

# SIEMENS



## FC361-xx, FC362-xx

## Cybersecurity Guidelines

## Application Guide

# Table of Contents

<b>1</b>	<b>About this document</b> .....	<b>7</b>
1.1	Applicable documents .....	10
1.2	Download center .....	10
1.3	Revision history .....	10
<b>2</b>	<b>Safety</b> .....	<b>11</b>
2.1	Safety notes .....	11
2.2	Safety regulations for the method of operation .....	12
2.3	Standards and directives complied with.....	14
2.4	Release Notes.....	14
2.5	Cyber security disclaimer .....	14
<b>3</b>	<b>IT Security Notices</b> .....	<b>16</b>
3.1	End of the Life Cycle (EOL).....	16
<b>4</b>	<b>Technical terms and abbreviations</b> .....	<b>17</b>
<b>5</b>	<b>The basics of cybersecurity</b> .....	<b>23</b>
5.1	Introduction.....	23
5.2	Threat and risk terminology.....	23
5.3	System security .....	24
5.4	Dedicated network.....	25
5.5	Network security.....	25
<b>6</b>	<b>Cybersecurity throughout the life cycle of the system</b> .....	<b>26</b>
6.1	Installation and commissioning .....	26
6.2	Operation and maintenance .....	26
6.3	Disposal / phase-out / EOL .....	26
<b>7</b>	<b>System security concept</b> .....	<b>28</b>
7.1	Installation and commissioning .....	28
7.1.1	Responsibility for IT security.....	28
7.1.2	Physical and environmental security .....	28
7.1.3	Implementing the required functionality.....	29
7.1.4	Communication security.....	29
7.1.5	Devices with access to the FS security zone .....	29
7.1.6	Guidelines for PCs.....	30
7.1.7	Password guidelines (for laptop/PC) .....	30
7.1.8	PIN guidelines.....	30
7.2	Operation and maintenance .....	30
7.2.1	Security of saved data .....	30
7.2.2	Regular patches and updates.....	31
7.2.3	Handling incidents.....	31
7.3	Disposal / phase-out / EOL .....	31
<b>8</b>	<b>Intended operating environment and application options</b> .....	<b>32</b>
8.1	Overall networked view .....	32
<b>9</b>	<b>Checklist for permitted applications</b> .....	<b>34</b>
<b>10</b>	<b>Maintenance of IT Components</b> .....	<b>35</b>

**Index .....36**

# Index of figures

Fig. 1: Threat and risk terminology ..... 24

Fig. 2: Overall view, networked ..... 33

# List of Tables

Table 1: Checklist for permitted applications.....34



# 1 About this document

This document must be transferred from the installation personnel to the system operator.

## Retention and availability

<b>!</b>	<b><i>NOTICE</i></b>
	<b>Missing information</b> Damage due to misuse <ul style="list-style-type: none"><li>• This document must be available in a usable format throughout the entire life cycle of the product. Keep the document for reference and ensure that it can be accessed by target groups.</li></ul>

Should you require another copy of this document, please contact the Customer Support Center, phone +49 89 9221-8000.

## Target groups

The information in this document is intended for the following target groups:

Target group	Activity	Qualification
System owner	<ul style="list-style-type: none"> <li>According to EN 50110-1, 'nominated person with the overall responsibility to ensure the safe operation of the electrical installation by setting rules and organisation or framework.'</li> </ul>	<ul style="list-style-type: none"> <li>'This person can be the owner, employer, proprietor or a delegated person.'</li> <li>'Some of these duties can be delegated to others as required. For large or complex electrical installations or networks, the duties can be delegated for parts of the installations or the network.'</li> </ul>
IT security officers	<ul style="list-style-type: none"> <li>Support companies when it comes to assessing the security of products, solutions, and services, and defining and implementing improvements.</li> </ul>	<ul style="list-style-type: none"> <li>Are technical experts in all aspects of IT security.</li> </ul>
Project Manager	<ul style="list-style-type: none"> <li>Coordinates the deployment of all persons and resources involved in the project according to schedule.</li> <li>Provides the information required to run the project.</li> </ul>	<ul style="list-style-type: none"> <li>Has obtained suitable specialist training for the function and for the products.</li> <li>Has attended the training courses for Project Managers.</li> </ul>
Project engineer	<ul style="list-style-type: none"> <li>Sets parameters for product depending on specific national and/or customer requirements.</li> <li>Checks operability and approves the product for commissioning at the place of installation.</li> <li>Is responsible for troubleshooting.</li> </ul>	<ul style="list-style-type: none"> <li>Has obtained suitable specialist training for the function and for the products.</li> <li>Has attended the training courses for Product Engineer.</li> </ul>
Installation personnel	<ul style="list-style-type: none"> <li>Assembles and installs the product components at the place of installation.</li> <li>Carries out a function check following installation.</li> </ul>	<ul style="list-style-type: none"> <li>Has received specialist training in the area of building installation technology or electrical installations.</li> </ul>
Commissioning personnel	<ul style="list-style-type: none"> <li>Configures the product at the place of installation according to customer-specific requirements.</li> <li>Checks the product operability and releases the product for use by the operator.</li> <li>Searches for and corrects malfunctions.</li> </ul>	<ul style="list-style-type: none"> <li>Has obtained suitable specialist training for the function and for the products.</li> <li>Has attended the training courses for commissioning personnel.</li> </ul>

### Source language and reference document

- The source/original language of this document is English (en).
- The reference version of this document is the international version in English. The international version is not localized.

### Document identification

The document ID is structured as follows:

ID code	Examples
ID_languageCOUNTRY_modification index -- = multilingual or international	A6V10215123_deDE_a A6V10215123_en--_a A6V10315123----_a



## Date format

The date format in the document corresponds to the recommendation of international standard ISO 8601 (format YYYY-MM-DD).

## Presentation conventions

### Text markups

Special text markups are used as follows in this document:

▷	Prerequisite for an instruction telling you what to do
1. 2.	Instruction with at least two steps
◇	Instruction with one step
–	Variant, option, or detailed information on an instruction
⇒	Interim result of an instruction
⇒	Final result of an instruction
•	Lists
[→X]	Reference to a page number
'Text'	Quote, exact match
<Button>	Identification of buttons
>	Indicates a link and identifies steps in a sequence, e.g., 'Menu bar' > 'Help' > 'Help topics'
↑ Text	Identifies a glossary entry

### Additional information and tips



The 'i' symbol identifies additional information and tips to simplify the procedure.

### Layout and page breaks



The layout of the PDF version of this document was generated automatically. For this reason, line breaks may occasionally occur within words, e.g., in text in tables. Page breaks have been generated with rules but have not been optimized in context.

This document contains guidelines and conditions for the connection to a panel and describes permitted applications for the intended operational environment. Security-related information for the system operator, relating to maintaining security throughout the life cycle of the system, is found in the 'Maintenance of IT components' chapter.

