placing a "no" in front of the file flag name: `doas chflags nosappnd /pfad/zu/datei`

One example of using file flags to make your system more secure is to protect your file system kernel from modification: `doas chflags schg /boot/kernel/kernel`

Note that the file flag must be cleared for system updates.

Use the `-R` option to set the file flag redundantly for directories and files in the folder you specify. You cannot remove all of your log files with the following command, but you and the system can still attach logs `doas chflags -R schg /var/log`

If you cannot easily remove file flags, then the system may be in a higher security level. By default TwinCAT/BSD is in security level -1, which provides no additional security for the system and allows file flags to be changed. In higher security levels it is not possible to change file flags.

5.3.5 Securelevel

Securelevels are security configurations that are set in the kernel. Changing the Securelevels defines how restrictive the system should be with regard to system changes.

Enable Securelevels at boot time by adding the following line to `/etc/rc.conf`:

```
kern_securelevel_enable="YES"
```

There are five Securelevels that you can switch between. The higher the Securelevel of your system, the more security features are added. Define the Securelevel by adding `kern_securelevel=2` in `rc.conf`. Here it has been configured to Securelevel 2. After a system restart, the change is active.

In the following the consequences for the system are described for the respective Securelevel:

-1: Default, no additional kernel security.

0: A system that is set to Securelevel "0" only boots with Securelevel "-1" and automatically switches to Securelevel "1" when it reaches multi-user mode (standard operation mode). This is recommended if autostart scripts are used whose execution would be forbidden at Securelevel 1.

1: Provides some basic security functions:

- File flags cannot simply be turned off (see: File flags [▶ 26]).
- The user cannot load and unload kernel modules.
- Programs cannot write to memory via devicenodes (`/dev/mem` and `/dev/kmem`).
- Devicenode `/dev/io` cannot be addressed.
- Debugging and panic of the system via the program `sysctl` is disabled.
- Writing to raw disk devices is prohibited.

2: Properties of "1" with additional properties:

- User cannot write to raw disk devices via devicenode.
- It is forbidden to change the system time by more than one second

3: Includes the features of security levels 1 and 2 and provides additional network security:

- Editing firewall rules is disabled.

Select the appropriate Securelevel

The choice of the Securelevel depends on your needs. If you are constantly making changes and need a flexible system, do not change anything and leave the default Securelevel (-1) active. If you hardly have to configure the system and the system is to be used in a productive environment, it is recommended to set the Securelevel higher. For systems in a production environment that do not require any further system changes, security level 2 is recommended. If your network is also already set and no further firewall changes are required, you can increase the Securelevel to 3.

5.3.6 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 accesses as well as user entries can be logged in TwinCAT/BSD. 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.

Have the audit daemon start automatically after each system start:

```
doas ee /etc/rc.conf
```

```
auditd_enable="YES"
```

Start the audit daemon for the current session:

```
doas service auditd start
```

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

`/etc/security/audit_control`: General, system-wide audit settings.

In the default settings, the audit logs are stored in `/var/audit`, when 5% of the memory is used for audit files, a warning message appears and after 10 months the audit logs are removed.

With `zroot/var/audit` there is already a separate ZFS dataset for the audit logs. It is advisable to set a quota, i.e. a memory limit, for this dataset. Even in the standard audit configuration, large amounts of data can already be generated - even when taking into account the automatic deletion of the audit logs after 10 months. To limit the storage limit of this dataset and thus ensure free storage for the other, important datasets, the following command can be used to limit the storage space for audit logs to, for example, 2 GB:

```
doas zfs set quota=2G zroot/var/audit
```

Alternatively, or in addition to this measure, the time period until the audit logs are deleted can be shortened in /etc/security/audit_control.

```
doas ee /etc/security/audit_control
```

```
expire-after:10M □ expire-after:2M
```

`/etc/security/audit_user`: Audit settings for individual users

Here, separate audit rules can be defined for individual users. A detailed description of audit rules and a list of options for defining audit rules for users can be found in the FreeBSD Handbook: https://docs.freebsd.org/en/books/handbook/audit/

5.4 Programs

5.4.1 Whitelisting for programs

Application whitelisting, such as is available for Windows with Applocker or so-called software restriction policies (SRP), is not available for TwinCAT/BSD. For Unix systems there are different approaches to realize an application whitelisting. These are less popular compared to Windows. The reason for this is an increased complexity due to command line and scripts in Unix compared to the mostly graphical input under Windows. Instead, pay close attention to the source of the packages and check what packages are installed on the system (see: Removing components that are no longer needed [▶ 28]).

5.4.2 Removing components that are no longer needed

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

The removal of system components should only be done by well-versed persons. Negative side effects may occur and programs can no longer be run correctly.

With `pkg info` 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. In addition to packages for TwinCAT with the abbreviation TC, the Beckhoff IPC diagnostics and packages for the basic system that begin with "os-generic", dependencies, i.e. programs that are required by other programs, are also located here.

