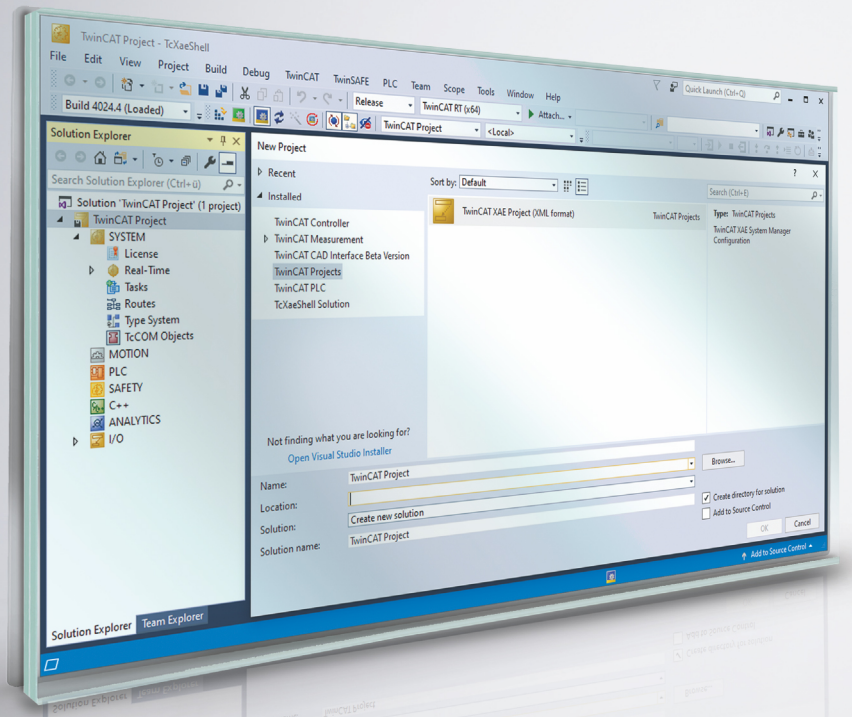
BECKHOFF New Automation Technology

Manual | EN

IPC Security Guideline

for Windows CE



2025-06-10 | Version: 1.3

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 normal 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® 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 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". Beckhoff offers two pre-installed versions of the operating system images on the IPC: In one variant, a random password is pre-set for "Administrator", which can be read from a label on the device. In the second version, the documented known password is preconfigured for this purpose. Please note the following: The latter is not "Secure by Default" with regard to the requirements of some environments, while it is well suited for others.

The operating systems mentioned are not developed by Beckhoff. The basis of the Windows 10 and Windows 11 images from Beckhoff is developed and maintained by the Microsoft Corporation. The basis of TwinCAT/BSD is developed and maintained by "The FreeBSD® Project". Both have been recognized for decades for their security functions for use 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 Control (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 [▶ 20]. 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.

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 [▶ 14])
- Set boot media (BIOS settings [▶ 14])
- Locked control cabinet [▶ 13]

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 [▶ 14])

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:

- Disable autostart (Autostart)
- Whitelisting USB devices (USB filter)
- Locked control cabinet [▶ 13]
- Disable interfaces in BIOS (BIOS settings [▶ 14])
- Whitelisting for programs

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 [▶ 16]
- 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:

- Hard disk encryption
- Locked control cabinet [▶ 13]
- Secure data destruction [▶ 13]

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:

- Hard disk encryption
- Secure data destruction [▶ 13]

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 [▶ 15])
- Whitelisting for programs

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:

- Windows updates (Updates [▶ 15])
- Regular or automatic software updates (Updates [▶ 15])
- Network-based detection mechanisms (IDS/IPS)
- Disabling unneeded services
- Removing components that are no longer needed

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 [▶ 15])
- 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

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.

Data on intact hard disks can be completely and unrecoverably erased by overwriting using special software. The data are overwritten once or several times with specified characters or random numbers, which is sufficient in most cases.

Windows now overwrites a partition completely with zeros during "slow" formatting. In the case of old hard disks (< 80 GB), the data should be overwritten 7 times. Modern hard disks allow the use of the command ATA-"Enhanced Security Erase". Here, a vendor-specific routine is initiated in the hard disk that should erase the entire hard disk, including defective memory areas. This method of erasure is recommended with SSD or SSHD. The command should be combined with the overwriting procedure mentioned above. The data carriers can still be used after overwriting.

Both freeware and commercial products are available on the market that perform the overwriting methods mentioned. Most of these tools offer different overwriting methods. We recommend the use of programs to overwrite the hard disk that can be started from a bootable medium (e.g. CD, USB flash drive) and overwrite the entire hard disk.

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.

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 Backup and recovery

A backup and recovery strategy should be drawn up for each device and protects against:

- security incidents,
- data loss due to defective storage media,
- or from corrupt data due to improper shutdown.