### Scope

The information contained in this document is valid for Cerberus™ FIT fire control panels FC361-xx and FC362-xx.

## 1.1 Applicable documents

### Main documents

Document ID	Title
A6V10421795	Technical manual, Fire control panel FC360

### Further documents

Document ID	Title
EN 50110-1	Operation of electrical installations – Part 1: General requirements
IEC/TS 62443-1-1	'Industrial communication networks – Network and system security' 'Part 1-1: Terminology, concepts and models'
IEC 62443-2-1	'Industrial communication networks – Network and system security' 'Part 2-1: Establishing an industrial automation and control system security program'
IEC 62443-3-3	'Industrial communication networks – Network and system security' 'Part 3-3: System security requirements and security levels'
ISO/IEC 27032	'Information technology – Security techniques – Guidelines for cybersecurity'
ISO/IEC 27033 Part 1...6	'Information technology – Security techniques – Network security'
ISO/IEC 27034 Part 1...6	'Information technology – Security techniques – Application security'

## 1.2 Download center

You can download various types of documents, such as data sheets, mounting instructions, and license texts via the following Internet address:

<https://siemens.com/bt/download>

- ◆ Enter the document ID in the 'Find by keyword' input box.



You will also find information about search variants and links to mobile applications (apps) for various systems on the home page.

## 1.3 Revision history

The reference document's version applies to all languages into which the reference document is translated.



The first edition of a language version or a country variant may, for example, be version 'd' instead of 'a' if the reference document is already this version.

The table below shows this document's revision history:

Version	Edition date	Brief description
a	2021-04-28	First version

## 2 Safety

### 2.1 Safety notes

The safety notices must be observed in order to protect people and property.

The safety notices in this document contain the following elements:

- Symbol for danger
- Signal word
- Nature and origin of the danger
- Consequences if the danger occurs
- Measures or prohibitions for danger avoidance

#### Symbol for danger



This is the symbol for danger. It warns of **risks of injury**.  
Follow all measures identified by this symbol to avoid injury or death.

#### Additional danger symbols

These symbols indicate general dangers, the type of danger or possible consequences, measures and prohibitions, examples of which are shown in the following table:



General danger



Explosive atmosphere



Voltage/electric shock



Laser light



Battery



Heat


#### Signal word

The signal word classifies the danger as defined in the following table:

Signal word	Danger level
<b>DANGER</b>	'DANGER' identifies a dangerous situation, which <b>will result directly in death or serious injury</b> if you do not avoid this situation.
<b>WARNING</b>	'WARNING' identifies a dangerous situation, which <b>may result in death or serious injury</b> if you do not avoid this situation.
<b>CAUTION</b>	'CAUTION' identifies a dangerous situation, which could result in <b>slight to moderately serious injury</b> if you do not avoid this situation.
<i>NOTICE</i>	'NOTICE' identifies a possibly harmful situation or possible damage to property that may result from non-observance. 'NOTICE' does not relate to possible bodily injury.


#### How risk of injury is presented

Information about the risk of injury is shown as follows:

	<b>⚠ WARNING</b>
	<b>Nature and origin of the danger</b> Consequences if the danger occurs <ul style="list-style-type: none"> <li>• Measures / prohibitions for danger avoidance</li> </ul>

### How possible damage to property is presented

Information about possible damage to property is shown as follows:


	<b>NOTICE</b>
	<b>Nature and origin of the danger</b> Consequences if the danger occurs <ul style="list-style-type: none"> <li>• Measures / prohibitions for danger avoidance</li> </ul>

## 2.2 Safety regulations for the method of operation



### National standards, regulations and legislation

Siemens products are developed and produced in compliance with the relevant European and international safety standards. Should additional national or local safety standards or legislation concerning the planning, mounting, installation, operation or disposal of the product apply at the place of operation, then these must also be taken into account together with the safety regulations in the product documentation.

### Electrical installations

	<b>⚠ WARNING</b>
	<b>Electrical voltage</b> Electric shock <ul style="list-style-type: none"> <li>• Work on electrical installations may only be carried out by qualified electricians or by instructed persons working under the guidance and supervision of a qualified electrician, in accordance with the electrotechnical regulations.</li> </ul>

- Wherever possible disconnect products from the power supply when carrying out commissioning, maintenance or repair work on them.
- Lock volt-free areas to prevent them being switched back on again by mistake.
- Label the connection terminals with external voltage using a 'DANGER External voltage' sign.
- Route mains connections to products separately and fuse them with their own, clearly marked fuse.
- Fit an easily accessible disconnecting device in accordance with IEC 60950-1 outside the installation.
- Produce earthing as stated in local safety regulations.

	<p><b>⚠ CAUTION</b></p>
	<p><b>Noncompliance with the following safety regulations</b> Risk of injury to persons and damage to property</p> <ul style="list-style-type: none"> <li>• Compliance with the following regulations is required.</li> </ul>
	<ul style="list-style-type: none"> <li>• Specialist electrical engineering knowledge is required for installation.</li> <li>• Only an expert is permitted to carry out installation work.</li> </ul> <p>Incorrect installation can take safety devices out of operation unbeknown to a layperson.</p>

### Mounting, installation, commissioning and maintenance

- If you require tools such as a ladder, these must be safe and must be intended for the work in hand.
- When starting the fire control panel ensure that unstable conditions cannot arise.
- Ensure that all points listed in the 'Testing the product operability' section below are observed.
- You may only set controls to normal function when the product operability has been completely tested and the system has been handed over to the customer.

### Testing the product operability

- Prevent the remote transmission from triggering erroneously.
- If testing building installations or activating devices from third-party companies, you must collaborate with the people appointed.
- The activation of fire control installations for test purposes must not cause injury to anyone or damage to the building installations. The following instructions must be observed:
  - Use the correct potential for activation; this is generally the potential of the building installation.
  - Only check controls up to the interface (relay with blocking option).
  - Make sure that only the controls to be tested are activated.
- Inform people before testing the alarm devices and allow for possible panic responses.
- Inform people about any noise or mist which may be produced.
- Before testing the remote transmission, inform the corresponding alarm and fault signal receiving stations.

### Modifications to the system design and the products

Modifications to the system and to individual products may lead to faults, malfunctioning and safety risks. Written confirmation must be obtained from Siemens and the corresponding safety bodies for modifications or additions.

### Modules and spare parts

- Components and spare parts must comply with the technical specifications defined by Siemens. Only use products specified or recommended by Siemens.
- Only use fuses with the specified fuse characteristics.
- Wrong battery types and improper battery changing lead to a risk of explosion. Only use the same battery type or an equivalent battery type recommended by Siemens.
- Batteries must be disposed of in an environmentally friendly manner. Observe national guidelines and regulations.

