

SIEMENS



FS720

Fire detection system

Commissioning

Maintenance

Troubleshooting

IP4

Impressum

Technical specifications and availability subject to change without notice.

© 2013 Copyright by Siemens Switzerland Ltd

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Issued by:

Siemens Switzerland Ltd.

Infrastructure & Cities Sector

Building Technologies Division

International Headquarters

Gubelstrasse 22

CH-6301 Zug

Tel. +41 41 724-2424

www.siemens.com/buildingtechnologies

Edition: 14.01.2013

Document ID: A6V10210416_f_en_--

Table of contents

1	About this document.....	7
1.1	Applicable documents.....	8
1.2	Technical terms.....	9
1.3	History of changes.....	9
2	Safety	11
2.1	Safety instructions	11
2.2	Safety regulations for the method of operation	12
2.3	Standards and directives complied with	14
2.4	Release Notes.....	14
3	Mounting/Installation.....	15
3.1	Installing and checking the detector line.....	15
3.1.1	Installing devices with serial number	15
3.1.2	Installing devices according to the wiring sequence.....	15
3.1.3	Checking the detector line.....	16
3.2	Mount and install 'Station'	16
4	Commissioning – overview.....	17
4.1	Commissioning variants.....	17
4.2	Definition of terms.....	18
4.3	Brief instructions on operating the 'Station'.....	19
5	Connectivity and communication with 'Station'.....	20
5.1	Connecting the PC to the station.....	20
5.2	Disconnecting PC from the 'Station'	20
5.3	Loading data to the 'Station'	21
5.4	Initializing 'Station'	21
5.5	Loading configuration from the PC to the 'Station'	23
5.6	Loading configuration from the 'Station' to the PC	24
5.7	Creating a back-up of the 'Site' configuration.....	25
6	General commissioning steps	27
6.1	Preparing 'Station' for commissioning.....	27
6.2	Preparing 'Station' for commissioning – without BDV installation	28
6.3	Auto-configuring 'Station'	28
6.4	Auto-configuring the detector line.....	28
6.5	Loading automatically created configuration to the PC	29
6.6	Adapting configuration	29
6.7	Switch on detector line.....	30
6.8	Switching off the detector line	30
6.9	Restarting the detector line	30
6.10	Switching off 'Zone'.....	30
6.11	Switching on 'Zone'.....	30
6.12	Reading in devices	31
6.13	Detaching the device	31

6.14	Delete the device on Person Machine Interface	31
6.15	Remove the elements.....	32
6.16	Switching on test mode.....	32
6.17	Switch on normal operation	32
6.18	Rectify localization errors.....	33
6.19	Checking 'Site' function.....	33
6.20	Completion work.....	34
7	A - Commissioning stand-alone 'Station' without PC	35
7.1	Configuring the power supply.....	36
7.2	Entering customer texts using the Person Machine Interface	36
7.3	Setting detector parameter sets	37
8	B1 - Commissioning stand-alone 'Station' with PC, without pre-configuration	38
9	B2 - Commissioning stand-alone 'Station' with PC, with pre-configuration.....	39
10	C- Commissioning networked 'Stations'	40
11	Adding a 'Station' to an existing 'Site'	41
12	Merging two 'Sites'	42
12.1	Adding 'Site' B to 'Site' A.....	43
12.2	Connecting 'Sites' physically to one another.....	45
13	Commissioning Ethernet switch (MM) FN2008-A1	46
13.1	Install Primary Setup Tool.....	47
13.2	Assign IP address.....	47
13.3	Configure FN2008-A1 using Internet browser	48
14	Commissioning safety module (firewall) FN2009-A1	49
14.1	Installing Security Configuration Tool.....	50
14.2	Selecting type and entering MAC address	50
14.3	Entering network settings.....	51
14.4	Creating IP service definitions.....	54
14.5	Creating firewall rules	55
15	Commissioning the fire brigade periphery module FCI2001-D1.....	57
16	Commissioning I/O card (remote transmission) FCI2007-A1 and I/O card (horn/monitored) FCI2009-A1	58
17	Testing detectors.....	59
17.1	Activate the detector.....	59
17.2	Testing logged test activations.....	59
18	Removing or replacing non-stationary devices	60
18.1	Base with loop contact.....	60
18.1.1	Temporarily removing an individual non-stationary device	60
18.1.2	Replacing non-stationary devices of the same type	60
18.1.2.1	Replacing a device	61
18.1.3	Replacing non-stationary devices of different types	61
18.1.3.1	Replacing a device in the 'Zone'.....	61

18.2	Base without loop contact.....	62
18.2.1	Temporarily removing an individual non-stationary device.....	62
18.2.2	Replacing non-stationary devices of the same type.....	62
18.2.3	Replacing a non-stationary device of a different type.....	63
18.2.3.1	Replacing a device in the 'Zone'.....	63
18.3	Temporarily removing multiple non-stationary devices.....	64
18.4	Permanently removing non-stationary devices.....	65
19	Change and extend the detector line.....	66
19.1	Extending the detector line to include additional devices.....	66
19.1.1	Mount and wire new devices.....	66
19.1.2	Configure a new device.....	66
19.2	Permanently removing stationary devices.....	67
19.3	Convert two stubs into a loop.....	67
19.4	Connecting a sub-stub to a loop.....	68
19.5	Replacing stationary devices of the same type.....	68
19.6	Replacing 'Manual call point' of the same type.....	69
19.6.1	Switching on the replace mode.....	69
19.6.2	Switching off replace mode.....	70
19.6.3	Testing 'Manual call point'.....	70
20	Updating the firmware of the 'Station'.....	71
20.1	Preparation and security.....	71
20.2	Updating the firmware of the main CPU and the additional CPUs – Overview.....	72
20.2.1	Standalone station and SAFEDLINK station.....	72
20.2.2	Router station and Ethernet station.....	73
20.2.3	Updating several 'Stations' simultaneously.....	73
20.3	Updating the firmware of the additional CPUs only – Overview.....	74
20.3.1	Standalone station and SAFEDLINK station.....	74
20.3.2	Router station and Ethernet station.....	75
20.4	Update only the BDV.....	76
20.4.1	Standalone station and SAFEDLINK station.....	76
20.4.2	Router station and Ethernet station.....	76
20.5	Converting the configuration.....	77
20.6	Setting Windows firewall.....	77
20.7	Updating the firmware of the main CPU and the additional CPUs.....	79
20.7.1	PMI & mainboard FCM2004.....	79
20.7.2	PMI & mainboard FCM2027.....	81
20.8	Update the firmware of the additional CPUs.....	84
20.9	Testing the firmware version of the additional CPUs.....	86
20.10	Creating diagnosis report.....	87
21	Updating the firmware of the peripheral devices.....	88
21.1	Updating the firmware of the MCL-USB adapter FDUZ221.....	88
21.2	Updating the firmware of the floor repeater terminal FT2010.....	89
21.3	Updating the firmware of the floor repeater display FT2011.....	91
21.4	Updating firmware of mimic display driver FT2001-A1.....	93
21.5	Updating the firmware of the radio gateway FDCW241.....	94

21.6	Updating firmware on the line tester FDUL221	95
21.7	Updating firmware on the line tester with serial interface FDUL221	97
22	Commissioning external printer	99
23	Maintenance.....	102
23.1	General	102
23.2	Spare parts.....	102
23.3	Testing and measuring instruments	103
23.4	Preparatory work	103
23.5	Test system data	104
23.6	Testing the 'Station'	104
23.7	Check the power supply	105
23.8	Testing the printer.....	106
23.9	Checking 'Site' function.....	106
23.10	Intervals for testing the system function	106
23.11	Completion work.....	107
24	Repair.....	108
24.1	Disconnecting 'Station' from the power supply.....	108
24.2	Spare parts.....	108
24.3	Fault messages on the Person Machine Interface.....	109
24.4	Fault indicators on components	109
24.5	Communication problems in networked systems.....	110
24.6	Non-stationary devices of the same type have been swapped over.....	110
24.7	Error message 'Topology is invalid'	111
24.8	Restart 'Station'	112
24.9	Restoring factory setting on the 'Station'	113
	Index	115

1 About this document

Goal and purpose

This document provides information and work steps for installing, commissioning, maintaining and repairing the fire detection system FS720. More information can be found in the corresponding documents under 'Applicable documents'.



To understand this document, you must have complete knowledge of document A6V10210355. See chapter 'Applicable documents'.

Scope

The information contained in this document is valid for introduction package IP4.

Target groups

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

Target group	Activity	Qualification
Installation personnel	<ul style="list-style-type: none"> Assembles and installs the product components at the place of installation. Carries out a performance check following installation. 	<ul style="list-style-type: none"> Has received specialist training in the area of building installation technology or electrical installations.
Commissioning personnel	<ul style="list-style-type: none"> Configure the product at the place of installation according to customer-specific requirements. Check the product operability and release the product for use by the operator. Searches for and corrects malfunctions. 	<ul style="list-style-type: none"> Has obtained suitable specialist training for the function and for the products. Has attended the training courses for commissioning personnel.
Maintenance personnel	<ul style="list-style-type: none"> Carries out all maintenance work. Checks that the products are in perfect working order. Searches for and corrects malfunctions. 	<ul style="list-style-type: none"> Has obtained suitable specialist training for the function and for the products.

Reference document and source language

- The source language of this document is German (de).
- The reference version of this document is the international version in English. The international version is not localized.

The reference document has the following designation:

ID_x_en_--

x = modification index, en = English, -- = international

Document identification

The document ID is structured as follows:

ID code	Examples
ID_ModificationIndex_Language_COUNTRY -- = multilingual or international	A6V10215123_a_de_DE A6V10215123_a_en_-- A6V10315123_a_--_--

Conventions for text marking

Markups

Special markups are shown in this document as follows:

▷	Requirement for a behavior instruction
⇒	Intermediate result of a behavior instruction
⇨	End result of a behavior instruction
[→ X]	Reference to a page number
'Text'	Quotation, reproduced identically
<Key>	Identification of keys

Supplementary information and tips



The 'i' symbol identifies supplementary information and tips for an easier way of working.

1.1 Applicable documents


Document ID	Title
A6V10210355	FS720 Fire Detection System, System Description
A6V10210362	FS720 Fire Detection System, Planning
A6V10210368	FS720 Fire Detection System, Product Data
A6V10210390	FS720 Fire Detection System, Mounting / Installation
A6V10210424	FS720 Fire Detection System, Configuration
A6V10211076	FC72x/FT724, Fire Control Panel / Fire Terminal, Operation
A6V10212047	Automatic Fire Detector, Technical Manual
A6V10224853	FS20/FS720 Fire Detection System, External Printer, Application Note
A6V10225323	FD720 Cerberus PRO, Synova, AlgoRex Detector System, Equipment Overview
A6V10227639	FDCW241 radio gateway, technical manual
A6V10227652	FS720 Cerberus PRO Fire Detection System, Components / Spare Parts / Repair Parts
A6V10229261	List of compatibility
A6V10260976	FS720 Fire Detection System, Site Conversion
008250	FDUL221 Line Tester, Operation
008860	FT201x, floor repeater terminal / floor repeater display, installation
009771	Open-source software (OSS) licenses
009854	FDUZ221 MCL-USB adapter, Installation

1.2 Technical terms

Term	Explanation
AI	Alarm indicator
BDV	Base data variant
C-NET	Addressed detector line
ES	Product version
MCL	Maintenance and commissioning link
'MCP'	Abbreviation for 'Manual call point'

You will find additional technical terms and their explanation in document A6V10210355, in the chapter 'Glossary'. See chapter 'Applicable documents'.

See also

 Applicable documents [→ 8]

1.3 History of changes

The reference document's modification index 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, have the modification index 'd' instead of 'a' if the reference document already has this modification index.

The table below shows this document's history of changes:

Modification index	Edition date	Brief description	
f	01.2013	Chapter 'Setting Windows firewall', for Windows 7 updated	
e	05.2012	Edition for IP4	
		New: Updating the firmware of the main CPU and additional CPUs in a single step Addition to chapter 'Setting Windows firewall', for Windows 7 Updating several 'Stations' simultaneously Update the firmware of the additional CPUs via GAP Creating a back-up of the 'Site' configuration Replacing the C-NET device: 20 s wait time instead of 40 s Updating the firmware of the peripheral devices: Resetting the line card no longer necessary Updating the FDCW241 FDCW221 removed Commissioning I/O card (remote transmission) FCI2007-A1 and I/O card (horn/monitored) FCI2009-A1	Revised: Creating diagnosis report Restart the station Checking 'Site' function Restoring factory settings Checking the detector line

Modification index	Edition date	Brief description
d	07.2010	Edition for MP3.0 XS: History of changes redefined and standardized Ethernet switch (MM) FN2008-A1 and safety module (firewall) FN2009-A1 added "Merging two sites" chapter added Chapter on 'Site' conversion removed. Reference to doc. A6V10244961 'Site conversion' added. Revised chapters: "Updating the firmware of the 'Station'", "Restarting 'Station'", "Restoring 'Station' to factory setting", "Loading configuration from the PC to the 'Station'" Chapter structure changed
c	08.2009	Modifications for MP1XS
b	05.2009	Modifications for MP1XS
a	11.2008	First edition


2 Safety

2.1 Safety instructions

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
DANGER	DANGER identifies a dangerous situation, which will result directly in death or serious injury if you do not avoid this situation.
WARNING	WARNING identifies a dangerous situation, which may result in death or serious injury if you do not avoid this situation.
CAUTION	CAUTION identifies a dangerous situation, which could result in slight to moderately serious injury if you do not avoid this situation.
<i>NOTICE</i>	<i>NOTICE</i> identifies possible damage to property that may result from non-observance.


How risk of injury is presented

Information about the risk of injury is shown as follows:

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

How possible damage to property is presented

Information about possible damage to property is shown as follows:


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

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, assembly, 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

	⚠ WARNING
	Electrical voltage Electric shock <ul style="list-style-type: none"> 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.

- 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 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.

Assembly, 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.

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

3 Mounting/Installation

3.1 Installing and checking the detector line

Most C-NET devices are installed on a base and can be changed with ease.

The bases of non-stationary C-NET devices and stationary C-NET devices must be installed and uninstalled when the C-NET detector line is switched off and disconnected from the power supply.

Prerequisites

- The C-NET detector line is not connected to the control panel and is disconnected from the power supply when the C-NET devices are being installed, wired and inserted.
- The C-NET detector line is tested with the line tester FDUL221.
- The control panel is commissioned by the commissioning personnel.

3.1.1 Installing devices with serial number



Before inserting or connecting an C-NET device, stick the **serial number** on the layout plan. The adhesive strip with the serial number can be found on the bottom of the device.

1. Install and wire the C-NET devices and stick the serial number for each device on the layout plan.
2. Install the detector dust caps on the optical point detector if necessary.
3. Install the designation plate if necessary.

3.1.2 Installing devices according to the wiring sequence

1. Install and wire the C-NET devices and document the wiring sequence in the layout plan.
2. Install the detector dust caps on the optical point detector if necessary.
3. Install the designation plate if necessary.

3.1.3 Checking the detector line

!	<p>NOTICE</p> <p>Simultaneous connection of line tester and C-NET detector line to the control panel</p> <p>Damage to line tester or control panel</p> <ul style="list-style-type: none"> Do not connect the line tester and the C-NET detector line to the control panel at the same time.
----------	--

Acceptance test

▷ The C-NET detector line is not connected to the control panel.

1. Connect the line tester FDUL221 to the newly installed C-NET detector line.
2. Test the C-NET detector line for short-circuits, open lines and earth faults.
3. Check the number of the devices on the C-NET detector line using the display on the line tester.
4. Check the branch-off position of the stubs and the number of devices at the stubs.
5. Check the type of all C-NET devices.
6. Remedy any errors you notice and carry out the acceptance test again.



You will find information on the line tester in document 008250. See chapter 'Applicable documents'.

Error when reading in the devices

If there are too many devices on the C-NET detector line for them all to be displayed on the line tester, a message to this effect is displayed. Proceed as follows should this happen:

- Read in the devices from both sides of the loop. To do this, change over the detector line cables as follows:
 - Connect the feed line of the detector line to connection socket B.
 - Connect the return line of the detector line to connection socket A.
- ⇒ The devices are read in from the other side of the loop. This allows the devices which previously couldn't be read in to be displayed.

3.2 Mount and install 'Station'

1. Mount and install the 'Station' according to the information in document A6V10210390. See chapter 'Applicable documents'.
2. Insert the cables for the detector lines and the mains supply into the housing but do not yet connect the the cables.
3. Insert the batteries but do not yet connect them.



You will find information about mounting and installation of 'Stations' components in the A6V10210390 document. See chapter 'Applicable documents'.


See also

Applicable documents [→ 8]

4 Commissioning – overview


The 'Stations' on the C-WEB, such as control panels FC722/FC724 and fire terminals FT724, are connected to the power supply and commissioned by the installation and commissioning personnel.

- Networked 'Stations' must only be commissioned with Cerberus-Engineering-Tool.
- Standalone control panels can be commissioned with or without Cerberus-Engineering-Tool.

	NOTICE
	Alternative commissioning procedure Faults during operation <ul style="list-style-type: none"> • Only the procedures described in this document are permitted.

4.1 Commissioning variants

In order to satisfy Directive 89/106/EEC (the Construction Products Directive – CPD), the firmware of a newly installed fire detection installation must be current market package version MP1XS or higher.


	NOTICE
	Firmware version of a newly installed fire detection installation not updated No CPD conformity <ul style="list-style-type: none"> • Compare the firmware version of a newly installed fire detection installation with the firmware version MP1XS. • Update the firmware if necessary.

The table below provides an overview of the procedure for commissioning the 'Stations'. The letters A, B1, B2 and C refer to the detailed descriptions in the following chapters.




		Standalone control panel	Networked 'Stations'
Without Cerberus-Engineering-Tool	No pre-configuration possible	A <ul style="list-style-type: none"> • Auto-configuration • Adaptations on the Person Machine Interface 	Not possible.
With Cerberus-Engineering-Tool	Without pre-configuration	B1 <ul style="list-style-type: none"> • Auto-configuration • Adaptations in Cerberus-Engineering-Tool 	C <ul style="list-style-type: none"> • Initialize the 'Stations' for networking • Read in C-NET devices line-by-line • Assign the logical elements in Cerberus-Engineering-Tool
	With pre-configuration	B2 <ul style="list-style-type: none"> • Read in devices line-by-line • Assign the logical elements in Cerberus-Engineering-Tool 	

Commissioning variants

4.2 Definition of terms


Auto-configuration	<p>Auto-configuration is performed using a command on the Person Machine Interface. In this process, the C-NET devices are read in and a configuration created.</p> <p>There are two types of auto-configuration.</p> <ul style="list-style-type: none"> ● Auto-configuration of an individual C-NET detector line ● Auto-configuration of Station <p>Auto-configuration results in the following:</p> <ul style="list-style-type: none"> ● One 'Section' is created for each C-NET detector line. ● One 'Zone' is created for each 'Sensor' 'Channel' ('Automatic detectors' and 'Manual call points'). ● One 'Technical zone' is created for each 'Input' 'Channel'. ● For all 'Output' channels and for each C-NET detector line, one 'Control' is created. ● One 'Control' is created for each alarm sounder. ● External alarm indicators are not auto-configured. ● Each 'Section' and each 'Zone' contains customer text, such as detector line no., zone no., and serial number of the device.
	<p>Detailed information about the result of auto-configuration can be found in the 'List of compatibility'.</p>
Pre-configuration	<p>The logical elements incl. customer texts are created in Cerberus-Engineering-Tool prior to commissioning:</p> <ul style="list-style-type: none"> ● In the 'Detection' task card up to and including 'Zone' level ● In the 'Control' task card up to and including 'Control' level ('Fire control', 'Evac control', 'Counter control') <p>In addition, the logical elements can subsequently be assigned as far as possible for alarming and control.</p> <p>Logical channels can be preconfigured. This makes sense if customer texts are to be configured down to this level.</p>
Read in by line	<p>The C-NET devices can be read in using one command via the Person Machine Interface. In this process, the C-NET devices are listed without sections and zones being created, i.e. no corresponding logical elements are created in the 'Detection tree' and 'Control tree'.</p>
Adaptations	<p>The following procedures are examples of adaptations:</p> <ul style="list-style-type: none"> ● Entering customer text for logical elements ● Changing detector parameter sets ● Configuring alarm devices ● 'Controls': Configuring ● Configuring the power supply
Non-stationary C-NET devices	<p>Point detectors installed on a base apart from radio detectors.</p>
Stationary C-NET devices	<p>All devices apart from point detectors, e.g.:</p> <ul style="list-style-type: none"> ● Manual call point ● Radio detector ● Input/output modules ● Alarm sounder ● Line separator ● Radio gateway ● Floor repeater terminal ● Floor repeater display ● Mimic display driver

4.3 Brief instructions on operating the 'Station'

Buttons	Description
 = <MENU>	Opens the main menu.
<▲> and <▼>	Navigation buttons for selecting the next or previous entry in a list.
<◀> and <▶>	Navigation buttons for changing to a higher or lower level in the hierarchy.
 = <ok>	Opens or runs a selected entry or menu item.
 = <C>	Cancels all operating procedures and closes an open list or an open window.
<1> to <9>	Buttons on the keypad to enter: <ul style="list-style-type: none"> ● PIN ● Shortcut ● Address ● Parameter ● Customer text

You will find detailed instructions for operating the 'Stations' in document A6V10211076. See chapter 'Applicable documents'.