The last backup created can be restored in the shortest possible time, thus preventing major production downtime. Apart from creating backups, it is also important to define a restore process.

Backup and recovery are not exclusively security matters, but help to minimize downtime in case of security incidents.

A process both for creating a safety copy as well as a process to restore it should be defined. Security aspects should also be taken into consideration when doing so.

If a completely automated backup solution is used, the backup system itself is mostly accessible in the network and thus also vulnerable; manual ("offline") backups are better here. Offsite backups, i.e. backups that are stored locally separated, have the advantage that they can be restored even in the case of a local incident where the machine itself is not affected.

A wide variety of implementations are thus available and conceivable.

Since the TwinCAT boot projects and all necessary information are stored as files on the file system of the respective operating system, file-based security is sufficient in this case.

Beckhoff provides a backup and recovery solution in the form of the "Beckhoff Service Tool (BST)". For more information on the BST, see: Infosys entry on BST.

If your Industrial PC is shipped with BitLocker encryption enabled for the system partition, then the key to decrypt the partition during an unattended boot is protected by the Trusted Platform Module (TPM) on the mainboard of the device. The TPM module provides the Windows kernel with the key for decryption only if the measurement of the early startup process shows that previously trusted software with a known configuration has been started and that neither the software nor the configuration nor the next software to be started (i.e. the kernel) has been manipulated.

A full backup must include the boot partition and the system partition. If you back up the entire boot disk as a raw device, your backup contains the encrypted system partition. In addition to the backup, you must also export a recovery key. A recovery key is especially needed to restore and use the backup on another hardware. Please keep this recovery key in a safe and secure place. It is also strongly recommended to always have a recovery key on hand in case legitimate changes have been made to the software and configuration that are part of the early startup process. This can be the case, for example, if the boot sequence of the firmware (BIOS) is changed by authorized persons.

If BitLocker encryption is enabled, there is an alternative to a full backup of the partitions including the encrypted system partition: you can temporarily disable the encryption of the system partition and create an offline backup as usual. Please do not forget to re-enable the encryption afterwards.

5.2 Updates

There are various ways to keep your operating system and programs up-to-date:

- Updating the entire image
- Updating individual programs
- Integrated operating system updates

Under Windows CE there is no operating system-specific update mechanism. Therefore, the only update option is to update the entire image. To find out which image is currently installed, there is a file in the folder `\Hard Disk\` , which is named after the image name (including the version).

For Windows CE, these can be procured via http://download.beckhoff.com/download/software/embPC-Control.

Example of the file name structure on the CX9020 with TwinCAT 3.1 Build 4024.7:

Name:	"CX9020_CB3011_WEC7_HPS_v608f_TC31_B4024.7"
Platform:	CX9020 or CB3011 motherboard
Operating system:	WEC7 = Windows Embedded Compact 7
Type:	HPS = HMI Protected Shell
Version:	v608f
TwinCAT Version:	TC31 = TwinCAT 3.1
TwinCAT Build:	4024.7

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

The following user is created by default in Windows CE on delivery:

User name	Default password
Administrator	1

NTML users can be created in Windows CE.

Setting the password in Windows CE

✓ The Windows CE user interface is running.

1. Select **Start > Control Panel > Password**.
2. Enter a password and confirm it.
3. Quit the dialog with **OK**.
4. Restart the system.

⇨ Users can only start programs if the password is entered.

5.3.1.2 Changing the password of the RAS server

RAS users can manage the controller remotely. The RAS server is disabled by default. The password should nevertheless be changed, in order to prevent access to the RAS server with the delivery password, if the server is activated.

✓ The Windows CE user interface is running.

1. Select **Start > Control Panel > CX Configuration**.
2. Select the **RAS Control** tab.

⇨ The user management section is on the right-hand side of the tab.

5.3.1.3 IPC Security Wizard

User passwords can be set via the IPC diagnostics webpage. It can be reached by https on Port 443.

In the delivery state, the IPC Security Wizard is started when a user connects by https or works locally on the device.

The IPC Security Wizard prompts the user to change the default password.

See also:

- Documentation on IPC diagnostics in the info system

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 [▶ 20] .

6.1 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.