## Disregard of the safety regulations

Before they are delivered, Siemens products are tested to ensure they function correctly when used properly. Siemens disclaims all liability for damage or injuries caused by the incorrect application of the instructions or the disregard of danger warnings contained in the documentation. This applies in particular to the following damage:


- Personal injuries or damage to property caused by improper use and incorrect application
- Personal injuries or damage to property caused by disregarding safety instructions in the documentation or on the product
- Personal injury or damage to property caused by poor maintenance or lack of maintenance


## 2.3 Standards and directives complied with

A list of the standards and directives complied with is available from your Siemens contact.

## 2.4 Release Notes

Limitations to the configuration or use of devices in a fire detection installation with a particular firmware version are possible.

	<b>⚠ WARNING</b>
	<p><b>Limited or non-existent fire detection</b></p> <p>Personal injury and damage to property in the event of a fire.</p> <ul style="list-style-type: none"> <li>• Read the 'Release Notes' before you plan and/or configure a fire detection installation.</li> <li>• Read the 'Release Notes' before you carry out a firmware update to a fire detection installation.</li> </ul>

	<b>NOTICE</b>
	<p><b>Incorrect planning and/or configuration</b></p> <p>Important standards and specifications are not satisfied. Fire detection installation is not accepted for commissioning. Additional expense resulting from necessary new planning and/or configuration.</p> <ul style="list-style-type: none"> <li>• Read the 'Release Notes' before you plan and/or configure a fire detection installation.</li> <li>• Read the 'Release Notes' before you carry out a firmware update to a fire detection installation.</li> </ul>

## 2.5 Cyber security disclaimer

Siemens provides a portfolio of products, solutions, systems and services that includes security functions that support the secure operation of plants, systems, machines and networks. In the field of Building Technologies, this includes building automation and control, fire safety, security management as well as physical security systems. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art security concept. Siemens' portfolio only forms one element of such a concept.

You are responsible for preventing unauthorized access to your plants, systems, machines and networks which should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. Additionally, Siemens' guidance on appropriate security measures should be taken into account. For additional information, please contact your Siemens sales representative or visit <https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrial-security.html>.

Siemens' portfolio undergoes continuous development to make it more secure. Siemens strongly recommends that updates are applied as soon as they are available and that the latest versions are used. Use of versions that are no longer supported, and failure to apply the latest updates may increase your exposure to cyber threats. Siemens strongly recommends to comply with security advisories on the latest security threats, patches and other related measures, published, among others, under <https://www.siemens.com/cert/en/cert-security-advisories.htm>.

## 3 IT Security Notices

### Responsibility of the system operator

The information technology (IT) used in a system is the responsibility of the system operator.

### National standards, regulations and legislation



Specifications for IT security are also put into effect through country-specific legislation. You must observe the country-specific legislation when planning and commissioning.

Siemens products are developed and produced in compliance with the relevant European and international safety standards. Should additional country-specific or local security standards or legislation concerning IT security apply at the place of operation, you must apply these in addition to the guidelines and the permitted applications in this document.

For example, the 'European Union Agency for Cybersecurity' [www.enisa.europa.eu](http://www.enisa.europa.eu) provides information on basic IT security in Europe: <https://www.enisa.europa.eu/topics/cybersecurity-education>.

For Germany, the 'Federal Office for Information Security' (BSI) [www.bsi.bund.de/EN](http://www.bsi.bund.de/EN) provides information on basic IT security in both [German](#) and [English](#).

Further links: [www.cisecurity.org](http://www.cisecurity.org)

### Siemens cybersecurity guidelines

The Siemens cybersecurity guidelines in this document provide the system operator with additional specifications – alongside basic IT security – for operating a corresponding system. These additional specifications are valid at the time of publication.

<b>!</b>	<b>NOTICE</b>
	<p><b>Modified Security Risks in the Life Cycle of the System</b></p> <p>Additional security risks</p> <ul style="list-style-type: none"> <li>You must log compliance with the specifications, see also 'Maintenance of IT Components [→ 35]'.</li> </ul>

### 3.1 End of the Life Cycle (EOL)

Any IT component involved in the access to the FS zone must be replaced as soon as it ceases to be supplied with security updates by the manufacturer. If this EOL IT component cannot be replaced, the FS zone must be immediately disconnected from connections with untrustworthy networks.

#### See also

Disposal / phase-out / EOL [→ 26]



## 4 Technical terms and abbreviations

Term	Explanation
AES	Advanced Encryption Standard (AES) is a FIPS publication developed by the NIST as the successor to DES. AES specifies a non-classified, publicly accessible, symmetric encryption algorithm which is available free of charge all over the world.
Autotrunking	Autotrunking is a function that enables one or more switch ports in a Cisco system of virtual local area networks (VLANs) to carry traffic for any or all of the VLANs accessible through a particular switch. In Cisco's Dynamic Trunking Protocol (DTP), a port can be set to autotrunking by default with 'DTP auto'.
AWS	Amazon Web Services
BA	Building automation
BACnet	BACnet is used for networks in building automation and building control BACnet is a network protocol for standardized communication between devices from different manufacturers in building automation.
BIOS	Basic Input/Output System is non-volatile firmware which is used to perform hardware initialization during the booting process and to provide runtime services for the operating systems and programs.
BLE	Bluetooth Low Energy is a wireless personal area network technology designed and marketed by the Bluetooth Special Interest Group aimed at novel applications in the healthcare, fitness, beacons, security, and home entertainment industries.
Bluetooth	Bluetooth is a wireless technology standard used for exchanging data between fixed and mobile devices over short distances using short-wavelength UHF radio waves in the industrial, scientific, and medical radio bands, from 2.402 GHz to 2.480 GHz, and building personal area networks (PANs).
CA	The certificate authority (CA) is an entity that issues digital certificates, particularly X.509 certificates, and vouches for the binding between the data items in a certificate.
CAN	Controller Area Network (CAN) is a bus standard designed to allow microcontrollers and devices to communicate with each other's applications without a host computer.
C-NET	Addressed detector line in the Cerberus portfolio
Container	Containers are an abstraction on the application layer and represent a standard method of packing application code, configurations, and dependencies into a single object.
CRL	A certificate revocation list (CRL) is a list of digital certificates that have been revoked by the issuing CA before their scheduled expiration date and should no longer be trusted.
Digital signature	A digital signature is a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity.
Digital certificate	A digital certificate is a certificate document in the form of a digital data object – a data object used by a computer – to which is appended a computed digital signature value that depends on the data object.
DMZ	A demilitarized zone (DMZ) refers to a computer network with security-controlled access to the connected servers and devices. A DMZ provides protection by isolating a system from two or more networks. A system in a DMZ is shielded from other networks, e.g., Internet or LAN, by means of one or more firewalls.