See also


 Applicable documents [→ 8]

5 Connectivity and communication with 'Station'

A PC does not have to be directly connected to a 'Station' to be able to communicate with a 'Station' in the 'Site'. The PC can be connected to any place in the Ethernet.

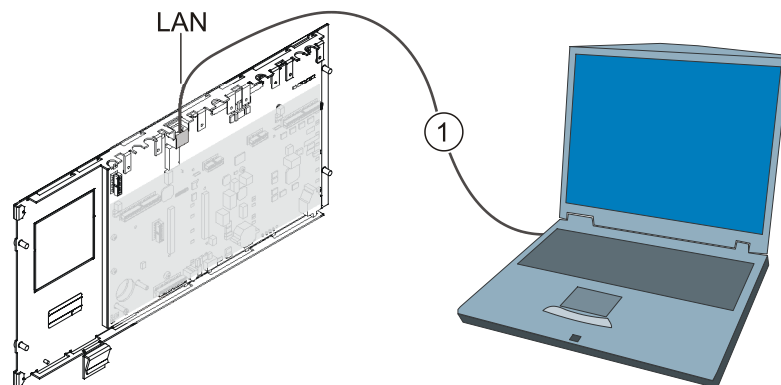
Detailed information about the connection variants can be found in the 'Establishing connection from PC to FS720 network' chapter in document A6V10210424. See chapter 'Applicable documents'.

See also

 Applicable documents [→ 8]

5.1 Connecting the PC to the station

For most commissioning, maintenance and repair work a PC with installed Cerberus-Engineering-Tool is required. The figure below shows the connection between the PC and 'Station'.




Rear panel of operating unit and PC

LAN Ethernet connection

1 Cable, type CAT 5 or CAT 7, crossover, max. 100 m

5.2 Disconnecting PC from the 'Station'

As the IP address is bound to the MAC address while there is a connection between the PC and the 'Station' and as it remains in the cache even in the case of a short break in the connection of ≤ 2 min., you must observe the following instructions.

	NOTICE
	Incorrect disconnection of 'Station' Establishing a connection to other 'Station' is not possible <ul style="list-style-type: none"> Disconnect the PC from the 'Station' as described in the following instructions.

The connection between the PC and the 'Station' must be disconnected as follows:

1. Select 'Commissioning' > 'Disconnect' in Cerberus-Engineering-Tool.
2. Disconnect the cable connection between PC and 'Station'.
3. Wait ≥ 2 min. before you establish a connection to another 'Station'.

5.3 Loading data to the 'Station'

Data is loaded from Cerberus-Engineering-Tool to the 'Station' when the following commands are performed.

- 'Initialize station'
- 'Download site'



If you use a number of network cards on the PC, observe the information in the chapter 'IP settings for several network cards' in document A6V10210424. See chapter 'Applicable documents'.

The table below shows which data is overwritten in the station 'Station'.

Command	Overwrites the BDV	Sets the address of the 'Station'	Overwrites the configuration
'Initialize station' ¹	Yes	Yes	Yes
'Download site'	Yes	No	Yes ²

¹ Command is only performed for the 'Station' that is connected to the PC via LAN.

² The configuration of all 'Stations' in the 'Site' can be overwritten as an option.

See also

- Loading configuration from the PC to the 'Station' [→ 23]
- Initializing 'Station' [→ 21]

5.4 Initializing 'Station'

- Each 'Station' in a fire detection system with several networked 'Stations' must have a unique address.
- Once a 'Station' has been started for the first time or once the firmware on the main CPU has been updated, a 'Station' has the address '1'. Networked 'Stations' must therefore all be initialized.
- If two 'Sites' are merged to form one 'Site', the 'Stations' with the same addresses in the added 'Site' must each be given a new address.
- The 'Initialize station' procedure issues the 'Station' an address within the 'Site' according to the configuration in Cerberus-Engineering-Tool.



A standalone 'Station' does not have to be initialized.



If you use a number of network cards on the PC, observe the information in the chapter 'IP settings for several network cards' in document A6V10210424. See chapter 'Applicable documents'.

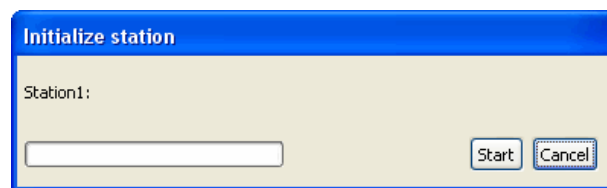
'Initialize 'Station'

!	<p>NOTICE</p> <p>Connection module (card cage) FCA2006-A1 defective or installed incorrectly Control panels identified incorrectly, e.g. FC726 identified as FC724.</p> <ul style="list-style-type: none"> Check that the connection module (card cage) FCA2006-A1 is installed correctly.
----------	---

▷ The PC is connected locally to the 'Station'.

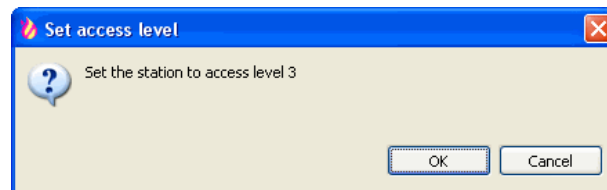
1. Highlight the 'Station' you want to initialize in the 'Hardware tree'.
2. Select the 'Commissioning' > 'Initialize station' menu item.

⇒ The following window is opened:



3. Click on 'Start'.

⇒ The following window is opened:




4. Press <MENU> on the 'Station' and enter a valid PIN.
5. Click on 'OK' in the 'Set access level' window.
 - ⇒ The 'Station' is initialized.
 - ⇒ The 'Station' is restarted.
 - ⇒ After a few minutes, the 'Buzzer' sounds twice.
6. Press <Acknowledge> on the Person Machine Interface to switch off the 'Buzzer'. Do not perform any more actions on the 'Station' until the 'Buzzer' has sounded for the second time.

See also

📄 Loading data to the 'Station' [→ 21]

5.5 Loading configuration from the PC to the 'Station'

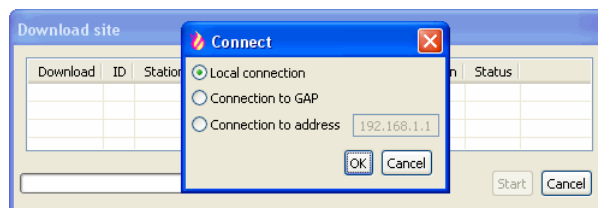
You can use the 'Download site' function to load the configuration of one 'Site' from the Cerberus-Engineering-Tool on the PC into the 'Station'.

	<p>NOTICE</p> <p>Different network configuration in 'Cerberus-Engineering-Tool' and networked 'Site'</p> <p>When the selection displayed for 'Download site' is manually modified, in special cases¹ it may be necessary to reset a 'Station' to the factory setting as well as a 'Initialize station'.</p> <ul style="list-style-type: none"> • Do not modify the selection displayed for 'Download site' in normal cases. • Check the sequence when loading different configuration states in special cases¹. • After any change of the network configuration, make sure that all 'Stations' in the 'Site' for the 'Download site' procedure are selected and can be accessed. • Temporarily update non-accessible 'Stations' to the latest status of the global network configuration prior to integration in the network.
---	---

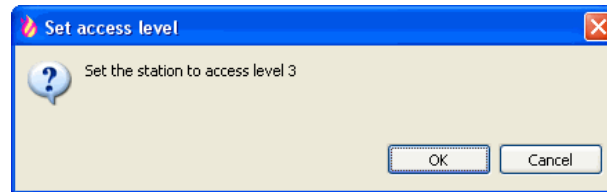


If you use a number of network cards on the PC, observe the information in the chapter 'IP settings for several network cards' in document A6V10210424. See chapter 'Applicable documents'.

- ▷ The 'Site' is opened in Cerberus-Engineering-Tool.
 - ▷ The PC is connected to the 'Station'.
 - ▷ Networked 'Stations' are initialized.
 - ▷ 'Station' and Cerberus-Engineering-Tool have the same 'Site' ID.
 - ▷ 'Station' and Cerberus-Engineering-Tool are in the same organizational unit.
1. Select 'Commissioning' > 'Download site'.
 - ⇒ The 'Download site' and 'Connect' windows are opened.



2. Select 'Connect' in the window and click on 'OK'.
 - ⇒ The 'Stations' are listed in the 'Download site' window.
3. Select the 'Stations' whose configuration you would like to load from 'Cerberus-Engineering-Tool' to the 'Stations' and click on 'Start'.
 - ⇒ The 'Set access level' window may be opened with the 'Set the station to access level 3' prompt. Press <MENU> on the 'Station', enter the PIN and press <ok>.



4. Click on 'OK' in the 'Set access level' window.
 - ⇒ The 'Action confirmation' window opens.
5. Click on 'Yes'.
 - ⇒ The configuration is loaded to the 'Station'.
 - ⇒ The advancement status is displayed in the 'Download site' window.
 - ⇒ The 'Station' restarts.
 - ⇒ After a few minutes, the 'Buzzer' sounds twice.
6. Press <Acknowledge> on the Person Machine Interface to switch off the 'Buzzer'. Do not perform any more actions on the 'Station' until the 'Buzzer' has sounded for the second time.

¹ Examples of special cases:

- A 'Station' will be added to a networked 'Site' and a new network configuration will be loaded upon initialization of this 'Station', different from the global network configuration of the connected 'Site'.
- During the 'Download site' procedure a 'Station' is temporarily not accessible.

Both examples can result in the 'Station' no longer starting after the 'Download site' procedure and the above actions having to be carried out.

See also

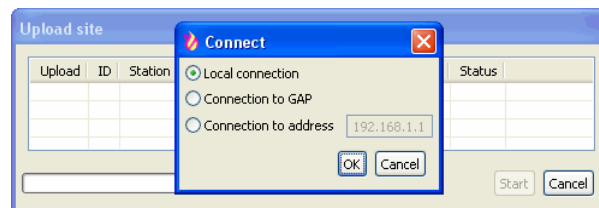
Loading data to the 'Station' [→ 21]

5.6 Loading configuration from the 'Station' to the PC

The 'Upload site' function can be used to load the configuration of a 'Site' to Cerberus-Engineering-Tool on the PC.

- ▷ The 'Site' is opened in Cerberus-Engineering-Tool.
- ▷ The PC is connected to the 'Station'.
- ▷ 'Station' and Cerberus-Engineering-Tool have the same 'Site' ID.
- ▷ 'Station' and Cerberus-Engineering-Tool are in the same organizational unit.

1. Select 'Commissioning' > 'Upload site'.
 - ⇒ The 'Upload site' and 'Connect' windows are opened.



2. Select 'Connect' in the window and click on 'OK'.
 - ⇒ The 'Stations' are listed in the 'Upload site' window.

3. Select the 'Stations' whose configuration you would like to load to Cerberus-Engineering-Tool and click on 'Start'.
⇒ The 'Action confirmation' window opens.
4. Click on 'Yes'.
⇒ The configuration is loaded to the PC.
⇒ The advancement status is displayed in the 'Upload site' window.

5.7 Creating a back-up of the 'Site' configuration

With the 'Create backup embedded configuration' function, you can create a back-up file of the 'Site' configuration.

The following conditions must be satisfied for a complete back-up:

- All of the 'Stations' in the 'Site' must be networked and commissioned.
- The 'Site' IDs for all 'Stations' must match the 'Site' ID for the 'Site' loaded in Cerberus-Engineering-Tool.
- The BDVs for all 'Stations' must be compatible with the BDV for the 'Site' loaded in Cerberus-Engineering-Tool.
 - The BDVs are compatible when the major version and the minor version are identical. The bugfix version is not relevant for the compatibility.
- The country codes of the BDVs for all 'Stations' must match the BDV for the 'Site' loaded in Cerberus-Engineering-Tool.

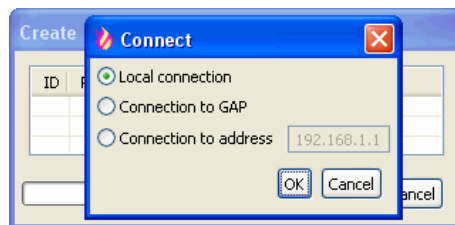


You will find Information about BDV names and versions in document A6V10210424. See chapter 'Applicable documents'.

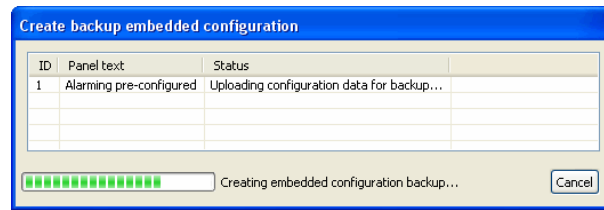
If the above-mentioned conditions are not satisfied, a corresponding message is displayed and an incomplete back-up file created. In this instance, 'incomplete' is added to the file name of the back-up file.

Creating a back-up

- ▷ The 'Site' is opened in Cerberus-Engineering-Tool.
- ▷ The PC is connected to a 'Station'.
- 1. Select 'Commissioning' > 'Create backup embedded configuration'.
⇒ The 'Create backup embedded configuration' and 'Connect' windows are opened.



2. Select 'Connect' in the window and click on 'OK'.
⇒ The 'Site' configuration is loaded to the PC and saved as a back-up file.
⇒ The advancement status is displayed in the 'Create backup embedded configuration' window.



Back-up file

- The back-up file is saved in the following directory as standard:
C:\Documents and Settings\All Users\Application Data\Siemens\FX7230
- The back-up file has the following name:
<'Site' name>_<back-up counter>(_incomplete).fsc
Example: Test_Site_007_incomplete.fsc
 - 'Site' name: Name of the 'Site'.
 - Back-up counter: Three-digit number that is automatically assigned to each back-up.
 - 'incomplete': If it was not possible to create a complete back-up, 'incomplete' is added to the file name.
- A maximum of ten 'Site' back-up files are saved. If more than ten back-up files are created, the oldest file is automatically deleted.



In the pre-settings, you can define that a back-up file is created automatically each time a configuration is loaded from the PC to the 'Station' using the 'Download site' command. To do this, select 'Options' > 'Preferences' > 'Commissioning preferences'.

6 General commissioning steps

The following chapter contains general commissioning steps that are referred to in several chapters.

6.1 Preparing 'Station' for commissioning

1. Connect the cables for the detector lines and the periphery devices.
2. Connect the power supply (mains and batteries).
 - ⇒ The 'Station' starts and reads in the internal hardware.
 - ⇒ During start-up, the 'AVERIA' LED flashes and the display shows the progress.
 - ⇒ During start-up, the firmware version F-FXS7211 is displayed.
3. Wait until the display indicates the selection of the BDV.
4. Press the 'Install' softkey and confirm with the 'Yes' softkey.
 - ⇒ The 'Station' restarts.
 - ⇒ During this process, the 'AVERIA' LED flashes and the display shows the progress.
5. Wait until only the green 'Sistema Servicio' LED lights up, the display shows the normal condition and the 'Station' can be operated.
6. Press <MENU> and select the 'Login/logout' menu item.
 - ⇒ You are prompted to enter a PIN.
7. Enter the PIN and confirm with <ok>.
 - ⇒ The 'User successfully logged in' message is displayed.
 - ⇒ The main menu is shown on the display.
8. Check the firmware of the 'Station' to ensure that it is up to date. To do this select the 'Topology' > 'Hardware tree' > 'Station' > 'More Options' > 'Show details' menu items.
 - ⇒ The 'Station' version and configuration data are displayed.
9. Update the firmware if necessary.
10. Enter the date and time. To do this, select the 'Settings/administration' > 'System commands' > 'Set system time' menu items.



Additional messages may be displayed depending on the configuration of the 'Station'.

6.2 Preparing 'Station' for commissioning – without BDV installation

1. Connect the cables for the detector lines and the periphery devices.
2. Connect the power supply (mains and batteries).
 - ⇒ The 'Station' starts and reads in the internal hardware.
 - ⇒ During start-up, the 'AVERIA' LED flashes and the display shows the progress.
 - ⇒ During start-up, the firmware version F-FXS7211 is displayed.
3. Wait until the display indicates the selection of the BDV.
 - ⇒ The 'Station' is prepared for commissioning.



It is not necessary to install the BDV for the further procedure. This saves having to restart the 'Station'.

6.3 Auto-configuring 'Station'

1. Select 'Topology' > 'Hardware tree' > 'Station' in the main menu.
2. Press the 'More Options' softkey and select 'Execute commands'.
3. Select the 'Auto-configure station' command.
 - ⇒ The 'Station' is auto-configured.
 - ⇒ The following message is shown following successful auto-configuration: 'Command executed'



You will find detailed information on the result of the auto-configuration in the 'List of compatibility'. See chapter 'Applicable documents'.

See also

Applicable documents [→ 8]

6.4 Auto-configuring the detector line

	<p>NOTICE</p> <p>Incorrect order for reading in a loop</p> <p>Error when reading in a loop</p> <p>The C-NET detector lines are detected as stubs during the first system start-up, e.g. 'Line' 11, 'Line' 12 (2-digit line number), even if they are connected as a loop.</p> <ul style="list-style-type: none"> • Always select the first 'Line' to read in a loop, in this case, 'Line' 11. 'Line' 12 is then read in automatically. After reading in, a loop is indicated with a 1-digit line number, in this case, as 'Line' 1. • Proceed in the same way from 'Line' 21/22 (loop 2) to 'Line' 41/42 (loop 4).
--	---

1. In the main menu, select 'Topology' > 'Hardware tree' > 'Station' > Line card > Detector line.
2. Press the 'More Options' softkey and select 'Execute commands'.
3. Select the 'Auto-configure line' command.
 - ⇒ The 'C-NET' detector line is auto-configured.
 - ⇒ The following message is shown following successful auto-configuration: 'Command executed'



You will find detailed information on the result of the auto-configuration in the 'List of compatibility'. See chapter 'Applicable documents'.

See also

Applicable documents [→ 8]

6.5 Loading automatically created configuration to the PC

1. Select the 'File' > 'New site' menu item.
 - ⇒ The 'Create new site' window opens.
2. Select the 'Upload from station(s)' option field.
3. Click on 'Next'.
 - ⇒ The 'Create site by uploading from station(s)' and 'Connect' windows are opened.
4. In the window, 'Connect' select 'Local connection' and then click on 'OK'.
 - ⇒ The configuration is loaded to 'Cerberus-Engineering-Tool'.
 - ⇒ The advancement status is displayed in the 'Create site by uploading from station(s)' window.
 - ⇒ The 'Site properties' window is opened after loading.
5. Change the entries if required and click on 'OK'.
 - ⇒ The 'New site confirmation' window opens.
6. Click on 'Yes'.
 - ⇒ The 'Site' is opened in Cerberus-Engineering-Tool.