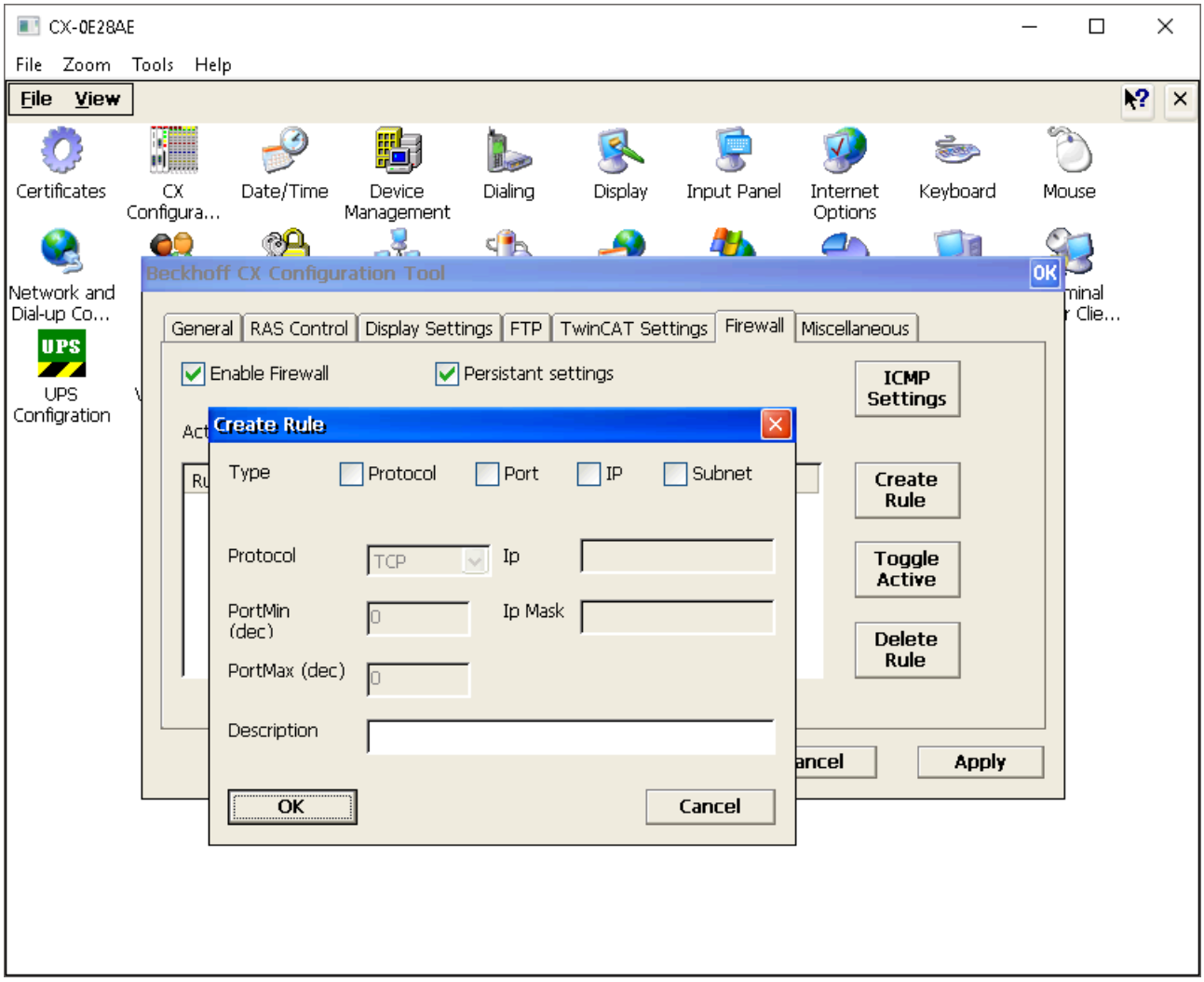
Firewalls with deep-packet inspection, which also evaluate the user data of the data packets, are not able to see the contents of encrypted connections. In order to be able to process the content (e.g. web applications), encryption is often terminated at the firewall and the data for the client is re-encrypted. 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 [▶ 20] contains a list of TCP/UDP ports that typically need to be considered in order to configure a firewall.

The firewall of Windows CE is configured via entries in the registry (see, for example, https://msdn.microsoft.com/en-us/library/ee494503(v=winembedded.60).aspx).

The **Firewall** tab in the Beckhoff CX Configuration Tool facilitates the configuration.



6.2 Network technologies

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

6.2.1 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.

6.2.2 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

6.2.3 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

6.2.4 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.

6.2.5 RDP

Remote Desktop Protocol (RDP) is a proprietary Microsoft protocol for graphical remote access.

6.2.6 CerHost

CerHost is a proprietary, non-encrypted protocol from Microsoft for graphic remote access to Windows CE-based operating systems.

It is recommended to use CerHost only in secured environments (for example via secured transport channels).

6.3 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.

6.4 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

Service	Ports (incoming)
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 (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.

Service	Port (default setting)
	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

6.5 CE Web Server

All web pages that are based on the web server will no longer work.

To disable the Windows CE web server, you can change the following registry entry:

`HKEY_LOCAL_MACHINE\Services\HTTPD\Flags`

If this entry is set to "DWORD 4", the web server is disabled.

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 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
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

Number	Title	Version	Language	Download	External CNA
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	
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 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

Trademark statements

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

Third-party trademark statements

FreeBSD is a registered trademark of The FreeBSD Foundation and is used by Beckhoff with the permission of The FreeBSD Foundation.

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

More Information:
www.beckhoff.com

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