Term	Explanation
	This separation makes it possible to grant access to publicly accessible services while also protecting the internal system in the DMZ from unauthorized external access. The aim is to make system services available to both the WAN (Internet) and the LAN (intranet) in as secure a manner as possible.
DNET	Network for connecting multiple FS20M voice stations with each other via the DNET card.
DNS	The Domain Name System (DNS) is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. The system contains a directory of names and their translations into IP addresses.
EOL	End of the Life Cycle (EOL)
FDnet	Addressed detector line in the Sinteso portfolio
FIN Framework	Flexible, modular software which enables building operators to record data from automation networks.
Firewall	The firewall is a network security system that monitors and controls incoming and outgoing network traffic on the basis of specified security rules.
Front-end processor	The front-end processor is a computer that extends and distributes connectivity to field networks. The purpose is to off-load from the host computer the work of managing the peripheral devices, transmitting and receiving messages, packet assembly and disassembly, error detection, and error correction.
FSI	The Foreign System Interface (FSI) is the combination of the physical equipment and the API document supplied to the customers which enables an FS20M system to be monitored and controlled via this interface.
FS security zone	Physically separated, private network. A fire detection system is a physically separated network and forms a fire detection system security zone. Network access from outside of this zone into this zone is only permissible via the protective component at the boundary to the FS zone.
FS security zone	The FS security zone is a physically separated, private network. A fire detection system is a physically separated network and forms a fire detection system security zone Network access from outside of this zone into this zone is only permissible via the protective component at the boundary to the FS security zone.
GB	National standards for China
GDPR	The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individual citizens of the European Union and the European Economic Area.
HNET	HNET is a network that is used to connect FS20M stations to FS20M transponders.
HTTPS	Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over computer networks, and is widely used on the Internet.
ICMP	Internet Control Message Protocol (RFC 792)
IDaaS	Identity as a Service is an authentication infrastructure that is managed by Siemens.
IEC	The International Electrotechnical Commission is an international standards organization that prepares and publishes international standards for all electrical, electronic, and related technologies – collectively known as electrotechnology.

Term	Explanation
IIS	<p>Internet Information Services (IIS) is a service platform from Microsoft for PCs and servers.</p> <p>This service platform can be used to make documents and files available in the network.</p> <p>The following communication protocols are used for this purpose: HTTP, HTTPS, FTP, SMTP, POP3, WebDAV.</p> <p>ASP or .NET applications (ASP.NET) can be executed via IIS.</p> <p>If the relevant ISAPI filters are installed, PHP and JSP can also be used.</p>
IoT	Internet of Things (IoT)
IPsec	<p>Internet Protocol Security (IPsec) is an encryption and authentication protocol for IP packets.</p> <p>IPsec offers two independent security mechanisms:</p> <ul style="list-style-type: none"> <li>- Encapsulating Security Payload (ESP) ensures confidentiality and, optionally, integrity of data packets.</li> <li>- Authentication Header (AH) ensures integrity and authenticity of data packets.</li> </ul> <p>AH is not an authentication protocol and does not authenticate people, applications, systems or devices. It provides protection for the data packet within the IPsec protocol.</p>
IPv4	<p>Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP). It is one of the core protocols of standards-based internetworking methods in the Internet and was the first version deployed for production in the ARPANET in 1983.</p> <p>IPv4 is a connectionless protocol for use on packet-switched networks. It operates on a best effort delivery model, in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol, such as the Transmission Control Protocol (TCP).</p>
IPv6	<p>Internet Protocol version 6 is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4.</p>
ISA 62443 (ISA99 / ANSI62443)	<p>ISA 62443 is a series of standards, technical reports, and associated information that define procedures for implementing electronically secure industrial automation and control systems (IACS).</p> <p>This guide is intended for end users, such as system owners, system integrators, security practitioners, and manufacturers of control systems, who are responsible for the manufacture, implementation, or management of industrial automation and control systems.</p> <p>These documents were originally known as ANSI/ISA-99 or ISA99 standards as they were created by the International Society for Automation (ISA) and published as documents of the American National Standards Institute (ANSI). In 2010, these documents were incorporated into the ANSI/ISA 62443 series. When this change took place, the numbering of the ISA and ANSI documents was aligned with the corresponding standards of the International Electrotechnical Commission (IEC).</p>
ISO	<p>The International Organization for Standardization is an international standard-setting body composed of representatives from various national standards organizations.</p>
IT/OT network	<p>Information technology/operational technology network.</p> <p>An IT network is used for electronic devices in an office, e.g., PCs, printers, etc.</p> <p>An OT network is used for hardware and software in order to detect or bring about changes in the physical processes through direct monitoring and control of physical devices such as valves, pumps, etc.</p> <p>Both types of network use Ethernet as the physical medium.</p>
JWT	<p>JSON Web Token (JWT) is an Internet standard for creating JSON-based access tokens for use in authentication methods.</p>

Term	Explanation
LogView	LogView is an FS20M diagnostics tool that is made available to customers in order to help with troubleshooting installation problems.
MDAC	MDAC is an outbound event dialer.
MFA	Multi-factor authentication is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism: Knowledge, possession, and inherence. Two-factor authentication (2FA) is a type, or subset, of multi-factor authentication.
MMS	Management station
MMS	Management station (MMS)
Modbus	Modbus is a data communication protocol for building automation and control networks.
MOSA	MOSA is a product which enables a LAN-IP-MMS interface.
Multi-homed	Connected with more than one network at the same time.
NCC	Management station for displaying the events of an FS20M system
NFC	Near-field communication (NFC) is a set of communication protocols for communication between two electronic devices over a distance of 4 cm or less. NFC offers a low-speed connection with simple setup that can be used to bootstrap more capable wireless connections.
On-premise	Within a building or site.
PAL	UL-listed parallel printer.
Public-key infrastructure	A public-key infrastructure (PKI) is a set of roles, policies, hardware, software, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
Public-key certificate	<p>In cryptography, a public-key certificate, also known as a digital certificate or identity certificate, is an electronic document used to prove the ownership of a public key.</p> <p>The certificate includes information about the key, information about the identity of its owner (called the subject), and the digital signature of an entity that has verified the certificate's contents (called the issuer).</p> <p>If the signature is valid, and the software examining the certificate trusts the issuer, then it can use that key to communicate securely with the certificate's subject.</p> <p>In email encryption, code signing, and e-signature systems, a certificate's subject is typically a person or organization.</p> <p>However, in Transport Layer Security (TLS) a certificate's subject is typically a computer or other device, though TLS certificates may identify organizations or individuals in addition to their core role in identifying devices. TLS, sometimes called by its older name Secure Sockets Layer (SSL), is notable for being a part of HTTPS, a protocol for securely browsing the web.</p> <p>In a typical public-key infrastructure (PKI) scheme, the certificate issuer is a certificate authority (CA), usually a company that charges customers to issue certificates for them. By contrast, in a web of trust scheme, individuals sign each other's keys directly, in a format that performs a similar function to a public-key certificate.</p> <p>The most common format for public-key certificates is defined by X.509. Because X.509 is very general, the format is further constrained by profiles defined for certain use cases, such as Public-Key Infrastructure (X.509) as defined in RFC 5280.</p>
RA	The registration authority (RA) is an optional system to which a CA delegates certain management functions.
RDP	Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer

Term	Explanation
	over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software.
RFID	Radio-frequency identification (RFID) uses electromagnetic fields to automatically identify and track tags attached to objects. An RFID tag consists of a tiny radio transponder; a radio receiver and transmitter.
SAFEDLINK	Physical network of an FS20 fire detection system with the network module SAFEDLINK and the network cable.
Secure boot	Secure booting was developed to protect systems and ensure that malicious code cannot be loaded and executed early in the boot process before the operating system has loaded. The aim is to prevent malicious software from installing a 'bootkit' and retaining control of a system in order to disguise its presence.
Single-homed	Connected with a maximum of one network at the same time.
SNU	The Single Node Upload (SNU) module enables access to the configuration port on the FS20M via a LAN Ethernet interface.
SPM	System Performance Management
SSH	Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network.
Standalone station	A standalone station is a station with only a local connection for the computer.
Station (in Algorex systems)	Designation for devices that are networked via the C-BUS, such as the compact station (CI), control terminal (CT), and main CPU (CC).
TCP	Transmission Control Protocol (TCP) is a standard that defines how to establish and maintain a network conversation through which application programs can exchange data. It is intended for use as a highly reliable host-to-host protocol between hosts in packet-switched computer communication networks, and especially in interconnected systems of such networks.
TLS	The Transport Layer Security (TLS) protocol provides communications security over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.
TPM	Trusted Platform Module (TPM) is an international standard for a secure cryptoprocessor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys.
UDP	The User Datagram Protocol (UDP) is defined to make available a datagram mode of packet-switched computer communication in the environment of an interconnected set of computer networks. The protocol is transaction-oriented, and delivery and duplicate protection are not guaranteed. Applications requiring ordered reliable delivery of streams of data should use the TCP.
USB	Universal Serial Bus (USB) is an industry standard that establishes specifications for cables and connectors and protocols for connection, communication, and power supply between devices.
UTNW	The term 'untrustworthy network' refers to users or devices of an area which is considered unsecure or unprotected. This area is generally a network outside the trustworthy network.
UTNW	Acronym for 'untrustworthy network'
VAP	Value added partner (VAP), solution partner
'Trustworthy network'	The term 'trustworthy network' refers to users or devices of an area which is

Term	Explanation
	<p>considered particularly secure or protected. This area is typically a private section of a network.</p> <p>This private section of the network must be protected from attacks by hackers and other security-related threats.</p>
VLAN	<p>A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2).</p> <p>VLANs work by applying tags to network frames and handling these tags in networking systems – creating the appearance and functionality of network traffic that is physically on a single network but acts as if it is split between separate networks.</p> <p>In this way, VLANs can keep network applications separate despite being connected to the same physical network, and without requiring multiple sets of cabling and networking devices to be deployed.</p>
VNT	Virtual Network Tunnel enables the expansion of the FS20M buses via IP.
VPN	Virtual Private Network
WAN	A wide area network (WAN) is a telecommunications network that extends over a large geographical area for the primary purpose of computer networking.
WebSocket	<p>WebSocket is a computer communications protocol, providing full-duplex communication channels over a single TCP connection.</p> <p>WebSocket is distinct from HTTP.</p> <p>Although the two protocols are different, RFC 6455 states that WebSocket "is designed to work over HTTP ports 80 and 443 as well as to support HTTP proxies and intermediaries," thus making it compatible with the HTTP protocol.</p>
X.509 certificate	In cryptography, X.509 is a standard defining the format of public-key certificates.
XDAC	XDAC is a second-generation outbound event dialer.
XND	XND is a product used to connect XNET or HNET products to another Siemens product which is connected to XNET or HNET via the serial XND protocol.
XNET	Network for connecting multiple FS20 stations.
ZBP	Zone boundary protection
Zeus	Windows-based configuration tool used to configure FS20M stations.

## 5 The basics of cybersecurity

### 5.1 Introduction

Cybersecurity covers all mechanisms for protecting IT systems, such as computers, devices like primary controllers, or web servers in a building automation system, from unauthorized access, faults, modifications, or destruction. It also prevents confidential information from being accessed and information obtained without authorization through fraud or other crimes from being used. In doing so, it minimizes the risk of losing system and data confidentiality, integrity, and availability.

Cybersecurity can be implemented in accordance with different industry and national standards, which usually set out different levels of protection depending on the system use and the acceptable risk level.

Up until now, most cybersecurity breaches have involved attacks on conventional computer systems, such as the Internet, intranet, or home networks. Denial of service, theft of critical private and commercial information, bank account and credit card fraud, and ransomware are all examples of the damage caused.

By contrast, there have been fewer attacks on industrial controls, such as building automation controls, as these types of systems often ran on proprietary operating systems, the hardware only had a limited functionality, and these systems were rarely connected to other networks.

Current computer standards are being used increasingly in industrial controls to make them cheaper and more powerful. What's more, industrial controls are usually connected to other customer networks and the Internet, which – in turn – makes them more vulnerable to attacks. Connections can also be used to start an attack on the automation network from the company network and vice versa.

It is therefore particularly important to provide an appropriate level of security for modern building technology solutions.

### 5.2 Threat and risk terminology

Below you will find a short glossary of terms related to IT security.

An **'Asset'** is a tangible or intangible item of property which needs to be protected by the security policy of an information system, which is to be protected by means of a countermeasure, or which is required for a system task.

An **'Information System'** is an organized collection of computing and communication resources as well as computing and communication procedures.

This system comprises equipment and services, along with the supporting infrastructure, facilities, and personnel which create, collect, record, process, save, transport, retrieve, display, distribute, control, or dispose of information to fulfill a certain range of functions.

A **'Vulnerability'** is a fault or flaw in the design, implementation, operation, or management of a system which could be exploited to breach the security of the system.

**'Susceptibility'** defines how easy it would be for an attacker to access the system to carry out malicious activities. The susceptibility is generally high if a system is connected to the Internet and can therefore be accessed externally.

A **'Threat'** is something that has the potential to breach security if an entity, circumstance, capability, action, or event exists which could cause damage.

The **'Common Criteria'** characterize a threat in relation to the following aspects:

- Risk factor
- Suspected method of attack
- Weaknesses which form a basis for the attack
- Attacked system resource

The **'Impact'** describes the extent of the damage sustained by the systems in the event of an IT security incident. In some cases, the extent of the damage can be assessed based on monetary value, for example, the cost of replacing the devices. Often, however, 'Impact' refers to damage to reputation and other intangible assets which are difficult to assess.

A **'Risk'** is an expectation of damage, expressed as probability, where a specific threat exploits a specific vulnerability, resulting in a specific harmful outcome.

The residual risk is the proportion of an original risk or series of risks which remains once countermeasures have been applied.