6.6 Adapting configuration

Adapt the configuration in the 'Site' in Cerberus-Engineering-Tool e.g.:

- Changing customer texts
- Setting the properties and the parameter sets
- Changing allocation of 'Zones' and 'Sections'
- Configuring controls
- Configuring the operating and display units
- Configuring the network



You will find information about configuring a 'Site' in document A6V10210424. See chapter 'Applicable documents'.

See also

Applicable documents [→ 8]

6.7 Switch on detector line

1. In the main menu, select 'Topology' > 'Hardware tree' > 'Station' > Line card > Detector line.
2. Press the 'More Options' softkey and select 'Execute commands'.
3. Select the 'Detector line ON' command.
 - ⇒ The yellow 'MENSAJES DE DESCONEXIONES' LED goes out.
 - ⇒ The C-NET detector line is switched on.

6.8 Switching off the detector line

1. In the main menu, select 'Topology' > 'Hardware tree' > 'Station' > Line card > Detector line.
2. Press the 'More Options' softkey and select 'Execute commands'.
3. Select the 'Detector line OFF' command.
 - ⇒ The yellow 'MENSAJES DE DESCONEXIONES' LED lights up.
 - ⇒ The C-NET detector line is switched off.

6.9 Restarting the detector line

1. In the main menu, select 'Topology' > 'Hardware tree' > 'Station' > Line card > Detector line.
2. Press the 'More Options' softkey and select 'Execute commands'.
3. Select the 'Restart line' command.
 - ⇒ The C-NET detector line is restarted.
 - ⇒ The following message is displayed following restart: 'Command executed'.


6.10 Switching off 'Zone'

1. Select 'Topology' > 'Detection tree' > 'Area' > 'Section' > 'Zone' in the main menu.
2. Press the 'More Options' softkey and select 'Execute commands'.
3. Select the 'Off' command.
 - ⇒ The yellow 'MENSAJES DE DESCONEXIONES' LED lights up.
 - ⇒ The 'Zone' is switched off.

6.11 Switching on 'Zone'

1. Select 'Topology' > 'Detection tree' > 'Area' > 'Section' > 'Zone' in the main menu.
2. Press the 'More Options' softkey and select 'Execute commands'.
3. Select the 'On' command.
 - ⇒ The yellow 'MENSAJES DE DESCONEXIONES' LED goes out.
 - ⇒ The 'Zone' is switched on.

6.12 Reading in devices

	<p>NOTICE</p> <p>Incorrect order for reading in a loop</p> <p>Error when reading in a loop.</p> <p>The C-NET detector lines are detected as stubs during the first system start-up, e.g. 'Line' 11, 'Line' 12 (2-digit line number), even if they are connected as a loop.</p> <ul style="list-style-type: none">• Always select the first 'Line' to read in a loop, in this case, 'Line' 11. 'Line' 12 is then read in automatically. After reading in, a loop is indicated with a 1-digit line number, in this case, as 'Line' 1.• Proceed in the same way from 'Line' 21/22 (loop 2) to 'Line' 41/42 (loop 4).
---	--

1. In the main menu, select 'Topology' > 'Hardware tree' > 'Station' > Line card > Detector line.
2. Press the 'More Options' softkey and select 'Execute commands'.
3. Select the 'Read in installed devices' command.
 - ⇒ The C-NET devices are read in.
 - ⇒ The following message is shown following successful reading in: 'Command executed'

6.13 Detaching the device

If you want to remove an C-NET device for good, uninstall the device and if required, the base and connect the wires of the detector line.

You will find more information about installing and uninstalling in the documentation for the corresponding 'C-NET' device.

6.14 Delete the device on Person Machine Interface


1. Mark the corresponding device fault message.
2. Press the 'More Options' softkey.
3. Select the 'Show topology' menu item.
 - ⇒ The logical channel is displayed. For some devices, 'Device' is displayed directly.
4. Press the 'More Options' softkey.
5. Select the 'Jump to link' menu item.
 - ⇒ The physical channel is displayed.
6. Press the 'Upper level' softkey.
 - ⇒ 'Device' is displayed.
7. Press the 'More Options' softkey.
8. Select the 'Execute commands' menu item.
9. Select the 'Remove/delete device' command.
 - ⇒ The control panel deletes the physical representation of the removed device.
 - ⇒ The logical channel element remains in the 'Zone'.

6.15 Remove the elements

If you have uninstalled an C-NET device for good, the corresponding elements, e.g. the 'Zone' must be removed from the logical structure trees in Cerberus-Engineering-Tool. You can search for elements using the 'Find' function.

You will find more information in document A6V10210424. See chapter 'Applicable documents'.

See also

 Applicable documents [→ 8]

6.16 Switching on test mode

1. Select 'Topology' > 'Detection tree' in the main menu.
 2. Select the element you want to switch to test mode: 'Area', 'Section' or 'Zone'.
 3. Press the 'More Options' softkey and select 'Execute commands'.
 4. Select a command from the following table.
- ⇒ The yellow 'DETECTORES EN PRUEBAS' LED lights up.
- ⇒ The element is in test mode.

Element	Command
Area	<ul style="list-style-type: none"> ● 'Non-MCP zones det.test' ● 'MCP zones det.test'
Section	<ul style="list-style-type: none"> ● 'Non-MCP zones det.test' ● 'MCP zones det.test'
Zone	<ul style="list-style-type: none"> ● 'Detector test'

6.17 Switch on normal operation



There is a shortened procedure for switching individual 'Zones' to normal operation. The procedure is described in the following section: "Switching 'Zone' to normal operation"

'Switching 'Area', 'Section' or 'Zone' to normal operation

1. Select 'Topology' > 'Detection tree' in the main menu.
 2. Select the element you want to switch to normal operation: 'Area', 'Section' or 'Zone'.
 3. Press the 'More Options' softkey and select 'Execute commands'.
 4. Select a command from the following table.
- ⇒ The element is switched to normal operation.
- ⇒ The yellow 'DETECTORES EN PRUEBAS' LED goes out.

Element	Command
Area	<ul style="list-style-type: none">• 'Non-MCP zones det.test END'• 'MCP zones det.test END'
Section	<ul style="list-style-type: none">• 'Non-MCP zones det.test END'• 'MCP zones det.test END'
Zone	<ul style="list-style-type: none">• 'Detector test END'

Commands under 'Execute commands'



You can also switch to normal operation at superordinate level for the command in question. Test mode can also be exited in the 'Zone', 'Section' or 'Area', for example.

'Switching 'Zone' to normal operation

There is a shortened procedure for switching individual 'Zones' to normal operation:

1. Select 'Message summary' > 'Test message' in the main menu.
2. Select the displayed 'Zone' in test mode and press the 'Execute Commands' softkey.
3. Select the 'Detector test END' command.
 - ⇒ The 'Zone' is switched to normal operation.
 - ⇒ The yellow 'DETECTORES EN PRUEBAS' LED goes out.

6.18 Rectify localization errors

1. Use 'Topology' > 'Hardware tree' > 'Station' > 'Line card' > 'Detector line' to select the corresponding detector line in the main menu.
2. Press the 'More Options' softkey and select 'Execute commands'.
3. Select the 'Accept replaced devices' command.
 - ⇒ The fault messages are no longer displayed.



If devices are missing or the device types do not correspond to the C-NET topology, error messages will continue to be displayed.

6.19 Checking 'Site' function

Test the functions of the 'Site' in the various test modes:

You will find information about testing a 'Site' in the chapter 'Testing' in document A6V10211076. See chapter 'Applicable documents'.

See also

Applicable documents [→ 8]

6.20 Completion work

1. Check the time and date and reset these. To do this, select 'Settings/administration' > 'System commands' > 'Set system time' in the main menu.
2. Set the PIN for the access levels 1, 2.1, 2.2 and 3. To do this, select 'Settings/administration' > 'Create PIN' in the main menu.
3. Fit the housing cover.
4. Label the installation plate, which should be outside on the housing, with the site number and the date of commissioning.
 - To do this, use a solvent-resistant pen.

7 A - Commissioning stand-alone 'Station' without PC



The procedure in this chapter is only valid for standalone 'Stations'.

In this commissioning variant, a 'Station' without a PC and a Cerberus-Engineering-Tool are commissioned.

Prerequisites

- The detector lines and C-NET devices are installed.
- The acceptance test has been carried out for the detector lines.
- The 'Station' is installed, but the batteries are not connected yet.
- The cables for the detector lines and the mains supply have been inserted in the 'Station', but not connected.



You will find additional information about the individual steps on the specified pages.

Commissioning

1. If necessary, configure the power supply. Link [→ 36]
2. Prepare the 'Station' for commissioning. Link [→ 27]
3. Perform auto-configuration:
 - 'Auto-configure 'Station' Link [→ 28]
 - OR
 - Auto-configure detector lines individually Link [→ 28]
4. Adapt the auto-configuration in the Person Machine Interface, e.g.:
 - Changing customer texts. Link [→ 36]
 - Setting parameter sets of the C-NET devices. Link [→ 37]
5. Test the function of the 'Site' and remedy the problems, if any. Link [→ 33]
6. Perform the completion tasks. Link [→ 34]

7.1 Configuring the power supply

If the 'Station' is equipped with a power supply and batteries, the power supply does not have to be configured. In all other cases the power supply must be configured. This may be done by wiring accordingly.


The following table shows the cases in which the monitoring signals of the power supply must be re-wired.

Operation mode	Connector on peripheral board	Connect with
Operation without batteries	X1 / pin 1 '#BATT'	X1 / pin 4 #COMMON
Operation without power supply unit	X1 / pin 1 '#BATT'	X1 / pin 4 #COMMON
	X1 / pin 2 '#CONV'	X1 / pin 4 #COMMON
	X1 / pin 3 '#MAINS'	X1 / pin 4 #COMMON

Configuring the power supply

You will find the pin assignments in document A6V10210368. See chapter 'Applicable documents'.

See also

 Applicable documents [→ 8]

7.2 Entering customer texts using the Person Machine Interface

1. Select 'Topology' > 'Detection tree' > 'Area' > 'Section' > 'Zone' in the main menu.
2. Select the element you want to label with a customer text.
3. Press the 'More Options' softkey and select 'Execute commands'.
4. Select the 'Set customer text' command.
5. Enter the customer text using the numeric keypad.
6. Press <ok> to save the customer text. There is no need to restart the Station.

Showing the customer text on the display

- All elements apart from 'Zone':
If a message associated with an element appears, the corresponding customer text is displayed. If no customer text is assigned to this element, the customer text of the next superordinate element, e.g. 'Detector' > 'Line' > 'Line card', appears.
- 'Zone' element:
If an alarm message for a 'Zone' appears, the customer text of the detector (sensor) is displayed. The customer text of the 'Zone' appears if no customer text is assigned to the 'Detector'. The customer text of the next superordinate element ('Detector' > 'Zone' > 'Section' > 'Area') appears if no customer text is assigned to the 'Zone' either.

7.3 Setting detector parameter sets

1. Select 'Topology' > 'Detection tree' > 'Area' > 'Section' > 'Zone' > 'Detect.' in the main menu.
 2. Press the 'More Options' softkey.
 3. Select 'Execute commands'.
 4. Select the corresponding command:
 - 'Select PS MANNED'
 - 'Select PS UNMANNED'
 - 'Select PS'
 5. Select the desired parameter set.
- ⇒ The following message is displayed: 'Command executed'

8 B1 - Commissioning stand-alone 'Station' with PC, without pre-configuration

First auto-configure the 'Station' in this commissioning variant. Then adapt the auto-configuration manually in Cerberus-Engineering-Tool.



The procedure in this chapter is only valid for standalone 'Stations'.

Prerequisites

- The detector lines and C-NET devices are installed.
- The acceptance test has been carried out for the detector lines.
- The 'Station' is installed, but the batteries are not connected yet.
- The cables for the detector lines and the mains supply have been inserted in the 'Station', but not yet connected.
- Cerberus-Engineering-Tool is installed on the PC.
- The current firmware and BDV are available on the PC.



You will find additional information about the individual steps on the specified pages.

Commissioning

1. Prepare the 'Station' for commissioning. Link [→ 27]
2. Perform auto-configuration:
 - 'Auto-configure 'Station' Link [→ 28]
 - OR
 - Auto-configure detector lines individually Link [→ 28]
3. Connect the PC to the 'Station'. Link [→ 20]
4. Load the automatically created configuration to the PC. Link [→ 29]
5. Adapt the configuration in Cerberus-Engineering-Tool. Link [→ 29]
6. Load the configuration from the PC to the 'Station'. Link [→ 23]
7. Test the function of the 'Site'. Link [→ 33]
8. Remedy any errors you notice and load the corrected configuration from the PC to the 'Station'. Link [→ 23]
9. Disconnect the PC from the 'Station'. Link [→ 20]
10. Perform the completion tasks. Link [→ 34]

9 B2 - Commissioning stand-alone 'Station' with PC, with pre-configuration

In this commissioning variant, in Cerberus-Engineering-Tool, first manually configure a 'Site' up to 'Line' level. Then read in the C-NET devices and adapt the configuration manually in Cerberus-Engineering-Tool.

Prerequisites

- The detector lines and C-NET devices are installed.
- The acceptance test has been carried out for the detector lines.
- The 'Station' is installed, but the batteries are not connected yet.
- The cables for the detector lines and the mains supply have been inserted in the 'Station', but not yet connected.
- Cerberus-Engineering-Tool is installed on the PC.
- The current firmware and BDV are available on the PC.




You will find additional information about the individual steps on the specified pages.

Commissioning

1. In Cerberus-Engineering-Tool create a 'Site' and configure it manually to the 'Zone' level.
2. Prepare the 'Station' for commissioning - without BDV installation. Link [→ 28]
3. Connect the PC to the 'Station'. Link [→ 20]
4. Load the configuration from the PC to the 'Station'. Link [→ 23]
5. Read-in the C-NET devices. Link [→ 31]
6. Load the configuration from the 'Station' to the PC. Link [→ 24]
7. Adapt the configuration in Cerberus-Engineering-Tool. Link [→ 29]
8. Load the configuration from the PC to the 'Station'. Link [→ 23]
9. Test the function of the 'Site'. Link [→ 33]
10. Remedy any errors you notice and load the corrected configuration from the PC to the 'Station'. Link [→ 23]
11. Disconnect the PC from the 'Station'. Link [→ 20]
12. Perform the completion tasks. Link [→ 34]

10 C- Commissioning networked 'Stations'

	NOTICE
	<p>Commissioning as standalone 'Station'</p> <p>Commissioned as standalone 'Station', 'Stations' cannot be combined to form a networked 'Site' later on.</p> <ul style="list-style-type: none"> • Initialize networked 'Stations' using a network address right from the start.

Prerequisites

- The detector lines and C-NET devices are installed.
- The acceptance test has been carried out for the detector lines.
- The 'Station' is installed, but the batteries are not connected yet.
- The cables for the detector lines and the mains supply have been inserted in the 'Station', but not yet connected.
- Cerberus-Engineering-Tool is installed on the PC.
- The current firmware and BDV are available on the PC.



You will find additional information about the individual steps on the specified pages.

Commissioning

1. Create a 'Site' and the 'Stations' in Cerberus-Engineering-Tool and pre-configure, if required.
2. Prepare each 'Station' individually for commissioning - without BDV installation. Link [→ 28]
3. Connect the PC to each 'Station' individually. Link [→ 20]
4. Initialize each 'Station' individually. Link [→ 21]
5. Read-in the C-NET devices for all 'Stations'. Link [→ 31]
6. Load the configuration from the 'Station' to the PC. Link [→ 24]
7. Adapt the configuration in Cerberus-Engineering-Tool. Link [→ 29]
8. Load the configuration from the PC to the 'Station'. Link [→ 23]
9. Test the function of the 'Site'. Link [→ 33]
10. Remedy any errors you notice and load the corrected configuration from the PC to the 'Station'. Link [→ 23]
11. Disconnect the PC from the 'Station'. Link [→ 20]
12. Perform the completion tasks. Link [→ 34]

11 Adding a 'Station' to an existing 'Site'

Prerequisites

- The detector lines and C-NET devices are installed.
- The acceptance test has been carried out for the detector lines.
- The 'Station' is installed, but the batteries are not connected yet.
- The cables for the detector lines and the mains supply have been inserted in the 'Station', but not yet connected.
- Cerberus-Engineering-Tool is installed on the PC.
- The current firmware and BDV are available on the PC.



You will find additional information about the individual steps on the specified pages.

Commissioning

1. In Cerberus-Engineering-Tool, create the 'Station' to be integrated and configure it, if required.
2. Prepare the 'Station' for commissioning - without BDV installation. Link [→ 28]
3. Connect the PC to the 'Station'. Link [→ 20]
4. Initialize the 'Station'. Link [→ 21]
5. Read-in the C-NET devices. Link [→ 31]
6. Load the configuration from the 'Station' to the PC. Link [→ 24]
7. Adapt the configuration in Cerberus-Engineering-Tool. Link [→ 29]
8. Load the configuration from the PC to the 'Station'. Link [→ 23]
9. Test the function of the 'Site'. Link [→ 33]
10. Remedy any errors you notice and load the corrected configuration from the PC to the 'Station'. Link [→ 23]
11. Disconnect the PC from the 'Station'. Link [→ 20]
12. Perform the completion tasks. Link [→ 34]

12 Merging two 'Sites'

You can merge two 'Sites' to form one 'Site'.

Prerequisites

- Both 'Sites' are in the same organizational unit.
- Both 'Sites' have the same firmware version and BDV version (version 32 or higher)
- Both 'Sites' have one network.
- Both 'Sites' combined have at most the allowed number of 'Stations' for a 'Site'.
- Both 'Sites' combined have at most the allowed number of SAFEDLINK sub-nets for a 'Site'.
- Wiring between the two 'Sites' is prepared:
 - The 'Ethernet switch (MM) FN2008-A1' is installed in the 'Stations' intended as router station and connected to an optical network (C-WEB/LAN).
 - Large SAFEDLINK sub-nets are in the original state and not yet divided.
 - Ethernet sub-net are in the original state.



You will find additional information about the individual steps on the specified pages.

Commissioning

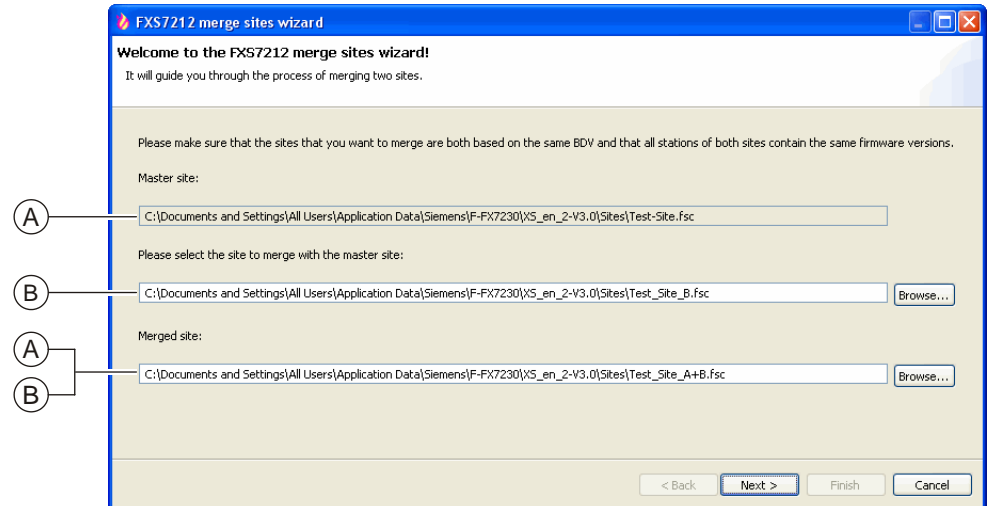
1. Add Site' B to 'Site' A. Link [→ 43]
2. Initialize all 'Stations' that have a new address. Link [→ 21]
3. Load the configuration of all 'Stations' in 'Site' A from the PC to the 'Station'. Link [→ 23]
4. Connect the 'Sites' physically to one another. Link [→ 45]
5. Load the configuration of the merged 'Site' from the 'Station' to the PC. Link [→ 24]
6. Adapt the configuration in Cerberus-Engineering-Tool. Link [→ 29]
7. Load the configuration from the PC to the 'Station'. Link [→ 23]
8. Test the function of the 'Site'. Link [→ 33]
9. Remedy any errors you notice and load the corrected configuration from the PC to the 'Station'. Link [→ 23]

12.1 Adding 'Site' B to 'Site' A

► 'Site' A is opened in Cerberus-Engineering-Tool.