If you delete a package that is a dependency of another package, the system asks you whether you also want to delete the associated packages. This allows you to determine if a package is a dependency of a package that is still installed. Packages that you know are no longer needed can be deleted with `doas pkg delete <pkg-name>`. Afterwards, the command `doas pkg autoremove` can be used to delete all dependencies that are no longer needed. This ensures that no packages that are no longer needed remain on the system.

5.4.3 Package audit

The Package Tool, which is used for installing and updating software under TwinCAT/BSD, has an audit function for checking installed software for known vulnerabilities.

```
doas pkg audit -F
```

The command downloads the list of known vulnerabilities and compares it with the local packages. You will receive the CVE number (Common Vulnerabilities and Exposures) and a link to more information about the vulnerability.

5.4.4 Antivirus programs

Antivirus programs do not appear to be necessary for TwinCAT/BSD and UNIX systems in general, because malicious software for UNIX systems tends to be rare. Viruses for Unix 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 TwinCAT/BSD, 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. Spreading over the system is not easily possible due to the strict rights management.

However, security holes must be closed by 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 Unix 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 level to the system. For TwinCAT/BSD, 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 Write filter

TwinCAT/BSD has a write filter that protects certain data sets against write access. The advantage of a write filter is that the user can secure a system in a preconfigured state. Following a restart, the system is automatically reset to the originally defined state.

The dataset `zroot/ROOT/default`, which contains most of the system and TwinCAT, is protected against write accesses when the Write filter is active. No other data sets are covered by the Write filter. For example, user files can still be persistently stored at `/home` or log files at `/var/log`, even if the rest of the system is reset after a restart.

5.5.1 Enabling or disabling the write filter

This step shows how to enable or disable a write filter under TwinCAT/BSD. Note that the changes to the write filter only take effect after a restart.

Proceed as follows:

1. Enter the command `doas service bwf enable` in the console to enable the write filter.
2. Confirm the command with the administrator password.

   ```
   Administrator@CX-3D6912:~ $ doas service bwf enable
   Password:
   bwf_enable: NO -> YES
   writefilter enabled, please reboot to make your changes take effect.
   ```
3. Restart the Industrial PC with `shutdown -r now` to apply the settings.

⇨ The write filter is active after the restart. The write filter is deactivated again with the command `doas service bwf disable`.

5.5.2 Defining exceptions

Exceptions for the write filter can be defined by creating new datasets, since only the dataset `zroot/ROOT/default` is protected from write accesses; all other system datasets, including newly created datasets, are excluded from the protection.

This chapter shows an example of how a separate dataset can be created for the TwinCAT boot directory, thereby excluding this directory from the write filter protection.

Requirements:

- Save the TwinCAT boot directory in advance if you follow this example.
- Disable the write filter (see Enabling or disabling the write filter [▶ 29]).

Proceed as follows:

1. Enter the command `doas rm -rf /usr/local/etc/TwinCAT/3.1/Boot/*`.
2. The directory `usr/local/etc/TwinCAT/3.1/Boot` is detached from the file hierarchy.
3. Enter the command `doas zfs create -o mountpoint=/usr/local/etc/TwinCAT/3.1/Boot zroot/usr/TwinCAT-Boot` to mount the new dataset `zroot/usr/TwinCAT-Boot`.

⇨ You have successfully created a new dataset for the TwinCAT boot directory. Use `zfs mount` to display all mounted datasets, including the new dataset `zroot/usr/TwinCAT-Boot`. From now on, all directories below this directory are no longer protected from write access by an active write filter.

5.6 USB filter

For security reasons, USB storage devices are not mounted automatically. You must link them manually for each session or configure automatic linking. Both are described in the TwinCAT/BSD documentation.

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 [▶ 33] .

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 [▶ 32]

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 additionally installed software, part of the operating system or a self-contained device. Each of these forms has advantages and disadvantages. For example, unlike an external firewall, with a firewall that is part of the operating system rules for programs can be configured, but it is also easier for malware to modify and activate or deactivate it.

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

TwinCAT/BSD uses packet filters (PF) as a firewall. This is part of the FreeBSD base system and is a system for filtering TCP/IP network traffic. In addition, other network-relevant settings such as NAT and port forwarding can be made.

By default, the system is hardened pre-configured and only a few encrypted connections are allowed. For example, ADS port 48898 is blocked ex factory and only ADS Secure is allowed on port 8016. Further ports required by TwinCAT functions and other Beckhoff applications are opened dynamically in the firewall. Furthermore, SSH, HTTPS and Ping are allowed through the firewall.

With `cat /etc/pf.conf` the general firewall rules are output.

`cat /etc/pf.conf.d/bhf` is used to output the firewall rules that are relevant for Beckhoff applications.