A **'Measure'**, also known as a **'Countermeasure'** or **'Control'**, is implemented to reduce the risk. Such measures can include hardware or software methods to minimize the probability of an attacker gaining access to the system, for example, isolating a system from the rest of the system with the aid of standard passwords.

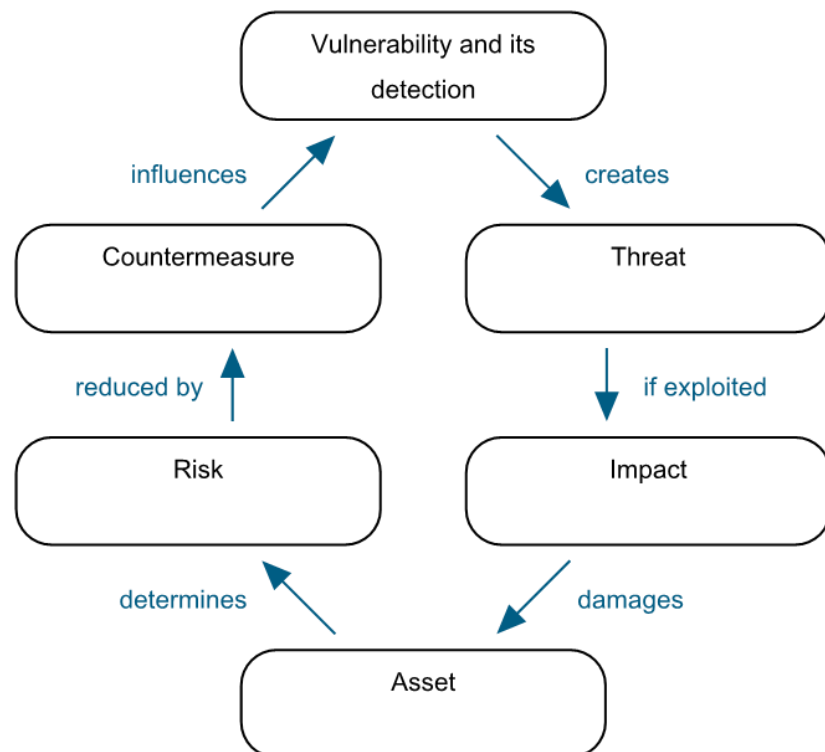


Fig. 1: Threat and risk terminology

### 5.3 System security

As explained in the 'Introduction [→ 23]', every modern building automation system must have an appropriate degree of IT security. However, it is not possible to ensure complete security, so there will always be a residual risk. The costs of a countermeasure should not exceed the potential damage from which they are to protect. In every case, the system operator must be aware of the residual risk and decide whether it is acceptable for the company.

It is important to consider the security requirements systematically so that the effectiveness of the measures is assessed as a whole and each component is not treated separately. Most notably, compensatory countermeasures can be used to alleviate the vulnerabilities of given subsystems so that the total required security level is achieved.

It is also important that the various parties involved – manufacturers, system integrators, and system operators – contribute to the system in line with their specific role. The manufacturer is responsible for supplying products that offer the degree of security specified in their product specification and product documentation. The system integrators are responsible for designing and applying the solution in line with the safety requirements of the system operator and for



taking the intended operating environments of the products being used into account. The system operator is responsible for keeping the security measures up to date during the service life of the solution.

To uphold the level of security of the solution, a framework for a continuous security program needs to be established. This must regularly assess the target security level, the risks of the system, the status, and the effectiveness of the measures applied and implement corrective measures.

The guidelines in this document support a continuous process for achieving IT security on a system level.

## 5.4 Dedicated network

- Create a dedicated network for your system.
- Ensure that only the necessary IT components are used in the network for your system.

## 5.5 Network security

All measures aligned toward securing the network must reduce the risk of potential security loopholes or security vulnerabilities in the fire detection system.

Observe the security measures in the following chapters:

- 'System security concept'
- 'Intended operating environment and application options'



### **⚠ WARNING**

#### **System manipulation due to unauthorized access**

Limited or lacking fire detection; personal injury and damage to property in the event of a fire.

- Observe the following points and facts about the fire detection system regarding security loopholes, vulnerabilities, and necessary security measures.
- Not all usable components for the fire detection system meet the current IT security requirements without further security measures.
- Without suitable security measures, the fire detection system is not sufficiently protected against current IT attack strategies and there is a danger that potential security loopholes or security vulnerabilities will be exploited.
- As the result of a thorough risk assessment, an appropriate and sufficient degree of IT security can be achieved for the fire detection system with suitable security measures.

## 6 Cybersecurity throughout the life cycle of the system

The following sections contain general information on cybersecurity and how a system can be secured throughout each phase of its life cycle.

### 6.1 Installation and commissioning

During the initial phase of a system's life cycle, the security assessments are key to ensuring meticulous and early integration.

These ensure that threats, requirements, and potential restrictions regarding functionality and integration are taken into account from an early stage. In this initial phase, security – with the involvement of the information security officer – is considered from the point of view of business risk.

Advance planning and awareness enables savings in terms of costs and time to be made as appropriate risk management planning is implemented.

Security discussions should be held as part of the development project, not as a separate element, in order to ensure that all employees involved in the project have a sound understanding of the business decisions and their risk impacts on the development project as a whole.

Important activities to support the installation and commissioning of a secure standard system include the following:

- Create an inventory list for the system.
- Create a diagram containing an overview of the system.
- Identify the critical data in the system.
- Determine the protection requirements for the system.
- Follow the guidelines for hardening the individual components, if available.

Based on this information, measures to reduce risk can be taken to achieve the best possible level of security for the system.

### 6.2 Operation and maintenance

The system is set up and put into operation in this phase. Expansions and/or modifications to the system are developed and tested. Hardware and/or software is added or replaced.

The system is monitored in accordance with the security requirements to ensure continuous performance. Necessary system modifications are incorporated. The operating system is regularly assessed to determine how the system can be designed more effectively, more securely, and more efficiently.

Operation continues for as long as the system can be effectively adapted to the needs of an organization, while maintaining an agreed risk level.

The most important security activities in this phase are as follows:

- Examining operational readiness
- Managing the system configuration
- Implementing processes and procedures for secure operation
- Continuous monitoring of system security controls

### 6.3 Disposal / phase-out / EOL

Disposal – the last phase of the system life cycle – concerns the disposal of the system and the termination of existing contracts. Questions regarding information security in the context of the disposal of information and systems should be addressed explicitly.

If information systems are transferred, become obsolete, or are no longer usable, it is important to ensure that the resources and assets of the owner are protected.

As a rule, there is no definite end to a system. Systems are normally developed further on account of changes in requirements and technological improvements, or they transition to the next generation.

System security plans should be continuously developed as the system is developed. When the security plan for the subsequent system is developed, most of the environmental, management, and operational information should continue to be relevant and useful.