1. In the 'Edit' menu, select the 'Merge sites' menu item.

⇒ The following window is opened:



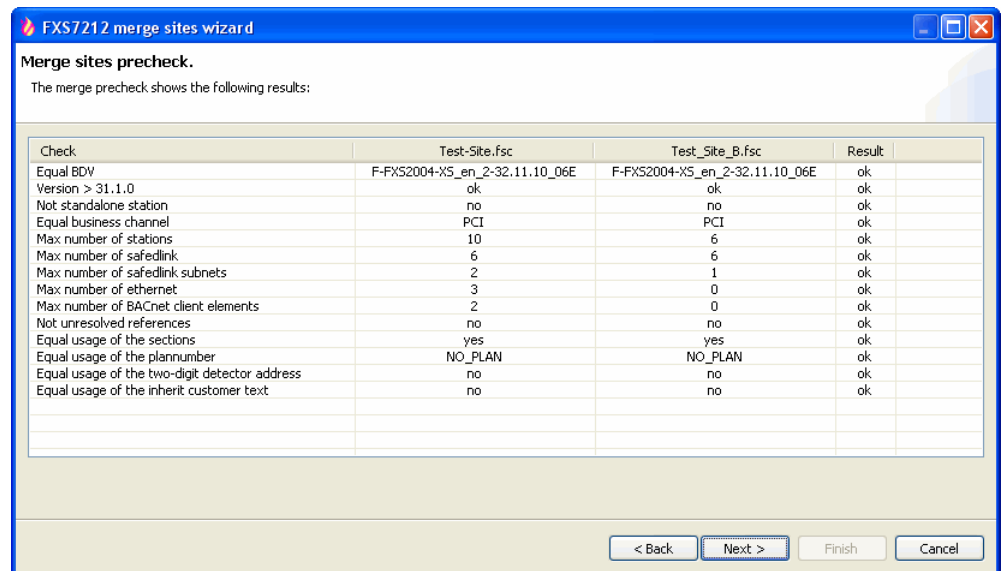
2. Enter the path and name of 'Site' B that you would like to merge with 'Site' A.

3. Enter the path and name of the new merged 'Site'.

4. Click on 'Next'.

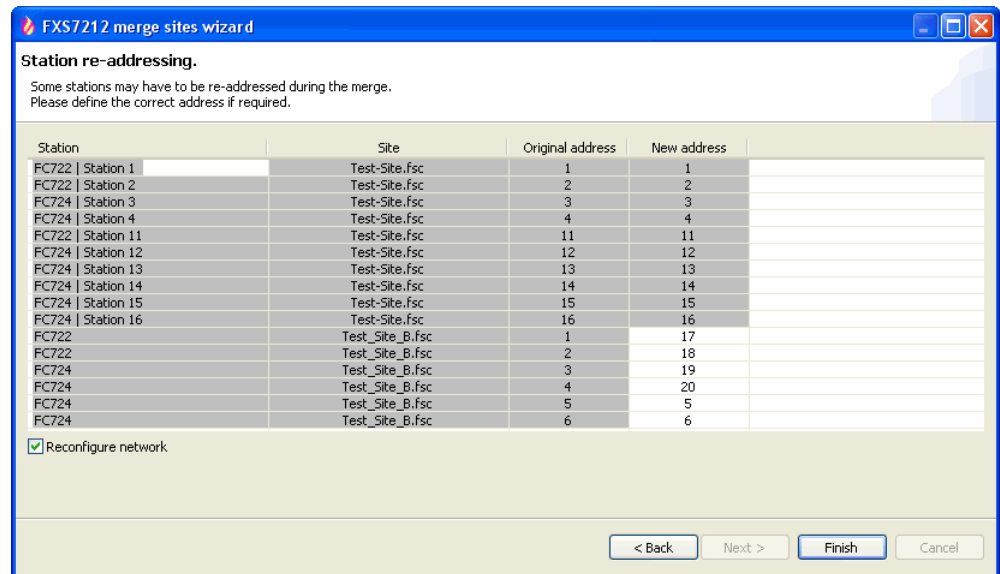
⇒ The conditions for merging are checked.

⇒ The results are listed in the window below:

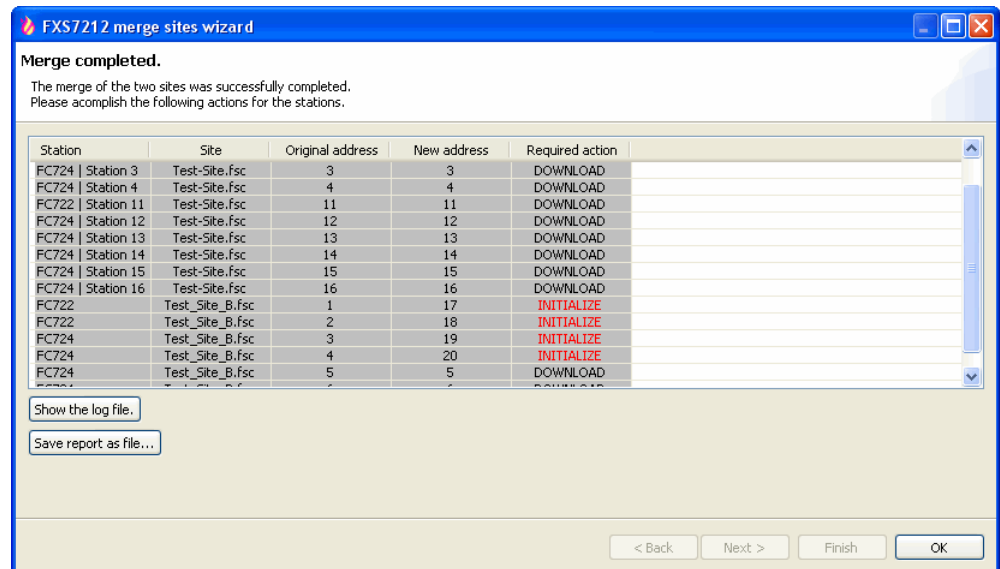


5. Click on 'Next' if 'ok' is everywhere in the 'Result' column. If 'ok' is not everywhere, click on 'Cancel' and ensure that all the conditions that are listed in the 'Check' column are satisfied.

⇒ Cerberus-Engineering-Tool checks whether there are address conflicts at 'Stations' levels and suggests a possible new address.



6. Check the suggested addresses for the 'Stations' in 'Site' B and adapt them if necessary. The 'New address' column can be edited.
7. Check the 'Reconfigure network' checkbox if you want to reset the existing network configurations for the original 'Sites'. All network configuration values are then reset to the standard values.
8. Click on 'Finish'.
 - ⇒ The 'Sites' are merged.
 - ⇒ The following window is opened. In the 'Required action' column, you are shown which 'Stations' need initializing and for which 'Stations' a download is sufficient.




9. Click on 'Show the log file.' to view the protocol.
10. Click on 'Save report as file...' to save and print a merging report. This report also shows which 'Stations' must be initialized.
11. Click on the 'OK' button to close the window.

12.2 Connecting 'Sites' physically to one another

Connect the two 'Sites' physically to one another.


You will find more information in document A6V10210390. See chapter 'Applicable documents'.

See also

 [Applicable documents \[→ 8\]](#)

13 Commissioning Ethernet switch (MM) FN2008-A1

This description focuses on correctly integrating the 'Ethernet switch (MM) FN2008-A1' in the fire detection installation. More information about the product can be found on the data carrier in the scope of supply and at the following address: <http://support.automation.siemens.com> (Manufacturer designation: Scalance X204-2)

	NOTICE
	<p>Alternate products for 'Ethernet switch (MM) FN2008-A1'</p> <p>No compliance with EN 54</p> <ul style="list-style-type: none"> For an EN-54-compliant fire detection installation, you must use the permitted 'Ethernet switch (MM) FN2008-A1'.



The 'Ethernet switch (MM) FN2008-A1' is a class A equipment and may cause radio interference in residential areas. If interference does occur, observe the relevant information in document A6V10210390. See chapter 'Applicable documents'.

Commissioning

1. Install the 'Primary Setup Tool' software. Link [→ 47]
2. Assign the IP address. Link [→ 47]
3. Configure FN2008-A1 using the Internet browser Link [→ 48]
4. In Cerberus-Engineering-Tool, create the links you want e.g. for the following monitoring functions in a 'Technical zone'.
 - Redundant power
 - Display error contact




You will find detailed instructions on creating a link in document A6V10210424. See chapter 'Applicable documents'.



The FN2008-A1 has no IP address in the factory setting. You must manually assign the IP address.

See also

-  Applicable documents [→ 8]

13.1 Install Primary Setup Tool



The 'Primary Setup Tool' software is included in the scope of supply for the FN2008-A1.

- Start 'Primary Setup Tool' installation.
- ⇒ Primary Setup Tool is installed.
- ⇒ The DLC and PROFINET RT protocols are installed.
- ⇒ Primary Setup Tool recognizes one or more connected FN2008-A1 without IP address via the DLC protocol.



The FN2008-A1 is displayed as X204-2 in the Primary Setup Tool.

13.2 Assign IP address



The FN2008-A1 is displayed as X204-2 in the Primary Setup Tool.

- ▷ Primary Setup Tool is installed on the PC.
- ▷ Several FN2008-A1 are physically linked in the system.
- 1. Connect the PC to any available FN2008-A1 port P1...P4 using a network cable.
- 2. Start the Primary Setup Tool via 'Start' > 'Programs' > 'Simatic'.
 - ⇒ Primary Setup Tool lists one or more FN2008-A1 (X204-2).
- 3. Select each FN2008-A1 one after the other and issue a unique IP address (192.168.1.xxx) to each FN2008-A1.
- 4. Click on the connected FN2008-A1 in the tree view and select the 'Load' menu item.
 - ⇒ The assigned IP address is saved to the FN2008-A1.
- 5. Repeat the 'Load' process for each FN2008-A1.
 - ⇒ Each FN2008-A1 in the system has an individual IP address.

13.3 Configure FN2008-A1 using Internet browser



A configuration is available via the localization manager. We recommend using the configuration and if necessary making system-specific adaptations.



NOTICE

Incorrect settings of the ports

Malfunction

- The factory setting 'auto-negotiation' for the ports may not be changed.

1. Open the Internet browser and enter the FN2008-A1's address in the address field.
⇒ The login window opens.
 2. Login:
 - User name = 'admin'
 - Password = 'admin'
 3. Select 'System' > 'Passwords' in the tree view and set a new password for the following fields:
 - 'New User Password'
 - 'New Admin Password'
 4. Confirm the entered password with 'Confirmation'.
 5. Click 'Set Values'.
 6. Select 'X204-2' > 'Ring' in the tree view and check the 'Enable ring redundancy' checkbox.
 - Select the 'Automatic Redundancy Detection' redundancy mode.
 7. Select 'X204-2' > 'Fault Mask' in the tree view and check the 'Enable Link Down Monitoring' checkbox for each connected port:
 - Port 5 and 6 = Ring
 - Port 1 = The connected 'Station'
 - Port 2 to 4 only if more stations 'Stations' are connected
- ⇒ FN2008-A1 is configured.

14 Commissioning safety module (firewall) FN2009-A1

This description focuses on correctly configuring and integrating the 'Security module (firewall) FN2009-A1' in the fire detection installation. More information about the product can be found on the data carrier in the scope of supply and at the following address: <http://support.automation.siemens.com> (Manufacturer designation: Scalance S612)



A configuration is available via the localization manager. We recommend using the configuration and if necessary making system-specific adaptations.

Commissioning

1. Install the 'Security Configuration Tool' software. Link [→ 50]
2. Select the type and enter the MAC address. Link [→ 50]
3. Enter the network settings. Link [→ 51]
 - Load configuration.
4. Create IP service definitions. Link [→ 54]
5. Create firewall rules. Link [→ 55]
 - Load configuration.



The 'Security module (firewall) FN2009-A1' is a class A equipment and may cause radio interference in residential areas. If interference does occur, observe the relevant information in document A6V10210390. See chapter 'Applicable documents'.



The FN2009-A1 has no IP address in the factory setting. You must manually assign the IP address.

	<p>NOTICE</p> <p>FN2009-A1 is not in the factory setting and already has an IP address</p> <p>It is not possible to upload a new configuration</p> <ul style="list-style-type: none"> • Press the Reset button on the live FN2009-A1.
--	--

14.1 Installing Security Configuration Tool



The 'Security Configuration Tool' software is included in the scope of supply for the FN2009-A1.

- Install the 'Security Configuration Tool' software.
- ⇒ The software is installed in the standard path 'SIMATIC' > 'SCALANCE' > 'Security' > 'Security Configuration Tool'.
- ⇒ FN2009-A1 can be configured.



The FN2009-A1 is displayed as S612V2 in the Security Configuration Tool.

14.2 Selecting type and entering MAC address



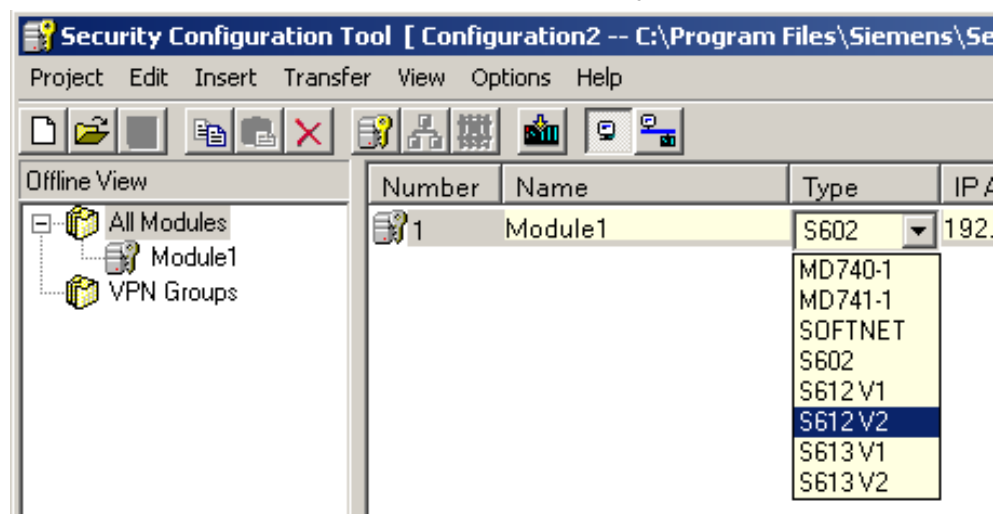
The corresponding MAC address can be found on the front of the FN2009-A1.
The FN2009-A1 is type S612V2.

Preparation

- ▷ The PC is connected to FN2009-A1.
- ▷ 'Security Configuration Tool' is started.
- 1. Create a new project using the 'Project' > 'New' menu and enter the administrative project data, 'User name' and 'Password'.
- 2. Save the new project.
- 3. Select 'View' > 'Advanced Mode'.
- ⇒ More entry masks for required settings can be viewed.

Selecting type

- 1. Highlight the field below the 'Type' designation.
- ⇒ The button for the dropdown list field is displayed.



- 2. Select 'S612V2'.
- ⇒ Type is selected.

Entering MAC address

▷ The MAC address is known.

1. Double-click on the field below the 'MAC Address' designation.

⇒ The MAC address can be edited.

Subnet Mask int.	Default Router	MAC Address	Comment
		08-00-06-00-00-00	

2. Enter the MAC address for the FN2009-A1.

⇒ MAC address is entered.

14.3 Entering network settings

▷ The network topology is known.

▷ 'Advanced Mode' is selected.

● Enter the network settings in the following order:

- External IP address 'IP Address ext.'
- Routing mode 'Routing Mode'
- Router network data 'Router'
- Load the network settings to FN2009-A1.

Entering external IP address, 'IP Address ext.'

1. Double-click on the field below the 'IP Address ext.' designation.

⇒ The external IP address for the FN2009-A1 can be edited.

2. Enter the following IP address: 10.169.29.80.

Entering routing mode, 'Routing Mode'



The following settings apply for the planned network access to GAP with activated DHCP server.

'192.168.201.X' must be changed accordingly for network access to the standby router or with IP address details.

▷ 'Module 1' is highlighted in the 'View' window.

1. Press <F4> on the keyboard or open the 'Edit' > 'Properties' menu.

⇒ The 'Module Properties' window is displayed:

Module Properties - Module1

Network | Firewall Settings | VPN | Routing Modus | DHCP-Server

Router

Net ID	Subnet Mask	Router IP

Add Router Remove Router

OK Cancel Help

2. Select the 'Routing Mode' tab.

⇒ The following entry mask is displayed:

Module Properties - Routing-Smpl

Network | Firewall Settings | SSL Certificate | Time Synchronization | Logging | Nodes

VPN | Routing Modus | DHCP-Server

Routing

☒ Routing active

external module IP address 10.169.29.80 external subnetmask 255.255.255.0

internal module IP address 192.168.201.2 internal subnetmask 255.255.255.0

NAT

☐ NAT active

☐ Allow Internal>External for all users

external IP address	internal IP address	Direction

Add Remove

NAPT

☐ NAPT active

external IP address 10.169.29.80

external port	internal IP address	internal port

Add Remove

OK Cancel Help

3. Check the 'Routing active' checkbox.

4. Enter the following 'internal module IP address': 192.168.201.2.

5. Confirm input with 'OK'.

⇒ 'Internal sub-net mask' is automatically created.

⇒ 'Routing Mode' is active.

Entering router network data, 'Router'



The following settings apply for the planned network access to GAP with activated DHCP server.

1. Open the 'Module Properties' window again.
 - ⇒ The 'Network' tab is displayed.
2. Click on 'Add Router'.
 - ⇒ The 'Sub-net Mask' '255.255.255.0' is already entered.
3. Correct the 'Sub-net Mask' from '255.255.255.0' to '255.255.0.0'.
4. Enter the following network data:
 - 'Router IP': 192.168.201.1
 - 'Network ID': 192.168.0.0
5. Confirm input with 'OK'.
 - ⇒ The router network data is entered.

Load the network settings to FN2009-A1.

- ▷ MAC address is entered.
 - ▷ IP addresses are entered.
1. Highlight the FN2009-A1 module in the project.
 2. Select the 'Transfer > 'To Module' menu.
 - ⇒ The network settings are loaded to FN2009-A1.
 - ⇒ Network settings are entered.