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 application 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)
IPC diagnostics	https: 443 / tcp
Remote Desktop – RDP (Windows 7/10 only)	3389 / tcp
TwinCAT ADS	Discovery: 48899 / udp (also outgoing) Not secured: 48898 / tcp (also outgoing). Port under TwinCAT/BSD® closed Secure ADS: 8016 / tcp (also outgoing)

Further services

The table below provides an overview of frequently used services that can additionally be opened

Service	Ports (incoming)
SMB	137-139 / tcp 445 / tcp OPC-UA: 4852 / tcp
Cerhost (Windows CE)	987 / tcp
FTP	21 / tcp

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 / tcp (local) 1020 / 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

Service	Port (default setting)
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

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

Countermeasures	Description
	• 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/english.php?content=../content/1033/tf6100_tc3_opcua/1448394251.html&id=2325029100913163478
IO Client-Security	https://infosys.beckhoff.com/english.php?content=../content/1033/tf6100_tc3_opcua/1452984075.html&id=
PLCLib Client Security	https://infosys.beckhoff.com/english.php?content=../content/1033/tf6100_tc3_opcua/1452984075.html&id=7305736008379229744
Gateway Security	https://infosys.beckhoff.com/english.php?content=../content/1033/tf6100_tc3_opcua/1452984075.html&id=954414165455750259

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 URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_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 and includes a link to download the document.

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

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

Number	Title	Version	Language	Download
2023-001	Open redirect in TwinCAT/BSD package “authelia-bhf”	1.0	EN	Link
2022-001	Null Pointer Dereference vulnerability in products with OPC UA technology	1.0	EN	Link
2021-003	Relative path traversal vulnerability through TwinCAT OPC UA Server	1.0	EN	Link
2021-002	Stack Overflow and XXE vulnerability in various OPC UA products	1.0	EN	Link
2021-001	DoS-Vulnerability for TwinCAT OPC UA Server and IPC Diagnostics UA Server	1.2	EN	Link
2020-003	Privilege Escalation through TwinCAT System Tray (TcSysUI.exe)	1.1	EN	Link
2020-002	EtherLeak in TwinCAT RT network driver	1.1	EN	Link
2020-01	BK9000 couplers - Denial of service inhibits function	1.0	EN	Link
2019-07	Denial-of-Service on TwinCAT using Profinet protocol	1.1	EN	Link
2019-06	CE Remote Display behaves incorrectly with wrong credentials	1.2	EN	Link
2019-05	Remote Code Execution in Remote Desktop Service ("Dejablue")	1.0	EN	Link
2019-04	ADS Discovery	1.1	EN	Link

Number	Title	Version	Language	Download
2019-03	Remote Code Execution in Remote Desktop Service	1.4	EN	Link
2019-02	Microarchitectural Data Sampling (MDS) vulnerabilities	1.2	EN	Link
2019-01	Spectre-V2 and impact on application performance as well as TwinCAT compatibility	1.4	EN	Link
2018-02	Updates for OPC-UA components (Several Vulnerabilities)	1.0	EN	Link
2018-01	TwinCAT 2 and 3.1 Kernel Driver Privilege Escalation	1.1	EN	Link
2017-02	Add Route using "Encrypted Password" bases on fixed key	1.3	EN	Link
2017-01	ADS is only designed for use in protected environments	1.4	EN	Link
2015-001	Potential misuse of IPC Diagnostics version < 1.8 backend	1.1	EN	Link
2014-003	Recommendation to change default passwords	1.1	EN	Link
2014-002	ADS communication port allows password bruteforce	1.1	EN	Link
2014-001	Potential misuse of several administrative services	1.1	EN	Link

8.3 Support and Service

Beckhoff and their partners around the world offer comprehensive support and service, making available fast and competent assistance with all questions related to Beckhoff products and system solutions.

Download finder

Our download finder contains all the files that we offer you for downloading. You will find application reports, technical documentation, technical drawings, configuration files and much more.

The downloads are available in various formats.

Beckhoff's branch offices and representatives

Please contact your Beckhoff branch office or representative for local support and service on Beckhoff products!

The addresses of Beckhoff's branch offices and representatives round the world can be found on our internet page: www.beckhoff.com

You will also find further documentation for Beckhoff components there.

Beckhoff Support

Support offers you comprehensive technical assistance, helping you not only with the application of individual Beckhoff products, but also with other, wide-ranging services:

- support
- design, programming and commissioning of complex automation systems
- and extensive training program for Beckhoff system components

Hotline:	+49 5246 963-157
e-mail:	support@beckhoff.com

Beckhoff Service

The Beckhoff Service Center supports you in all matters of after-sales service:

- on-site service
- repair service
- spare parts service
- hotline service

Hotline:	+49 5246 963-460
e-mail:	service@beckhoff.com

Beckhoff Headquarters

Beckhoff Automation GmbH & Co. KG

Huelshorstweg 20
33415 Verl
Germany

Phone:	+49 5246 963-0
e-mail:	info@beckhoff.com
web:	www.beckhoff.com

List of tables

List of figures

More Information:
www.beckhoff.com/TwinCAT-BSD

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