The disposal activities ensure that the system is phased out in an orderly manner and retain the vital information about the system to enable some or all of the information to be reactivated in the future if necessary.

One area of focus is the orderly retention of data to ensure that the data can be migrated to another system effectively or, in compliance with the applicable regulations and guidelines for the management of documents, to enable data to be archived for possible future access.

The most important security activities for this phase are as follows:

- Creating and implementing a transition plan
- Creating and implementing a disposal plan
- Orderly retention of data
- Archiving critical information
- Deleting media securely
- Disposing of hardware and software

## 7 System security concept

An FC360 fire detection system is a system used to protect people and property and must be protected against attacks and unauthorized access.

Setting up the system network, including zone boundary protection, is the responsibility of the system operator.

If a networked system is envisaged, the FC360 fire detection system must be used in a physically separated network. This network forms an FS security zone. Zone boundary protection has the function of 'Incoming protection'/'Outgoing protection' for the FS security zone.

**⚠ CAUTION! A separate VLAN does not meet the requirements for zone boundary protection.**

The components in the FS security zone must not be connected to other networks, such as the intranet or Internet.

The required connections described in this document are the exceptions here.

### 7.1 Installation and commissioning

#### 7.1.1 Responsibility for IT security

<b>!</b>	<b>NOTICE</b>
	The system operator is responsible for setting up and maintaining an appropriate level of IT security. The following points and measures are to be considered in particular:

- Use of virus scanners
- Disabling of unnecessary services and network connections
- Regular application of patches and updates for the operating system and all installed applications
- Firmware update

#### 7.1.2 Physical and environmental security

The following restrictions apply with regard to physically protecting the FC360 system against unauthorized and malicious use:

- The technical room in which the panel is installed must be protected against unauthorized access.
- The panel must be protected against unauthorized access (e.g., in a separate room or behind reception desk).
- As a general rule, publicly accessible data transmission lines, such as cabling for danger management system (DMS), Pager interface (ESPA) and external printer, must be protected against unauthorized access.
- C-NET bus, serial interfaces, and cabling must be physically protected if one of these components is located in a publicly accessible area.
- The serial (RS232/RS485) and Ethernet endpoints must be physically, organizationally, or logically protected. Only connect approved devices to these interfaces. If no devices are connected, the interface must be disabled.
- Define and implement processes to grant and revoke physical access.
- Additional controls, such as location protection, additional restrictive access control for the building and rooms, security personnel, or monitoring, can help to improve the physical security of the system.

### 7.1.3 Implementing the required functionality

- Make sure that no unknown hardware is physically connected to the interfaces of the systems.
- Disable interfaces or interface types which are not being used in the current setup.
- Make sure that no ports other than those specified in the firewall rules are open.
- Make sure that no services other than those necessary to ensure complete system functionality are running during normal system operation.
- Use the fire detection system in line with its intended operation and in accordance with the fire protection regulations.

### 7.1.4 Communication security

As a general rule, secure protocols must be used for communication with the FS security zone.

Only local client communication is permitted for the FC360 system. This means that the client is part of the FS security zone and cannot be connected to another network zone at the same time.

To further enhance the security situation, the client should only be used in a controlled environment.

- A corresponding protection component must be set up at the boundary to the FS security zone for each connection to external networks or other systems.
- Local connections to the system will require additional protective measures unless the component with access to the FS security zone is single-homed and therefore does not interface with other systems.
- Communication between the FS security zone and other zones must be restricted to a minimum and pass through a firewall.

### 7.1.5 Devices with access to the FS security zone

Comply with the following measures to improve the security of devices with access to the FS security zone:

**⚠ WARNING! Untrustworthy applications** on the service laptop/PC which have access to the FS security zone are a risk and may prevent alarms or faults from being recorded and processed, causing fire to spread unnoticed.

- Operate all corresponding devices such as PCs and Android smartphones/tablets with a current, continually updated operating system and active, continually updated antivirus software.
- Operate devices such as routers, hardware firewalls, and other components used to protect the FS security zone with current firmware and ensure that updates and patches are continually installed.
- Replace devices used to protect the FS security zone if they have reached the end of their life cycle. See also 'Disposal / phase-out / EOL [→ 31]'.  
• Ensure that components used to protect the FS security zone are not publicly accessible.

## 7.1.6 Guidelines for PCs

<b>!</b>	<p><b>NOTICE</b></p> <p><b>Missing updates on the PC operating system</b> Access to fire detection system data and possible misuse of data when accessing a fire detection installation</p> <ul style="list-style-type: none"> <li>• Maintain and configure your PC in accordance with the guidelines in the Siemens CERT <a href="#">'Security Measure Plan for Windows'</a>.</li> </ul>
----------	---

- In general, PCs are only permitted for use if manufacturer support is in place for the operating system used.
- All the updates and patches provided by the manufacturer must be installed on the operating system. In addition, a continually updated antivirus software must be installed.

You will find the Security Measure Plan for Windows here:

<https://www.cert.siemens.com/platforms/windows>



Please contact your Siemens contact partner if you do not have access to the web pages at <https://www.cert.siemens.com/>.

### 7.1.7 Password guidelines (for laptop/PC)

- In general, preset passwords need to be changed during or immediately after installation.
- A password should be made up of uppercase and lowercase letters, special characters, and numbers. At least two of these character types need to be used.

### 7.1.8 PIN guidelines

You can log into the system and enable an 'access level' with a Personal Identification Number (PIN).

- In general, preset PINs need to be changed during or immediately after installation.
- We do not recommend that service technicians create a PIN or change the number of figures required for a PIN to a smaller number. This must be documented.
- Do NOT label the PIN code on the panel.

## 7.2 Operation and maintenance

### 7.2.1 Security of saved data

Generally, data is saved unencrypted in the system.

Confidential customer data is saved on various devices such as CD/DVD-ROMs, USB drives, and the service laptop. To protect this confidential data, the following additional measures must be taken:

- Encrypt the confidential customer data saved on the removable media and treat the encryption password as confidential.
- Store the removable media in a lockable system housing designed for storing such media.
- Lock the system housing used to store the removable media.
- Encrypt confidential data on the service laptop/PC.

A service laptop/PC which stores confidential customer data is subject to the same protection requirements as removable media.

- Continually perform maintenance on the service laptop/PC, in accordance with 'Guidelines for PCs [→ 30]'.
  - Correct configuration
  - Hardening
  - Maintenance
  - Patching

## 7.2.2 Regular patches and updates

The maintenance of IT security is a sustained process for which the corresponding tasks must be continually repeated. Every specified security measure must therefore be checked to determine whether it only needs to be implemented once or whether it needs to be performed at regular intervals, for example, regular updates to antivirus software.

- Log all maintenance measures implemented.
- Observe the information in the 'The basics of cybersecurity [→ 23]' section.
- Install security updates regularly.
- Run a risk analysis on the security properties of the applied software at regular intervals.