14.4 Creating IP service definitions



NOTICE

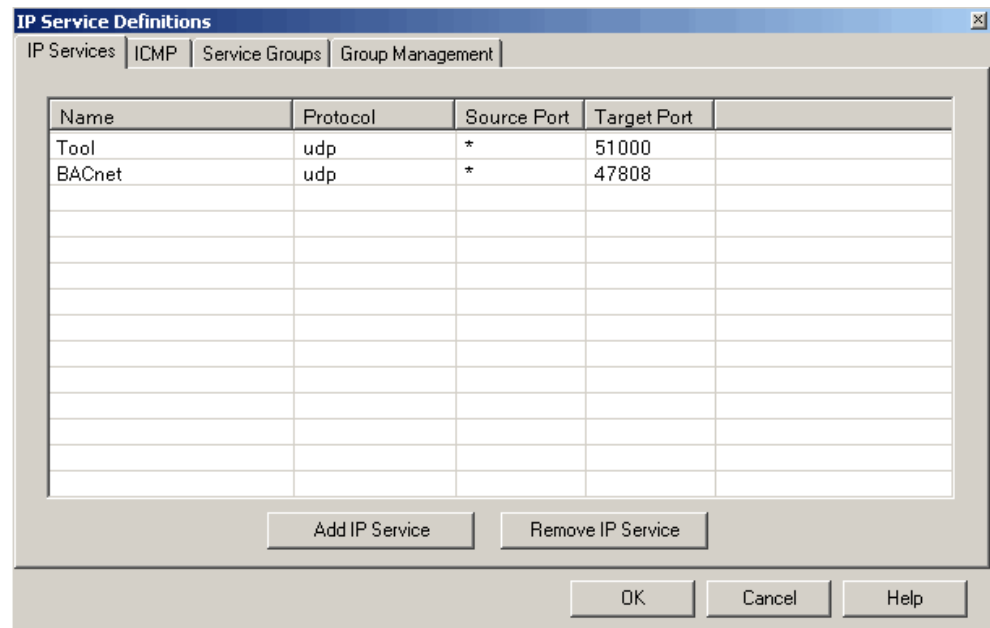
Different BACnet port settings in FN2009-A1 and Cerberus-Engineering-Tool

No communication possible

- Configure the same BACnet port in FN2009-A1 and Cerberus-Engineering-Tool.

1. Open the 'Options' > 'IP Service Definitions' menu.

⇒ The 'IP Service Definitions' window is opened.



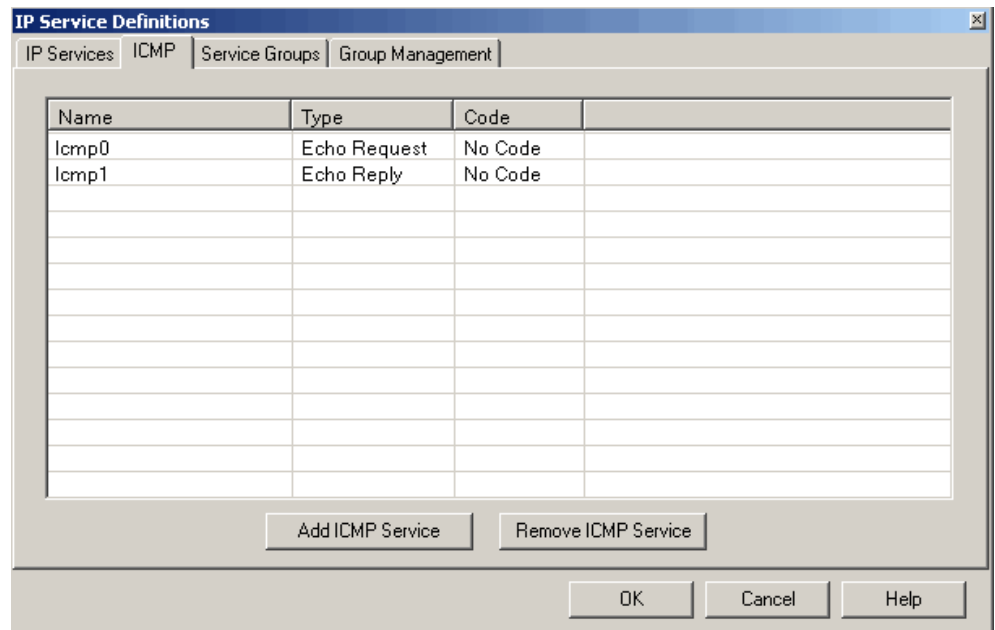
2. Select the 'IP Services' tab.
3. Click on 'Add IP Service'.

⇒ One row can be edited for one IP service.
4. Enter the two IP services required as shown in the figure above:
 - 'Name': Tool, 'Protocol': udp, 'Source Port': *, 'Target Port': 51000
 - 'Name': BACnet, 'Protocol': udp, 'Source Port': *, 'Target Port': 47808

⇒ Required IP services are created.
5. Select the 'ICMP' tab.
6. Click on 'Add ICMP Service'.

⇒ One row can be edited for one ICMP service.
7. Enter the two optional ICMP services required as shown in the figure below:
 - 'Name': ICMP0, 'Type': Echo Request, 'Code': No code
 - 'Name': ICMP1, 'Type': Echo Reply, 'Code': No code

⇒ Optional IP services are created.

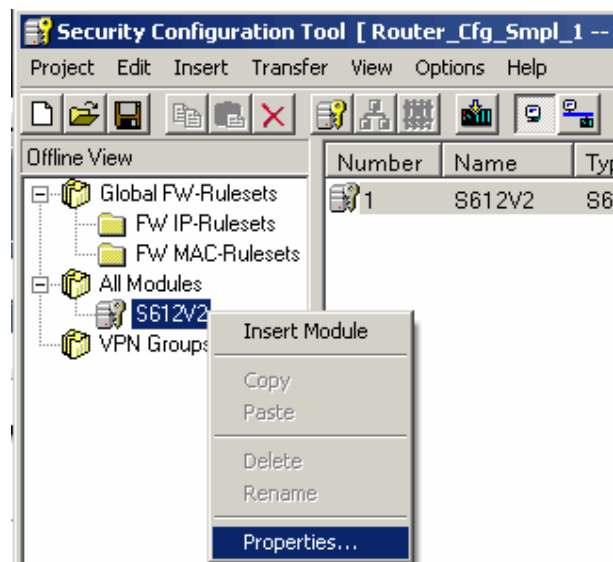


8. Confirm input with 'OK'.
- ⇒ 'IP Service Definitions' are created.

14.5 Creating firewall rules

- ▷ IP service definitions are created.
- ▷ The network addresses are known.

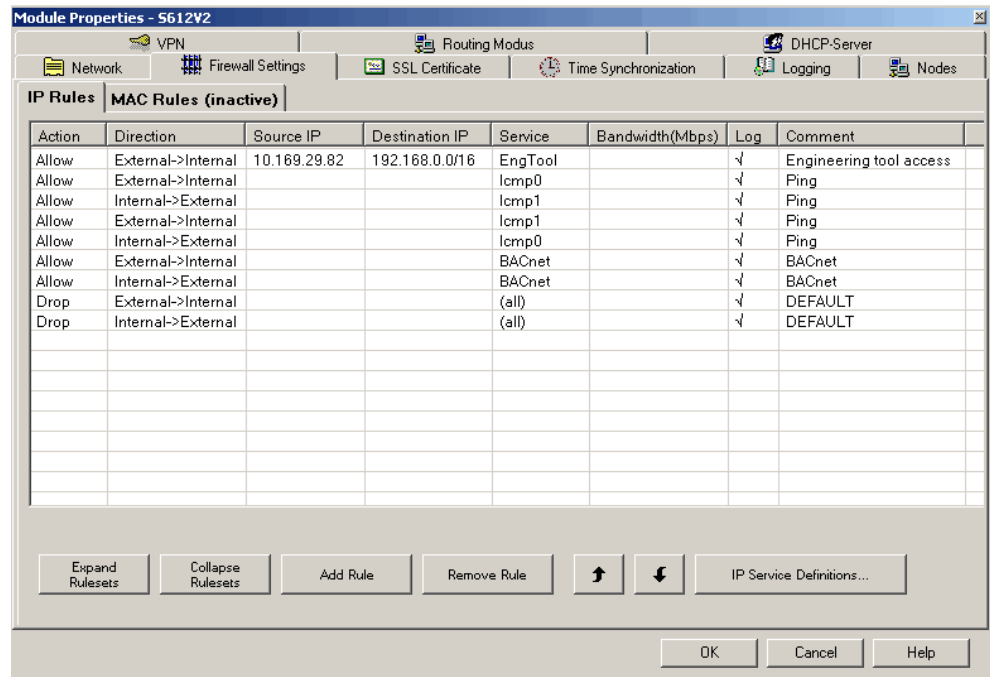
1. Right-click on the module for which you want to create firewall rules.



2. Select 'Properties...'.
 - ⇒ The 'Module Properties' window for the selected module is displayed:

3. Select the 'Firewall Settings' tab.

⇒ The following window is displayed without entries:



4. Click on 'Add Rule' for each firewall rule you would like to create.

5. Select the corresponding settings and IP services from the dropdown list fields.

6. Enter the required IP addresses.

7. Confirm input with 'OK'.

⇒ The firewall rules are created.

Loading the firewall rules to FN2009-A1

▷ The firewall rules are created.

1. Highlight the FN2009-A1 module in the project.

2. Select the 'Transfer > 'To Module' menu item.

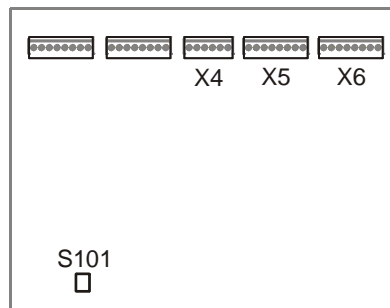
⇒ The firewall rules are loaded to FN2009-A1.

15 Commissioning the fire brigade periphery module FCI2001-D1

The fire department periphery module FCI2001-D1 monitors the monitored inputs and outputs for short-circuit and open line. The resistance values of the lines may be read in and stored at the push of a button. If a deviation from the quiescent value is detected, the control panel evaluates a short-circuit or an open line.

The following table shows the monitored inputs and outputs:

Terminal	Pin	Function
X4	4, 5 and 1, 2	Remote transmission or transmission device (RT Alarm) and release element ('FSE')
X5	7, 8	'Key depot' (tamper monitoring)
X6	5, 6	Local alarm



View of the fire department periphery module

X4–X6 Connection terminals

S101 Button

Procedure

1. Check the connected lines for short-circuit and open line.
2. Connect the lines.
 - ⇒ During the commissioning of the control panel, fault messages are indicated, provided that there are any deviations from the basic settings.
3. Press the push-button S101.
 - ⇒ The resistance values are read in.

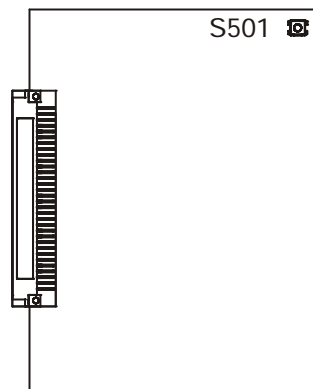
16 Commissioning I/O card (remote transmission) FCI2007-A1 and I/O card (horn/monitored) FCI2009-A1

With the I/O card (remote transmission) FCI2007-A1 and I/O card (horn/monitored) FCI2009-A1, the monitored outputs are monitored for short-circuit and open line. The resistance values of the lines may be read in and stored at the push of a button. If a deviation from the quiescent value is detected, the control panel evaluates a short-circuit or an open line.

The following outputs must be calibrated upon commissioning:

- FCI2007-A1: 'OUT1' to 'OUT3'
- FCI2009-A1: 'OUT1' to 'OUT8'

You will find more information about the FCI2007-A1 and FCI2009-A1 I/O cards and planning monitored outputs in documents A6V10210362 and A6V10210368. See chapter 'Applicable documents'.



I/O card FCI2007-A1 and/or FCI2009-A1

S501 Button

Procedure

1. Check the connected lines for short-circuit and open line.
2. Connect the lines.
 - ⇒ During the commissioning of the control panel, fault messages are indicated, provided that there are any deviations from the basic settings.
3. Press the S501 button.
 - ⇒ The resistance values are read in.



You can also read in the resistance values via the control panel's Person Machine Interface.

17 Testing detectors

The commissioning personnel perform the function test for the automatic fire detectors and the 'Manual call points'.



You will find additional information about the individual steps on the specified pages.


- ▷ The detector line has been commissioned.
- 1. Switch the test mode on. Link [→ 32]
- 2. Initiate the detector. Link [→ 59]
- 3. Switch normal operation on. Link [→ 32]
- 4. Test the logged test activations. Link [→ 59]

17.1 Activate the detector

- ▷ 'DETECTORES EN PRUEBAS' is switched on.
- 1. Activate all automatic 'Detectors' and 'Manual call points' using the corresponding tools.
- 2. Write down the sequence of the test activations.
- ⇒ The alarm indicator for the activated detector flashes at each test activation.
- ⇒ If an external alarm indicator is connected and correspondingly configured, the external alarm indicator also lights up.

You will find information about triggering detectors in document A6V10212047. See chapter 'Applicable documents'.

See also

 Applicable documents [→ 8]

17.2 Testing logged test activations

1. Test the logged test activations. This can be done in two ways:
 - Person Machine Interface: Select 'Event memory' in the main menu.
 - Cerberus-Engineering-Tool: Select the 'Commissioning' > 'Upload site event memory' menu items.
2. Rectify existing errors if necessary, e.g. if the alarm indicator has not flashed or no test entries exist.

18 Removing or replacing non-stationary devices

The product range includes bases with or without a loop contact.

18.1 Base with loop contact

If an C-NET device is removed, the loop contact prevents the C-NET detector line from being interrupted and thereby prevents a fault message.

The work described in this chapter may be performed when the C-NET detector line is switched on.

18.1.1 Temporarily removing an individual non-stationary device

It may be possible that an C-NET device must be temporarily removed from the base. Afterwards the same C-NET device must be re-inserted at exactly the same place in the C-NET.

1. Remove the C-NET device.
 - ⇒ The control panel detects that the C-NET device is missing and reports a 'Fault'.
2. Perform the necessary activities.
3. Re-insert the C-NET device in the C-NET in the same, previous position.
4. Acknowledge the 'Fault'.
 - ⇒ If this 'Fault' is no longer displayed, the control panel updates the settings of the re-inserted C-NET device.
 - ⇒ If this 'Fault' is still displayed, and/or the detector line is not in normal operation, the 'detector line' has to be restarted.



The work described in this chapter may be performed when the C-NET detector line is switched on.

See also

Restarting the detector line [→ 30]

18.1.2 Replacing non-stationary devices of the same type



You will find additional information about the individual steps on the specified pages.

1. Switch the test mode on. Link [→ 32]
2. Replace the C-NET device. Link [→ 61]
3. Switch normal operation on. Link [→ 32]
4. Connect the PC to the 'Station'. Link [→ 20]
5. Load the configuration from the 'Station' to the PC. Link [→ 24]
6. Disconnect the PC from the 'Station'. Link [→ 20]



The work described in this chapter may be performed when the C-NET detector line is switched on.

18.1.2.1 Replacing a device

1. Remove the C-NET device you want to replace from the base.
2. Wait approx. 20 seconds.
3. Insert the new C-NET device of the same type.
 - ⇒ The internal alarm indicator flashes for 10 seconds following successful replacement.

Proceed as follows if the alarm indicator does not flash:

1. Ensure that you wait long enough before inserting.
2. Check whether other C-NET devices are missing on the detector line.
3. Check whether a device that is not of the same type has been inserted. If this is the case, insert a device of the same type.
4. Restart the C-NET line.

18.1.3 Replacing non-stationary devices of different types



You will find additional information about the individual steps on the specified pages.

1. Remove the C-NET device from its base.
 - ⇒ The 'Station' detects that the device is missing and reports a 'Fault'.
2. Delete the C-NET device individually on the Person Machine Interface on the control panel. Link [→ 31]
3. Insert the new C-NET device in the base.
4. Read-in the C-NET devices. Link [→ 31]
5. Connect the PC to the 'Station'. Link [→ 20]
6. Load the configuration from the 'Station' to the PC. Link [→ 24]
7. Replace the C-NET device in the 'Zone'. Link [→ 61]
8. Load the configuration from the PC to the 'Station'. Link [→ 23]
9. Disconnect the PC from the 'Station'. Link [→ 20]



The work described in this chapter may be performed when the C-NET detector line is switched on.

18.1.3.1 Replacing a device in the 'Zone'

1. Select the 'Zone' in which you have replaced a device in Cerberus-Engineering-Tool. The 'Find' or 'Find and replace' functions can be used to do this.
2. Replace the C-NET device.

You will find more information in document A6V10210424. See chapter 'Applicable documents'.

18.2 Base without loop contact

If a C-NET device is removed, the detector line is interrupted from this point. If the device is on a stub or sub-stub, communication between the control panel and downstream devices is interrupted. These devices are shown as missing on the control panel.

The work described in this chapter may only be performed when the C-NET detector line is switched off.

18.2.1 Temporarily removing an individual non-stationary device

Instances may arise when a C-NET device has to be temporarily removed from the base. Afterwards the same device must be re-inserted at exactly the same place in the C-NET.



Mark the allocation of the devices to the respective base to avoid additional work steps.



You will find additional information about the individual steps on the specified pages.

1. Switch the C-NET detector line off. Link [→ 30]
2. Remove the C-NET device from its base.
3. Perform the tasks.
4. Re-insert the C-NET device in the corresponding position.
5. Switch the C-NET detector line on. Link [→ 30]

If detectors have been swapped over or are missing, the following messages are shown on the display of the Person Machine Interface:

'Zone', 'Serial no. ("ID-Nr.")', 'Dev.location fault'

See also

- Non-stationary devices of the same type have been swapped over [→ 110]

18.2.2 Replacing non-stationary devices of the same type



You will find additional information about the individual steps on the specified pages.

1. Switch the C-NET detector line off. Link [→ 30]
2. Replace the C-NET device with a device of the same type. Several devices can be replaced.
3. Rectify localization errors. Link [→ 33]
4. Connect the PC to the 'Station'. Link [→ 20]
5. Load the configuration from the 'Station' to the PC. Link [→ 24]
6. Disconnect the PC from the 'Station'. Link [→ 20]

18.2.3 Replacing a non-stationary device of a different type



You will find additional information about the individual steps on the specified pages.


1. Switch the C-NET detector line off. Link [→ 30]
2. Remove the C-NET device from its base.
 - ⇒ The 'Station' detects that the device is missing and reports a 'Fault'.
3. Delete the C-NET device individually on the Person Machine Interface on the control panel. Link [→ 31]
4. Insert the new C-NET device in the base.
5. Read-in the C-NET devices. Link [→ 31]
6. Connect the PC to the 'Station'. Link [→ 20]
7. Load the configuration from the 'Station' to the PC. Link [→ 24]
8. Replace the C-NET device in the 'Zone'. Link [→ 63]
9. Load the configuration from the PC to the 'Station'. Link [→ 23]
10. Disconnect the PC from the 'Station'. Link [→ 20]

18.2.3.1 Replacing a device in the 'Zone'

1. Select the 'Zone' in which you have replaced a device in Cerberus-Engineering-Tool. The 'Find' or 'Find and replace' functions can be used to do this.
2. Replace the C-NET device.

You will find more information in document A6V10210424. See chapter 'Applicable documents'.

See also

 Applicable documents [→ 8]

18.3 Temporarily removing multiple non-stationary devices

The procedure in this chapter applies both for the base with loop contact and the base without loop contact.

For the purpose of painting work, it may be necessary to temporarily remove the C-NET devices in a room. Each C-NET device must then be re-inserted in its original base. The C-NET devices may not be exchanged.



Mark the allocation of the devices to the respective base to avoid additional work steps.



You will find additional information about the individual steps on the specified pages.

1. Switch the 'Zone' off. Link [→ 30]
2. Remove the C-NET devices from their bases.
3. Perform the tasks.
4. Re-insert the C-NET devices to the respective position.
5. Switch the 'Zone' on. Link [→ 30]
 - ⇒ For all the re-inserted C-NET devices, a localization fault is displayed.
6. Restart the C-NET detector line. Link [→ 30]

If detectors have been swapped over or are missing, the following messages are shown on the display of the Person Machine Interface:

'Zone', 'Serial no. ("ID-Nr.")', 'Dev.location fault'



The work described in this chapter may be performed when the C-NET detector line is switched on.

18.4 Permanently removing non-stationary devices

The procedure in this chapter applies both for the base with loop contact and the base without loop contact.




You will find additional information about the individual steps on the specified pages.

1. Switch the C-NET detector line off. Link [→ 30]
2. Remove the C-NET devices and their bases. Link [→ 31]
3. Switch the C-NET detector line on. Link [→ 30]
4. Delete the C-NET devices individually via the Person Machine Interface on the control panel. Link [→ 31]
5. Connect the PC to the 'Station'. Link [→ 20]
6. Load the configuration from the 'Station' to the PC. Link [→ 24]
7. Remove the logical elements in Cerberus-Engineering-Tool. Link [→ 32]
8. Load the configuration from the PC to the 'Station'. Link [→ 23]
9. Disconnect the PC from the 'Station'. Link [→ 20]

19 Change and extend the detector line

19.1 Extending the detector line to include additional devices

	<p>NOTICE</p> <p>Incorrect assignment between detector/detector group and customer text Inaccurate messages in the event of an alarm</p> <ul style="list-style-type: none"> • You must not change the C-NET topology at the same time as adding extra devices. • After extending or changing a Site always run a test to check the assignment between detector/detector group and customer text.
---	--



You will find additional information about the individual steps on the specified pages.

1. Switch the C-NET detector line off. Link [→ 30]
2. Fit and wire the new devices. Link [→ 66]
3. Read-in the C-NET devices. Link [→ 31]
4. Connect the PC to the 'Station'. Link [→ 20]
5. Load the configuration from the 'Station' to the PC. Link [→ 24]
6. Configure the new devices. Link [→ 66]
7. Load the configuration from the PC to the 'Station'. Link [→ 23]
8. Test the function of the 'Site'. Link [→ 33]
9. Remedy any errors you notice and load the corrected configuration from the PC to the 'Station'. Link [→ 23]
10. Disconnect the PC from the 'Station'. Link [→ 20]

19.1.1 Mount and wire new devices

During an extension of the line, all possible wiring work on the bases must be carried out from devices that have already been localized. When replacing these devices, these must be re-inserted in exactly the same place (observe the serial number).

1. Remove these devices from their bases.
2. Fit and wire the new devices, like bases.
3. Insert the new devices into the new bases and write down the serial numbers on the layout plan.

19.1.2 Configure a new device

1. Extend the configuration in Cerberus-Engineering-Tool, e.g. in the 'Detection tree'.
2. Allocate the read-in devices to the elements of the detection tree or the control tree in Cerberus-Engineering-Tool.
3. If required, configure additional 'Controls' (also for several 'Stations') using the layout plan or finalize available 'Controls'.

19.2 Permanently removing stationary devices



You will find additional information about the individual steps on the specified pages.

1. Switch the C-NET detector line off. Link [→ 30]
2. Remove the C-NET devices. Link [→ 31]
3. Switch the C-NET detector line on. Link [→ 30]
⇒ The control panel reports a 'Fault' per missing device.
4. Delete the C-NET devices on the Person Machine Interface. Link [→ 31]
5. Connect the PC to the 'Station'. Link [→ 20]
6. Load the configuration from the 'Station' to the PC. Link [→ 24]
7. Remove the logical elements in Cerberus-Engineering-Tool. Link [→ 32]
8. Load the configuration from the PC to the 'Station'. Link [→ 23]
9. Disconnect the PC from the 'Station'. Link [→ 20]

19.3 Convert two stubs into a loop



You will find additional information about the individual steps on the specified pages.

- ▷ The two stubs are assigned to the same line pair, e.g. 'Line' 11 and 'Line' 12.
1. Switch both the C-NET detector lines off. Link [→ 30]
 2. Wire both stubs to a loop. You will find more information about this in document A6V10210390. See chapter 'Applicable documents'.
 3. Read-in the C-NET devices. Link [→ 31] Start with the first 'Line' (in the example 'Line' 11).
⇒ The second 'Line' is adopted and the loop is formed (in this example, 'Line' 1).
 4. Connect the PC to the 'Station'. Link [→ 20]
 5. Load the configuration from the 'Station' to the PC. Link [→ 24]
 6. Test the function of the 'Site'. Link [→ 33]
 7. Remedy any errors you notice and load the corrected configuration from the PC to the 'Station'. Link [→ 23]
 8. Disconnect the PC from the 'Station'. Link [→ 20]

See also

- 📖 Applicable documents [→ 8]

19.4 Connecting a sub-stub to a loop



You will find additional information about the individual steps on the specified pages.

1. Switch the C-NET detector line off. Link [→ 30]
2. Physically connect the sub-stub to the loop. You will find more information about this in document A6V10210390. See chapter 'Applicable documents'.
3. Read-in the C-NET devices. Link [→ 31]
4. Connect the PC to the 'Station'. Link [→ 20]
5. Load the configuration from the 'Station' to the PC. Link [→ 24]
6. Test the function of the 'Site'. Link [→ 33]
7. Remedy any errors you notice and load the corrected configuration from the PC to the 'Station'. Link [→ 23]
8. Disconnect the PC from the 'Station'. Link [→ 20]

See also

Applicable documents [→ 8]

19.5 Replacing stationary devices of the same type



NOTICE

Incorrect assignment between detector/detector group and customer text

Inaccurate messages in the event of an alarm

- You must not change the C-NET topology at the same time as adding extra devices.
- After extending or changing a Site always run a test to check the assignment between detector/detector group and customer text.



You will find additional information about the individual steps on the specified pages.

1. Switch the C-NET detector line off. Link [→ 30]
2. Replace the C-NET device with a device of the same type. Several devices can be replaced.
3. Rectify localization errors. Link [→ 33]
4. Connect the PC to the 'Station'. Link [→ 20]
5. Load the configuration from the 'Station' to the PC. Link [→ 24]
6. Test the function of the 'Site'. Link [→ 33]
7. Remedy any errors you notice and load the corrected configuration from the PC to the 'Station'. Link [→ 23]
8. Disconnect the PC from the 'Station'. Link [→ 20]

You will find information about installing and uninstalling in the documentation for the corresponding 'C-NET' device.

Refer to document A6V10227639 for information on how to replace radio detectors. See chapter 'Applicable documents'.

See also

Applicable documents [→ 8]

19.6 Replacing 'Manual call point' of the same type

!	<p>NOTICE</p> <p>Incorrect assignment between detector/detector group and customer text</p> <p>Inaccurate messages in the event of an alarm</p> <ul style="list-style-type: none"> • You must not change the C-NET topology at the same time as adding extra devices. • After extending or changing a Site always run a test to check the assignment between detector/detector group and customer text.
----------	---



You will find additional information about the individual steps on the specified pages.

1. Switch on the replace mode. Link [→ 69]
2. Replace the 'Manual call point' with a 'Manual call point' of the same type.
3. Switch off the replace mode. Link [→ 70]
4. Test the 'Manual call point'. Link [→ 70]
5. Switch normal operation on. Link [→ 32]
6. Connect the PC to the 'Station'. Link [→ 20]
7. Load the configuration from the 'Station' to the PC. Link [→ 24]
8. Test the function of the 'Site'. Link [→ 33]
9. Remedy any errors you notice and load the corrected configuration from the PC to the 'Station'. Link [→ 23]
10. Disconnect the PC from the 'Station'. Link [→ 20]

You will find more information about installing and uninstalling in the documentation for the corresponding 'Manual call point'.

19.6.1 Switching on the replace mode

1. Select 'Functions' > 'All functions' > 'Detector' in the main menu.
 2. In the 'Zone', enter the 'Zone' address and press <ok>.
 3. Enter the detector address in 'Detect.' and press <ok>.
 4. Select the 'Device replace mode ON' menu item.
- ⇒ The following message is shown following successful switching on: 'Command executed'.
- ⇒ The yellow 'MENSAJES DE DESCONEXIONES' LED lights up.
- ⇒ The C-NET detector line is de-energized.

19.6.2 Switching off replace mode

1. Select 'Functions' > 'All functions' > 'Detector' in the main menu.
 2. Enter the zone address in 'Zone' and press <ok>.
 3. Enter the detector address in 'Detect.' and press <ok>.
 4. Select the 'Device replace mode OFF' menu item.
- ⇒ The following message is shown following successful switching off: 'Command executed'.
 - ⇒ The yellow 'MENSAJES DE DESCONEXIONES' LED goes out.
 - ⇒ The yellow 'DETECTORES EN PRUEBAS' LED lights up.
 - ⇒ The 'Manual call point' is in test mode.

19.6.3 Testing 'Manual call point'

1. Check whether the 'Manual call point' is in test mode using the LED.
 2. Activate the 'Manual call point' using the corresponding tools.
- You will find information about this in the 'Manual call point' documentation.

20 Updating the firmware of the 'Station'

20.1 Preparation and security

The following points must be observed before updating the firmware.

- The firmware must be updated individually for each 'Station'. Exception: 'Stations' networked via C-WEB/LAN. See the chapter 'Updating several 'Stations' simultaneously'.
- Data backup
 - When the firmware of the main CPU is updated, the configuration data, event memories and the alarm counter value are deleted. Load the configuration data and event memories before updating in Cerberus-Engineering-Tool. You will find more information about the event memory and the alarm counter in document A6V10210424. See chapter 'Applicable documents'.
- Converting the configuration data
 - Updating the firmware requires the configuration data to be converted if the new firmware and existing configuration are not compatible with one another.
- BDV compatibility
 - The BDVs are compatible when the major version and the minor version are identical. The Bug fix version is not relevant for the compatibility. You will find Information about BDV names and versions in document A6V10210424. See chapter 'Applicable documents'.
- The procedure for updating the firmware depends on the 'Station' configuration. A 'Station' can be configured as follows:
 - Standalone Station
 - SAFEDLINK Station
 - Router Station, Ethernet Station
 - Modular 'Station' with CPU card
- Windows firewall setting
 - To connect the PC to the 'Station', the Windows firewall settings must be changed if possible. You will find more information on this in chapter 'Setting Windows firewall [→ 77]'.
- Communication with GAP via C-WEB/LAN
 - A GAP with DHCP must be configured for a connection with the PC via C-WEB/LAN. You will find more information in document A6V10210424. See chapter 'Applicable documents'.
- Once the firmware has been updated, the 'Station' configuration must be loaded to 'Cerberus-Engineering-Tool' in order to update the LRC data to the current firmware status.





⚠ WARNING

Fire detection installation is deactivated during the firmware update

Fire may spread unhindered.

- Supervision by people is required.
- Re-activate the fire detection installation as soon as possible.

	NOTICE
	<p>Data loss during the firmware update</p> <p>Configuration data and event memory are deleted in the 'Station'.</p> <ul style="list-style-type: none"> • Load the configuration data and event memory to Cerberus-Engineering-Tool before updating the firmware.
	NOTICE
	<p>Power failure during the firmware update</p> <p>Firmware is not updated and 'Station' is not working. The firmware update cannot be repeated and must be performed by the manufacturer.</p> <ul style="list-style-type: none"> • Do not disconnect the Station from the power supply during the firmware update.

See also

 Updating several 'Stations' simultaneously [→ 73]

20.2 Updating the firmware of the main CPU and the additional CPUs – Overview

The procedure for updating the firmware depends on the nature and function of the 'Station'. The procedures are described in the following chapters.

20.2.1 Standalone station and SAFEDLINK station



You will find additional information about the individual steps on the specified pages.

- ▷ Familiarize yourself with the information in 'Preparation and security [→ 71]'.
- 1. Import the new firmware into Cerberus-Engineering-Tool.
 - Select the 'File' > 'Import new FW package' menu item and open the file you want.
- 2. Load the configuration from the 'Station' or your archive to the PC. Link [→ 24]
- 3. Convert the configuration if necessary and rectify conversion faults. Link [→ 77]
- 4. Connect the PC to the 'Station'. Link [→ 20]
- 5. Update the firmware on the main CPU and the additional CPUs. Link [→ 79]
- 6. Initialize the 'Station'. Link [→ 21]
- 7. Test the firmware version on the additional CPUs. Link [→ 86]
 - Update the firmware, if required, of the additional CPUs again, if there is a higher firmware version available. Link [→ 84]
- 8. Load the configuration from the 'Station' to the PC. Link [→ 24]
- 9. Disconnect the PC from the 'Station'. Link [→ 20]

20.2.2 Router station and Ethernet station



You will find additional information about the individual steps on the specified pages.

- ▷ Familiarize yourself with the information in 'Preparation and security [→ 71]'.
- ▷ A GAP with DHCP must be configured for the connection with the PC via C-WEB/LAN.
- 1. Import the new firmware into Cerberus-Engineering-Tool.
 - Select the 'File' > 'Import new FW package' menu item and open the file you want.
- 2. Load the configuration from the 'Station' or your archive to the PC. Link [→ 24]
- 3. Convert the configuration if necessary and rectify conversion faults. Link [→ 77]
- 4. Connect the PC to the C-WEB/LAN via the Ethernet switch (MM) FN2008-A1.
- 5. Update the firmware on the main CPU and the additional CPUs. Link [→ 79]
- 6. Initialize the 'Station'. Link [→ 21]
 - Remove the network connection to the 'Station' and connect the PC locally to the 'Station'. Link [→ 20]
- 7. Test the firmware version on the additional CPUs. Link [→ 86]
 - Update the firmware, if required, of the additional CPUs again, if there is a higher firmware version available. Link [→ 84]
- 8. Load the configuration from the 'Station' to the PC. Link [→ 24]
- 9. Disconnect the PC from the 'Station'. Link [→ 20]
- 10. Restore the network connection.

20.2.3 Updating several 'Stations' simultaneously

You can update the firmware of max. eight networked 'Stations' simultaneously. The 'Stations' and the CPU cards must be connected to one another via C-WEB/LAN.

Example: Several 'Stations' are connected to each other via one or several 'Ethernet switch (MM) FN2008-A1.'



You will find additional information about the individual steps on the specified pages.

- ▷ Familiarize yourself with the information in 'Preparation and security [→ 71]'.
- ▷ A GAP with DHCP must be configured for the connection with the PC via C-WEB/LAN.
- ▷ The 'Stations' are displayed together.
- ▷ You can update not more than eight 'Stations' simultaneously.
- 1. Import the new firmware into Cerberus-Engineering-Tool.
 - Select the 'File' > 'Import new FW package' menu item and open the file you want.

2. Load the configuration from the 'Station' or your archive to the PC. Link [→ 24]
3. Convert the configuration if necessary and rectify conversion faults. Link [→ 77]
4. Connect the PC to the 'Ethernet switch (MM) FN2008-A1.'
5. Update the firmware on the main CPU and the additional CPUs. Link [→ 79]
 - Set each 'Station' individually in update mode. You can set the 'Stations' in update mode without any waiting time one directly after the other.
 - Wait until the update of each 'Station' is completed.
6. Initialize each 'Station' individually. Link [→ 21] To do so, you must connect the PC to each 'Station' locally. Link [→ 20]
7. Test the firmware version on the additional CPUs on each 'Station'. Link [→ 86]
 - Update the firmware, if required, of the additional CPUs again, if there is a higher firmware version available. Link [→ 84]
8. Load the configuration from the 'Station' to the PC. Link [→ 24]
9. Disconnect the PC from the 'Station'. Link [→ 20]
10. Restore the network connection, if required.

20.3 Updating the firmware of the additional CPUs only – Overview

If the Station firmware is up-to-date and components have been changed then it is only necessary to update the additional CPUs. The procedure for updating the firmware depends on the 'Station' function. The procedures are described in the following chapters.

20.3.1 Standalone station and SAFEDLINK station



You will find additional information about the individual steps on the specified pages.

- ▷ Familiarize yourself with the information in 'Preparation and security [→ 71]'.
1. Connect the PC to the 'Station'. Link [→ 20]
 2. Enable the 'Station'.
 - Press <MENU> and enter a valid PIN.
 3. Update the firmware of the additional CPUs if there is a higher firmware version status. Select the local connection as the connection type. Link [→ 84]
 4. Load the configuration from the 'Station' to the PC. Link [→ 24]
 5. Disconnect the PC from the 'Station'. Link [→ 20]

20.3.2 Router station and Ethernet station

You can update the additional CPUs in a networked 'Station' via C-WEB/LAN. In this way, you can update networked 'Stations' without disconnecting the network connection and restoring the factory setting.



You will find additional information about the individual steps on the specified pages.


- ▷ Familiarize yourself with the information in 'Preparation and security [→ 71]'.
 - ▷ A GAP with DHCP must be configured for the connection with the PC via C-WEB/LAN.
- 1. Load the configuration from the 'Station' or your archive to the PC. Link [→ 24]
- 2. Connect the PC to the C-WEB/LAN via the Ethernet switch (MM) FN2008-A1.
- 3. Enable the 'Station'.
 - Press <MENU> and enter a valid PIN.
- 4. Update the firmware of the additional CPUs if there is a higher firmware version status. Select the connection via GAP and enter the address of the 'Station' you want to update. Link [→ 84]
- 5. Load the configuration from the PC to the 'Station'. Link [→ 23]
- 6. Load the configuration from the 'Station' to the PC. Link [→ 24]
- 7. Disconnect the PC from C-WEB/LAN.

20.4 Update only the BDV

If the old and new BDVs are compatible (identical major and minor versions) and there is no new firmware version available for the main CPU, it is also only possible to update the BDV. You will find Information about BDV names and versions in document A6V10210424. See chapter 'Applicable documents'.

The procedure for updating the BDV depends on the 'Station' function. The procedures are described in the following chapters.

See also

 Applicable documents [→ 8]

20.4.1 Standalone station and SAFEDLINK station



You will find additional information about the individual steps on the specified pages.

- ▷ Familiarize yourself with the information in 'Preparation and security [→ 71]'.
- 1. Import the new BDV into Cerberus-Engineering-Tool.
 - Select the 'File' > 'Import new BDV' menu item and open the file you want.
- 2. Load the configuration from the 'Station' or your archive to the PC. Link [→ 24]
- 3. Convert the configuration and rectify conversion faults. Link [→ 77]
- 4. Connect the PC to the 'Station'. Link [→ 20]
- 5. Enable the 'Station'.
 - Press <MENU> and enter a valid PIN.
- 6. Load the converted configuration from the PC to the 'Station'. Link [→ 23]
- 7. Disconnect the PC from the 'Station'. Link [→ 20]

20.4.2 Router station and Ethernet station



You will find additional information about the individual steps on the specified pages.

- ▷ Familiarize yourself with the information in 'Preparation and security [→ 71]'.
- 1. Import the new BDV into Cerberus-Engineering-Tool.
 - Select the 'File' > 'Import new BDV' menu item and open the file you want.
- 2. Load the configuration from the 'Station' or your archive to the PC. Link [→ 24]
- 3. Convert the configuration and rectify conversion faults. Link [→ 77]
- 4. Remove the network connection to the 'Station' and connect the PC. Link [→ 20]
- 5. Enable the 'Station'.
 - Press <MENU> and enter a valid PIN.
- 6. Load the converted configuration from the PC to the 'Station'. Link [→ 23]
- 7. Disconnect the PC from the 'Station'. Link [→ 20]
- 8. Restore the network connection.

20.5 Converting the configuration

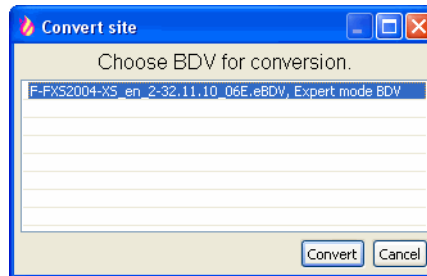
In document A6V10260976, you will find detailed information about converting 'Sites'. See chapter 'Applicable documents'.

Converting the configuration

▷ The 'Site' you want to convert is saved and loaded in Cerberus-Engineering-Tool.