## 7.2.3 Handling incidents

If a security-related event occurs, please contact your Siemens contact partner immediately, for example, a field engineer, a sales employee, or contact the Siemens Computer Emergency Response Team for products – 'ProductCERT':

Website: <https://www.siemens.com/cert/advisories>

E-mail: [productcert@siemens.com](mailto:productcert@siemens.com)

To ensure that your problem can be resolved quickly, we request that you write your inquiry to 'ProductCERT' in either English or German.

## 7.3 Disposal / phase-out / EOL

As soon as an IT component which is involved in access to the FS security zone is no longer able to be provided with security updates, this IT component must be replaced.

If this 'EOL' IT component cannot be replaced, the FS security zone must be immediately disconnected from connections with untrustworthy networks.

As soon as the system operator decides that FC360 system components are to be systematically taken out of operation, the data and settings of these components must be properly destroyed and the systems reset to the manufacturer's default settings prior to disposal.

## 8 Intended operating environment and application options

The FC360 fire detection system is a system used to protect people and property and comprises the following components:

- Core components
  - FC360 fire control panel
- Peripheral components
  - Fire detectors
  - Alarm devices
  - I/O modules
  - Floor repeaters
- Engineering component
  - Engineering laptop/PC
- Accessories
  - Key switch
  - Evacuation module [NL]
  - LED indicator (32 zones)
  - RS232/RS485 module
  - 4M card
- Third-party devices via RS232/RS485 module
  - External printer (via RS232 module)
  - Pager interface (ESPA, via RS485 module)
  - Danger management system (DMS, via RS485 module)

The envisaged applications and the operating environments are presented in the following chapters and figures.

- The technical room in which the panel is installed must be protected against unauthorized access.
- The panel must be protected against unauthorized access (e.g., in a separate room or behind reception desk).
- Take organizational measures to restrict access.
  - Define and implement processes to grant and revoke physical access.
- Assess the need for additional controls, such as location protection, additional restrictive access control for the building and rooms, security personnel, or monitoring.
- Protect publicly accessible data transmission lines against unauthorized access.
- Only connect allowed devices, e.g., DMS, ESPA interface and external printer, and protect them against unauthorized access.
- Make sure that no unknown hardware is physically connected to the system interfaces.
- Disable physical interfaces which are not being used in your operating environment.

### 8.1 Overall networked view

#### Intended Operational Environment

Access in the FS security zone to an FC360 system with the following components:

- FC360 fire control panel
- Engineering laptop/PC for temporary use
- RS232/RS485 module



Enable correct settings for applications specified below. Use only with third-party devices:

- External printer (via RS232 module)
- Pager interface (ESPA, via RS485 module)
- Danger management system (DMS, via RS485 module)



Fig. 2: Overall view, networked

- Panel FC360 fire control panel
- Third-party devices Third-party devices, e.g., ESPA
- PC Engineering laptop/PC

- An engineering laptop/PC is temporarily connected via the RJ45 interface.

Component	Requirements
Engineering laptop/PC	<ul style="list-style-type: none"> <li>• The operating system of the PC is the latest version of the approved system and has up-to-date patches.</li> <li>• Up-to-date antivirus software is active on the PC.</li> <li>• PC shall directly<sup>1</sup> connect to the panel while do engineering.</li> <li>• Not connected to other networks or systems (e.g. Internet connection via WLAN).</li> </ul>
Third-party device	<ul style="list-style-type: none"> <li>• The third-party device shall directly<sup>1</sup> connect to the panel.</li> <li>• Make sure the cables between control panel and the third-party devices are physically protected, e.g. with pipe protection, protect cabling against unauthorized access.</li> <li>• Make sure that no unknown hardware is physically connected to the interfaces.</li> <li>• Continuous monitoring of the third-party device is helpful in improving the physical security.</li> </ul>



<sup>1</sup> 'Directly' means that both devices and their cable connection are visible at the same time and any potential manipulations would therefore be detectable.

## 9 Checklist for permitted applications

Application case	Component	Requirement	Check performed YES / NO	Signature
Third-party device and panel engineering	Engineering laptop/PC	The operating system of the PC is the latest version of the approved system and has up-to-date patches.		
		Up-to-date antivirus software is active on the PC.		
		PC shall directly connect to panel while do engineering.		
		Not connected to other networks or systems (e.g. Internet connection via WLAN).		
		The default password (pin code) of authorized user or commissioning engineer has been changed.		
	Third-party device	The third-party device shall directly connect to panel.		
		Make sure the cables between control panel and the 3rd-party devices are physically protected, e.g. with pipe protection, protect cabling against unauthorized access.		
		Make sure that no unknown hardware is physically connected to the interfaces.		
		Continuous monitoring of the 3rd-party device is helpful in improving the physical security.		
	Chapter reference 3 hyperlink	Engineering laptop/PC	The operating system of the PC is the latest version of the approved system and has up-to-date patches.	
Up-to-date antivirus software is active on the PC.				
PC shall directly connect to panel while do engineering.				
Not connected to other networks or systems (e.g. Internet connection via WLAN).				
The default password (pin code) of authorized user or commissioning engineer has been changed.				

Table 1: Checklist for permitted applications

## 10 Maintenance of IT Components

The maintenance of IT security is a sustained process for which the corresponding tasks must be continually repeated. Each designated security measure must therefore be examined to determine whether it is sufficient to implement it once or whether implementation at regular intervals is required, such as regular antivirus software updates.

- Log all maintenance measures implemented.
- Observe the information in the 'IT Security Notices [→ 16]' chapter.
- Install security updates regularly.
- Run risk analyses on the security properties of the applied software at regular intervals.

You will find information on a corresponding risk analysis here, for example:

- [https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m\\_it\\_grundschutz.html](https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_it_grundschutz.html)
- [https://www.bsi.bund.de/EN/Topics/ITGrundschutz/Download/download\\_node.html](https://www.bsi.bund.de/EN/Topics/ITGrundschutz/Download/download_node.html)

# Index

<b>C</b>	
<b>Customer Support Center</b>	
Service .....	7
<b>D</b>	
<b>Download center</b>	
URL .....	10
<b>G</b>	
<b>Guideline</b>	
Password .....	30
PIN .....	30
<b>O</b>	
<b>Original language</b> .....	8
<b>P</b>	
<b>Password</b>	
Guideline .....	30
<b>PIN</b>	
Guideline .....	30
<b>S</b>	
<b>Service</b>	
Customer Support Center .....	7
<b>Source language</b> .....	8

Issued by  
Siemens Switzerland Ltd  
Smart Infrastructure  
Global Headquarters  
Theilerstrasse 1a  
CH-6300 Zug  
+41 58 724 2424  
[www.siemens.com/buildingtechnologies](http://www.siemens.com/buildingtechnologies)

© Siemens Switzerland Ltd, 2021  
Technical specifications and availability subject to change without notice.

---

A6V12080979\_en--\_a