1. Select the 'Edit' > 'Convert site' menu item.

⇒ The following window is opened:



2. Select the BDV you want and click on 'Convert'.

⇒ The 'Action confirmation' window opens.

3. Click on 'Yes'.

⇒ The 'Site' is converted.

20.6 Setting Windows firewall

The Windows firewall may prevent the PC connecting to the 'Station'. In this case, the firewall must be switched off in Windows XP or firewall rules set in Windows 7 when working with the fire detection installation.

To do this, proceed as follows:



You must have administrator rights to make the following settings.

Windows XP

▷ You have administrator rights on your PC

1. Open the Windows start menu.

2. Select 'Settings' > 'Control panel' > 'Administrative Tools' > 'Services'.

3. Right-click on 'Windows Firewall/Internet Connection Sharing (ICS)' in the new window.

4. Select 'All Tasks' > 'Exit' in the context menu.

5. Once the work is complete, reactivate the firewall. To do this, proceed as described above but select 'All Tasks' > 'Start' in the context menu.



NOTICE

Security vulnerability in operating system due to deactivated firewall

Unauthorized access to your PC

- Activate the firewall after the firmware update.

Windows 7



There are different ways of adjusting the firewall rules in Windows 7. The method described below has been tested successfully.

Make the following settings for the Windows 7 firewall:

▷ You have administrator rights on your PC

1. Open the Windows start menu.
2. Select 'Control Panel' > 'All Control Panel Items' > 'Administrative Tools' > 'Local Security Policy' > 'Windows Firewall with Advanced Security'.
3. Select 'Advanced settings' > 'Inbound Rules' > 'New Rule...'.
⇒ This opens the 'New Inbound Rule Wizard'.
4. Select 'Rule Type' and activate 'Program'.
5. Click 'Next >' to confirm and enter the program path to 'F-FXS2002.exe'.
- Example: C:\Program Files (x86)\Siemens\F-FX2030\XL_en_1-V4.0
6. Click 'Next >' to confirm and then confirm the default setting 'Allow the connection' in the next step ('Action').
7. In the next step ('Profile'), remove the check mark from the 'Domain' box.
⇒ The 'Private' and 'Public' boxes are checked.
8. Click 'Next >' to confirm and enter an appropriate name in the next step ('Name'), such as 'FS20 application'.
9. Click 'Finish' to complete the process.
⇒ A 'New Rule' has now been set and appears in the 'Inbound Rules' list.

It is necessary to make additional settings for the new rule:

1. Right-click the new rule and select 'Properties'.
2. In the '<rule name> Properties' window, select the 'Protocol and Ports' tab.
3. Set the following values:
 - 'Protocol type': 'UDP'
 - 'Local port': 'Specific Ports', and enter the value range '50067-50070' in the box.
 - 'Remote port': 'All Ports'
4. Confirm with 'OK'.
⇒ The new firewall rule is now configured.



NOTICE

Security vulnerability in operating system due to open ports

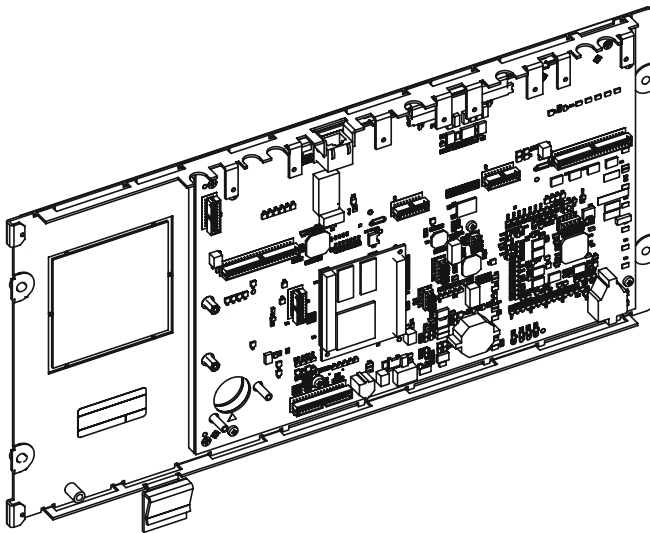
Unauthorized access to your PC

- Deactivate the firewall rule configured above after the firmware update.

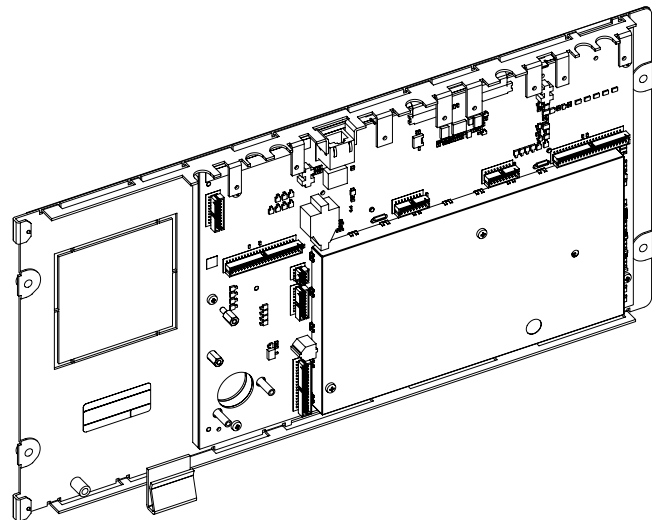
20.7 Updating the firmware of the main CPU and the additional CPUs

The procedure for updating the main CPU and additional CPUs depends on whether the PMI & mainboard FCM2004 or FCM2027 is used in the 'Station.' The procedures are described in the following chapters:

- 'PMI & mainboard FCM2004 [→ 79]'
- 'PMI & mainboard FCM2027 [→ 81]'



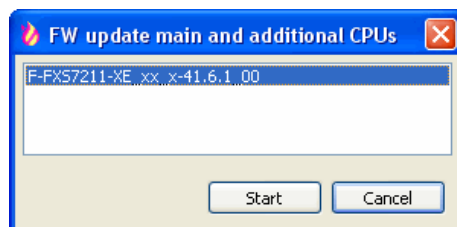
PMI & mainboard FCM2004



PMI & mainboard FCM2027

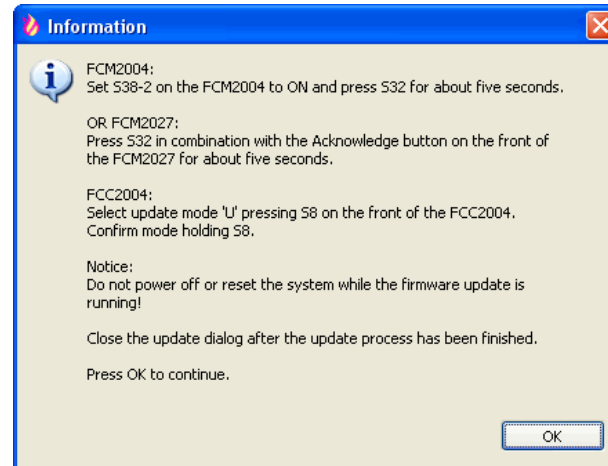
20.7.1 PMI & mainboard FCM2004

- ▷ Familiarize yourself with the information in 'Preparation and security [→ 71]'.
- 1. Select 'Update' > 'FW update main and additional CPUs' from the menu bar.
- 2. If the 'Password check' window is open, enter the password '1234' and click on 'OK'.
 - ⇒ The 'Confirmation' window opens.
- 3. **NOTICE! Data loss. Save the configuration data before updating the firmware.**
- 4. Click on 'Yes'.
 - ⇒ The 'FW update main and additional CPUs' window opens.

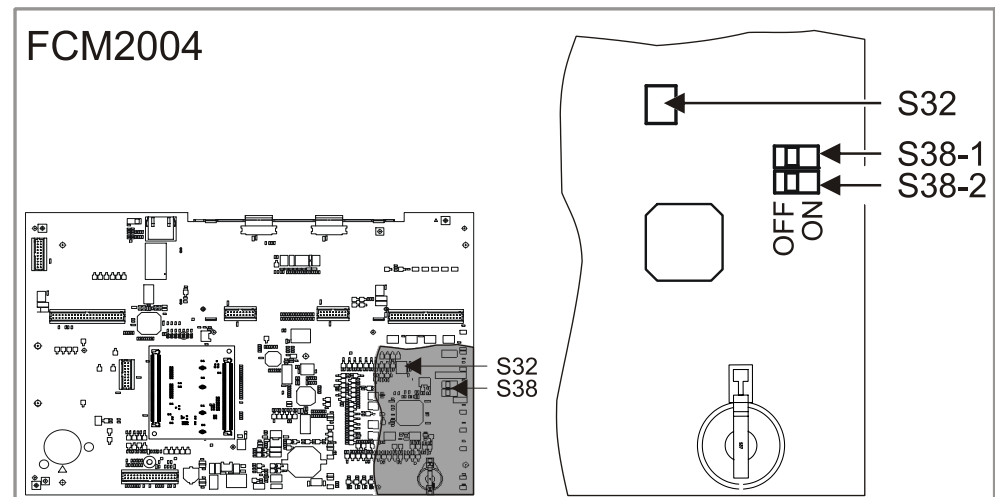


5. Select the firmware version you want and click on 'Start'.

⇒ The following window is opened:



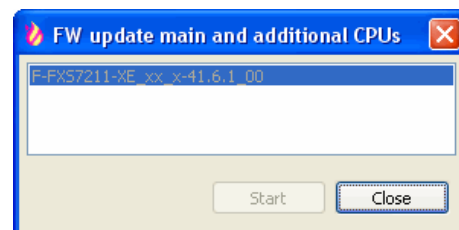
6. Set the 'S38-2' switch to 'ON' on the rear of the operating unit.
7. Press the 'S32' button for approx. 5 s until the 'Station' restarts.



⇒ The firmware update starts and takes up to ten minutes.

8. Click on 'OK' in the 'Information' window.

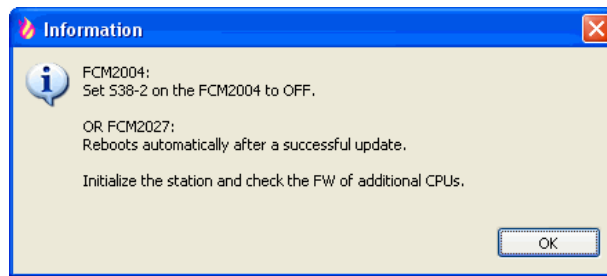
⇒ The 'FW update main and additional CPUs' window is displayed. Only close this window once the firmware update is complete.



9. Follow the procedures on the display of the 'Station' and wait until the following lines appear:
 - 'Switch-off S38-2 now'
 - 'The panel will reboot automatically'

10. Click on 'Close' in the 'FW update main and additional CPUs' window.

⇒ The following window is opened:



11. On the 'Station', set the 'S38-2' switch to 'OFF'.

⇒ The 'Station' is restarted many times. This procedure takes up to ten minutes.

12. Click on 'OK' in the 'Information' window.

⇒ After the restart, the 'Station' display shows the available BDVs. It is not necessary to install a BDV at this point.



Initializing the 'Station' instead of installing the BDV saves time. During initialization, the BDV and the configuration data are loaded to the 'Station'.

20.7.2 PMI & mainboard FCM2027

▷ Familiarize yourself with the information in the chapter 'Preparation and security'.

1. Select 'Update' > 'FW update main and additional CPUs' from the menu bar.

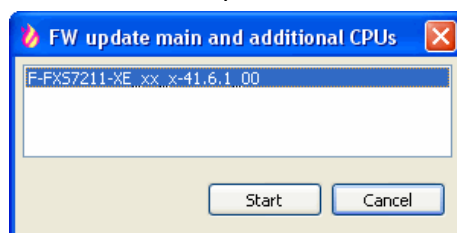
2. If the 'Password check' window is open, enter the password '1234' and click on 'OK'.

⇒ The 'Confirmation' window opens.

3. **NOTICE! Data loss. Save the configuration data before updating the firmware.**

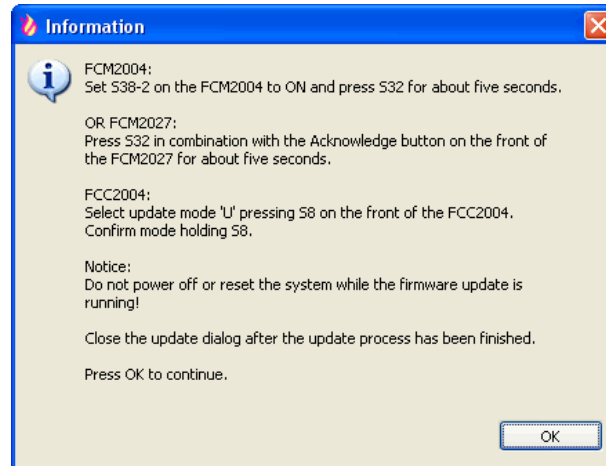
4. Click on 'Yes'.

⇒ The 'FW update main and additional CPUs' window opens.

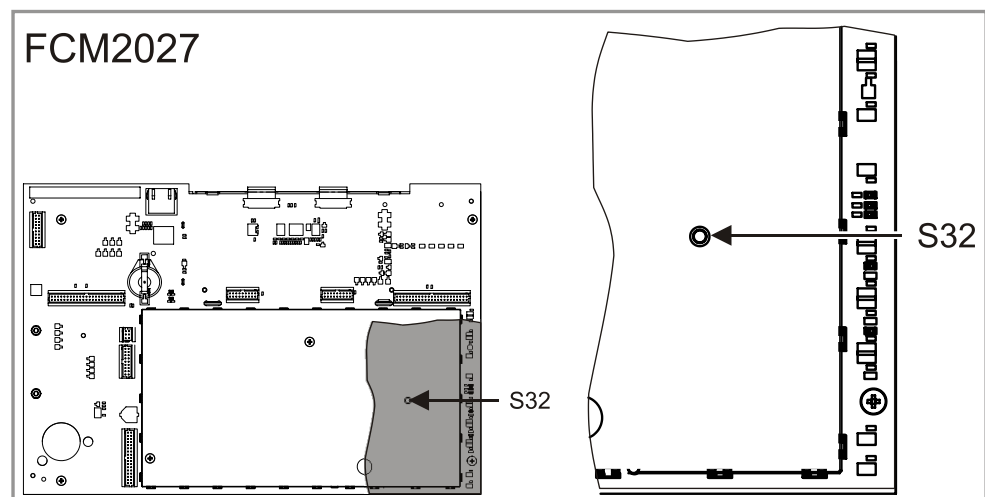


5. Select the firmware version you want and click on 'Start'.

⇒ The following window is opened:



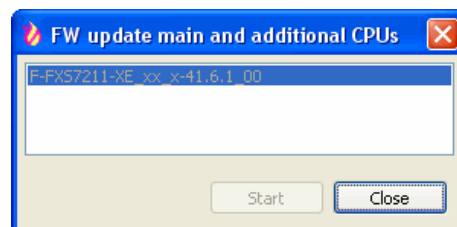
6. Keep the 'S32' button on the rear of the operating unit pressed and press <Acknowledge> on the Person Machine Interface at the same time for approx. 5 s until the 'Station' restarts.



- ⇒ A peeping sound confirms the function is being executed.
- ⇒ The firmware is updated and the 'Station' restarts several times. This procedure takes up to ten minutes.

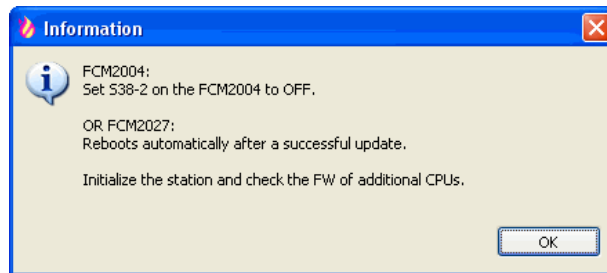
7. Click on 'OK' in the 'Information' window.

⇒ The 'FW update main and additional CPUs' window is displayed.



8. Click on 'Close' in the 'FW update main and additional CPUs' window once the 'Station' has restarted.

⇒ The following window is opened:



9. Click on 'OK'.

⇒ After the restart, the 'Station' display shows the available BDVs. It is not necessary to install a BDV at this point.



Initializing the 'Station' instead of installing the BDV saves time. During initialization, the BDV and the configuration data are loaded to the 'Station'.

Error during firmware update

If errors occur during the firmware update, the error messages are shown after the update on the 'Station' display. The line 'Press Silence buzzer button' is displayed after the error messages.

1. Press <Silence buzzer> on the Person Machine Interface.
 - ⇒ The 'Station' restarts.
 - ⇒ After a few minutes, the 'Buzzer' sounds twice.
2. Press <Acknowledge> on the Person Machine Interface to switch off the 'Buzzer'. Do not perform any more actions on the 'Station' until the 'Buzzer' has sounded for the second time.

See also

📄 Preparation and security [→ 71]

20.8 Update the firmware of the additional CPUs



NOTICE

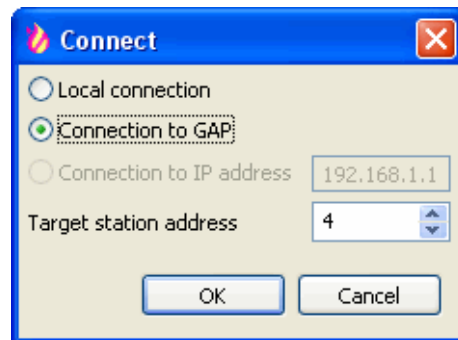
Updating the firmware of the degraded mode module FN2001

If the firmware of the degraded mode module FN2001 has to be updated, it must be temporarily connected to the slot for the main module FN2001 (from slot X12 to X13).

▷ Familiarize yourself with the information in the chapter 'Preparation and security'.

1. Select 'Update' > 'FW update additional CPUs' from the menu bar.
2. If the 'Password check' window is open, enter the password '1234' and click on 'OK'.

⇒ The following window is opened:



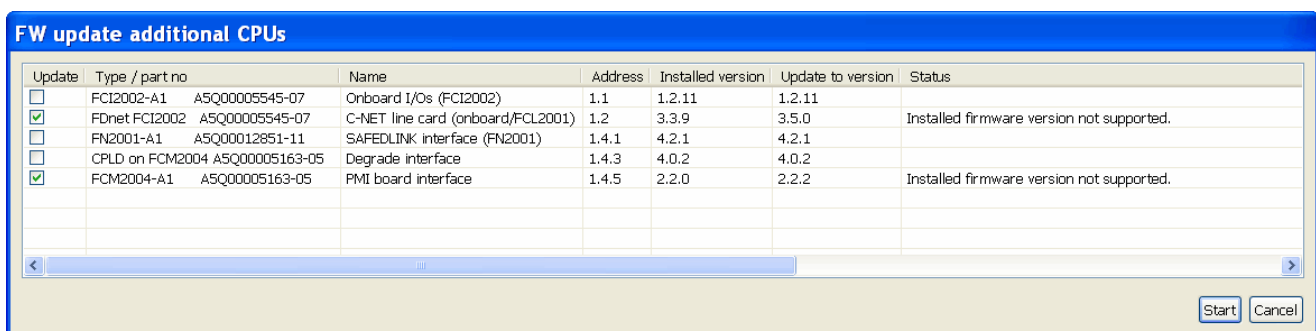
3. Select the connection type.

- Select 'Local connection' to establish a connection to the connected standalone or SAFEDLINK 'Station'.
- Select 'Connection to GAP' to establish a connection via GAP to a networked 'Station'. Enter the address of the 'Station' you want to update in the 'Target station address' field. If you want to update the GAP 'Station' itself, enter '0'.

4. Click on 'OK'.

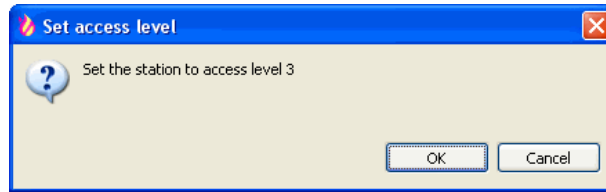
⇒ The following window is opened.

⇒ The checkboxes for the CPUs that can be updated are checked.



5. Select the CPUs you want to update and click on 'Start'.

⇒ The following window is opened:



6. Press <MENU> on the 'Station' and enter a valid PIN.
7. Click on 'OK' in the 'Set access level' window.
 - ⇒ The CPUs are updated.
 - ⇒ The 'Information' window is opened after updating.
8. Note the update information and information about other procedures in the 'Information' window.
9. Click on 'OK'.
 - ⇒ The 'Station' is restarted.
 - ⇒ After a few minutes, the 'Buzzer' sounds twice.
10. Press <Acknowledge> on the Person Machine Interface to switch off the 'Buzzer'. Do not perform any more actions on the 'Station' until the 'Buzzer' has sounded for the second time.
11. Click on 'Close' in the 'FW update additional CPUs' window.

See also

📄 Preparation and security [→ 71]

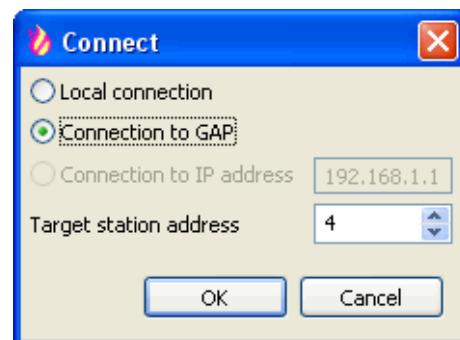
20.9 Testing the firmware version of the additional CPUs

If you have updated the firmware of the main CPU and the additional CPUs in a single step ('FW update main and additional CPUs'), you must then test the firmware version of the additional CPUs to ensure that the CPUs were updated correctly. Update the firmware, if required, of the additional CPUs again, if there is a higher firmware version available.

To test the firmware version on the additional CPUs, proceed as follows:

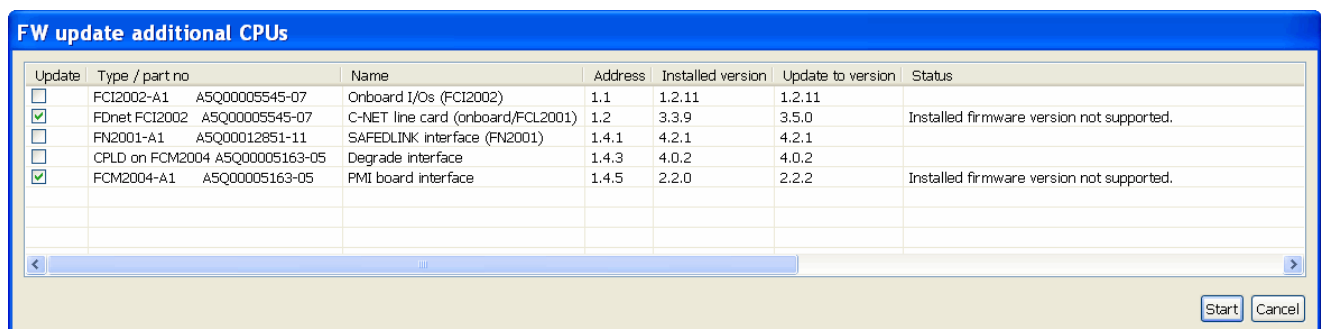
1. Select 'Update' > 'FW update additional CPUs' from the menu bar.
2. If the 'Password check' window is open, enter the password '1234' and click on 'OK'.

⇒ The following window is opened:



3. Select the connection type.
 - Select 'Local connection' to establish a connection to the connected standalone or SAFEDLINK 'Station'.
 - Select 'Connection to GAP' to establish a connection via GAP to a networked 'Station'. In the field 'Target station address' enter the address of 'Station'. If you want to create a connection to GAP 'Station' itself, enter '0'.
4. Click on 'OK'.

⇒ The following window is opened.



5. Test the firmware version on the additional CPUs.
6. Click on 'Cancel' in the 'FW update additional CPUs' window.

20.10 Creating diagnosis report

To update the firmware versions for the creation of the diagnosis report, the configuration data must be loaded in Cerberus-Engineering-Tool.

▷ The configuration data for the 'Station' is loaded to Cerberus-Engineering-Tool.

1. Select 'Commissioning' > 'Diagnostics report' from the menu bar.

⇒ The 'Reports' window opens.

2. Select 'Diagnostics report' in the 'Report type' field.

3. Select the page format, page orientation, file name and memory location of the report in the 'Output settings' section.


4. Click on 'Create report'.

⇒ The report is created and displayed.



You will find more information about creating reports and the diagnosis report in document A6V10210424. See chapter 'Applicable documents'.

See also

 Applicable documents [→ 8]

21 Updating the firmware of the peripheral devices

You need the following tools to update the firmware of the peripheral devices:

- Cerberus-Engineering-Tool
- MCL-USB adapter FDUZ221



If the hardware product version is not compatible with the current firmware, a corresponding error message is displayed during the update process.

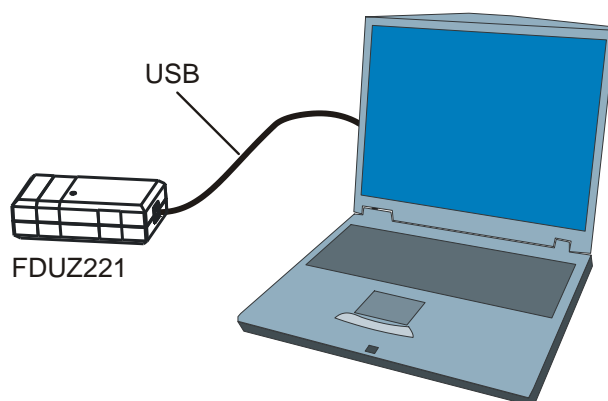
In this instance, the hardware must be replaced in accordance with the information in the 'Release Notes'.

21.1 Updating the firmware of the MCL-USB adapter FDUZ221

The firmware of the MCL-USB adapter FDUZ221 must be updated if a new firmware version is issued.

Preparation

- ▷ The driver for the MCL-USB adapter is installed on the PC. You will find instructions for installing the driver in document 009854. See chapter 'Applicable documents'.
- 1. Select 'File' > 'Import new FW package'.
- 2. In the selection window open the corresponding file F-FXS2007-XX_x_x_...zip.
- 3. Connect the MCL-USB adapter to the PC.
- ⇒ The orange LED on the MCL-USB adapter flashes for a short while. When the device is ready for operation, the green LED lights up.



Connection of the PC to the MCL-USB adapter

Updating the firmware

1. Select 'Update' > 'FW update FDUZ221 MCL USB adapter'.
 - ⇒ The connection to the device is established.
 - ⇒ The 'FW update FDUZ221 MCL USB adapter' window opens.
 - ⇒ The latest firmware package and the latest firmware version are suggested.
 - ⇒ The green LED goes out.

2. Click on 'Start'.
 - ⇒ When the hardware version is unknown, another 'FW update FDUZ221 MCL USB adapter' window is opened and you are prompted to check the hardware version.
 - ⇒ When the hardware version is known, the status bar indicates the update progress.
 - ⇒ The 'FW update FDUZ221 MCL USB adapter' window is closed after updating.
 - ⇒ The device is restarted.
 - ⇒ A success message is indicated.
 - ⇒ When the device is ready for operation, the green LED lights up.
3. Disconnect the MCL-USB adapter from the PC.
 - ⇒ The firmware is updated.

21.2 Updating the firmware of the floor repeater terminal FT2010



⚠ WARNING

Incorrect assignment between detector/detector group and customer text

Misleading messages in the event of an alarm

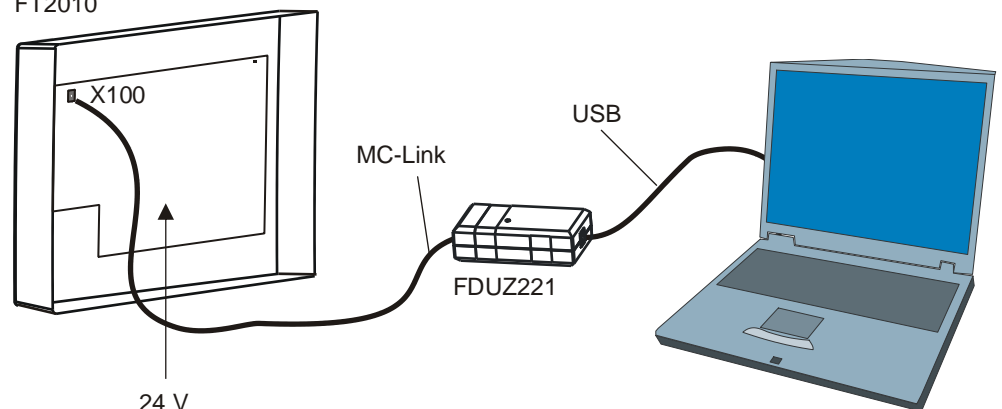
- Never change the wiring during the firmware update.

The firmware must be updated individually for each floor repeater terminal.

Preparation

- ▷ The floor repeater terminal is fed by a 24 V external power supply or by the C-NET detector line.
 - ▷ The driver for the MCL-USB adapter FDUZ221 is installed on the PC.
1. Select 'File' > 'Import new FW package'.
 2. Open an F-FXS7211-XX_x_x_...zip file that matches the 'Site' in the selection window.
 3. Open the device and connect the PC via the MCL-USB adapter to the device.

FT2010



Connect the PC to the floor repeater terminal

- FDUZ221 MCL-USB adapter (interface USB/MC-LINK)
- X100 Connection for the MCL-USB adapter
- FT2010 Floor repeater terminal

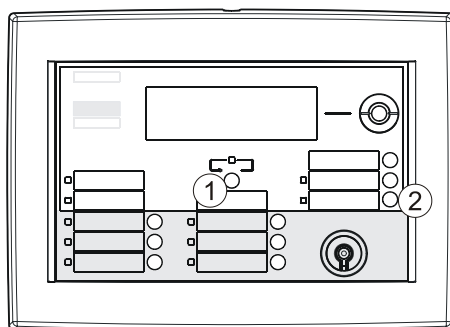
Updating the firmware

1. Select 'Update' > 'FW update standard peripheral device'.
 - ⇒ The 'FW update standard peripheral device' window opens.
 - ⇒ Cerberus-Engineering-Tool establishes the connection to the device and sets the device to update mode.
 - ⇒ The latest firmware package and the latest firmware version are suggested.
2. Select the firmware package that matches the 'Site'.
3. Click on 'Start'.
 - If the hardware version is not compatible, click on 'Cancel' and check the hardware version. Replace the hardware and start again at point 1.
 - ⇒ The status bar indicates the update progress.
 - ⇒ The 'FW update standard peripheral device' window is closed after updating.
 - ⇒ The device is restarted.
 - ⇒ A success message is indicated.
4. Remove the MCL-USB adapter and lock the device.
 - ⇒ The firmware is updated.

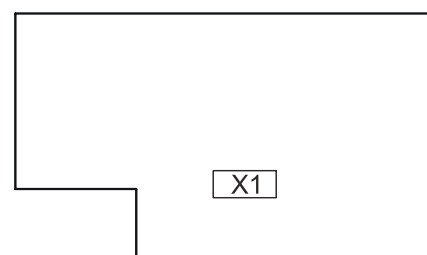
Manually setting device to update mode

Proceed as follows if you are prompted to manually set the device to update mode in step 1:

1. Keep the 'More alarms' (1) and 'Reset' (2) buttons pressed at the same time and disconnect the C-NET plug (X1) from the printed circuit board.
2. Wait at least ten seconds and re-insert the C-NET plug (X1).
 - ⇒ The device is set to update mode.
3. Click on the 'OK' button in the 'FW update standard peripheral device' window and go to 'Update firmware', step 2.



FT2010 Front view



FT2010 printed circuit board

21.3 Updating the firmware of the floor repeater display FT2011



⚠ WARNING

Incorrect assignment between detector/detector group and customer text

Misleading messages in the event of an alarm

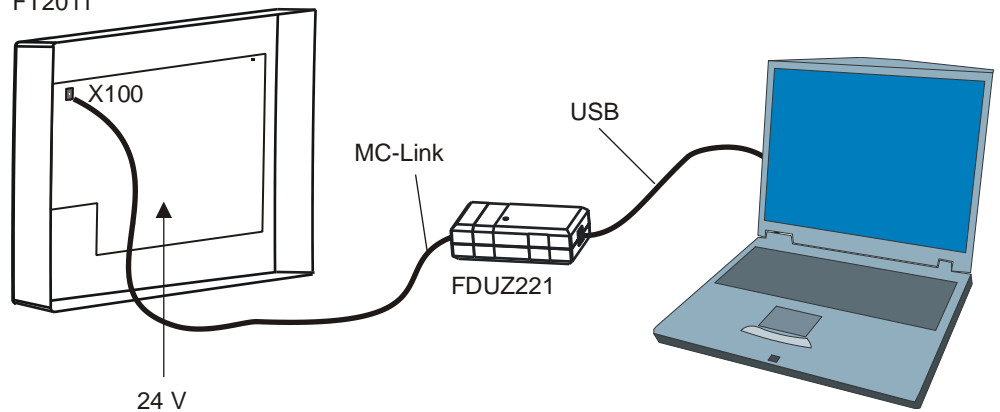
- Never change the wiring during the firmware update.

The firmware must be updated individually for each floor repeater display.

Preparation

- ▷ The floor repeater display is fed by a 24 V external power supply or by the C-NET detector line.
- ▷ The driver for the MCL-USB adapter FDUZ221 is installed on the PC.
- 1. Select 'File' > 'Import new FW package'.
- 2. Open an F-FXS7211-XX_x_x...zip file that matches the 'Site' in the selection window.
- 3. Open the device and connect the PC via the MCL-USB adapter to the device.

FT2011



Connect the PC to the floor repeater display

FDUZ221	MCL-USB adapter (interface USB/MC-LINK)
X100	Connection for the MCL-USB adapter
FT2011	Floor repeater display

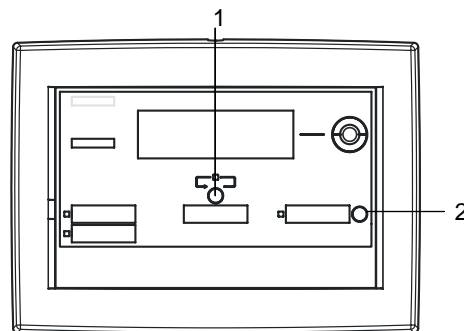
Updating the firmware

1. Select 'Update' > 'FW update standard peripheral device'.
 - ⇒ The 'FW update standard peripheral device' window opens.
 - ⇒ Cerberus-Engineering-Tool establishes the connection to the device and sets the device to update mode.
 - ⇒ The latest firmware package and the latest firmware version are suggested.
2. Select the firmware package that matches the 'Site'.
3. Click on 'Start'.
 - ⇒ If the hardware version is not compatible, click on 'Cancel' and check the hardware version. Replace the hardware and start again at point 1.
 - ⇒ The status bar indicates the update progress.
 - ⇒ The 'FW update standard peripheral device' window is closed after updating.
 - ⇒ The device is restarted.
 - ⇒ A success message is indicated.
4. Remove the MCL-USB adapter and lock the device.
 - ⇒ The firmware is updated.

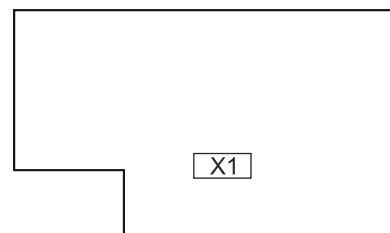
Manually setting device to update mode

Proceed as follows if you are prompted to manually set the device to update mode in step 1:

1. Keep the 'More alarms' (1) and 'Silence buzzer' (2) buttons pressed at the same time and disconnect the C-NET plug (X1) from the printed circuit board.
2. Wait at least ten seconds and re-insert the C-NET plug (X1).
 - ⇒ The device is set to update mode.
3. Click on the 'OK' button in the 'FW update standard peripheral device' window and go to 'Update firmware', step 2.



FT2011 Front view



FT2011 printed circuit board

21.4 Updating firmware of mimic display driver FT2001-A1



⚠ WARNING

Incorrect assignment between detector/detector group and customer text

Misleading messages in the event of an alarm

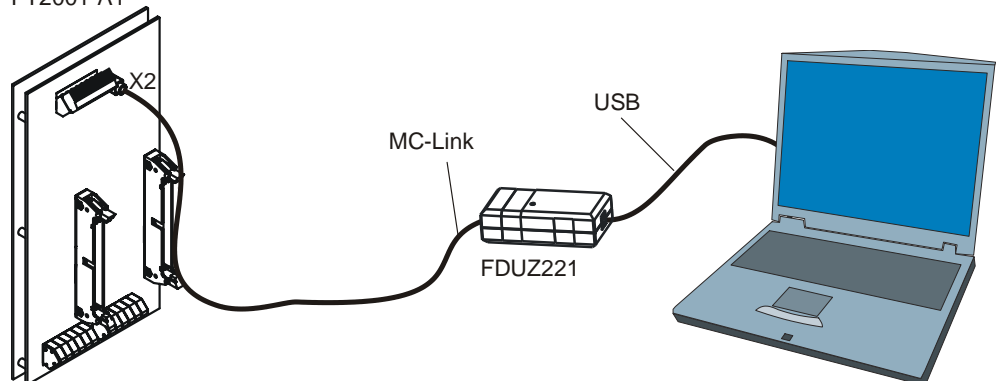
- Never change the wiring during the firmware update.

The firmware must be updated individually for each mimic display driver.

Preparation

- ▷ The mimic display driver is fed by a 24 V external power supply or by the C-NET detector line.
- ▷ The driver for the MCL-USB adapter FDUZ221 is installed on the PC.
- 1. Select 'File' > 'Import new FW package'.
- 2. Open an F-FXS7211-XX_x_x_...zip file that matches the 'Site' in the selection window.
- 3. Connect the PC to the device via the MCL-USB adapter.

FT2001-A1



Connection of the PC to the mimic display driver

FDUZ221 MCL-USB adapter (interface USB/MC-LINK)

X2 Connection for the MCL-USB adapter

FT2010 Mimic display driver

Updating the firmware

1. Select 'Update' > 'FW update standard peripheral device'.
 - ⇒ The 'FW update standard peripheral device' window opens.
 - ⇒ Cerberus-Engineering-Tool establishes the connection to the device and sets the device to update mode.
 - ⇒ The latest firmware package and the latest firmware version are suggested.
2. Select the firmware package that matches the 'Site'.
3. Click on 'Start'.
 - ⇒ The status bar indicates the update progress.

- ⇒ The 'FW update standard peripheral device' window is closed after updating.
- ⇒ The device is restarted.
- ⇒ A success message is indicated.

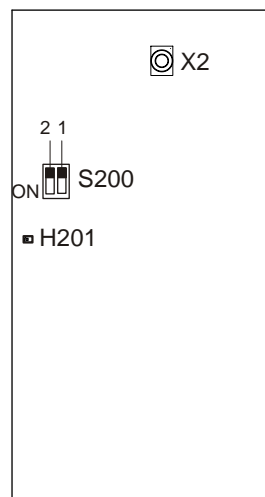
4. Remove the MCL-USB adapter.

- ⇒ The firmware is updated.

Manually setting device to update mode

Proceed as follows if you are prompted to manually set the device to update mode in step 1:

1. Set the DIP switch S200-1 to 'ON'.
 - ⇒ The device is set to update mode.
2. Click on 'OK' in the 'FW update standard peripheral device' window.
3. Set the DIP switch S200-1 to 'OFF'.
4. Go to 'Update firmware', step 2.



FT2001-A1 Printed circuit board view

21.5 Updating the firmware of the radio gateway FDCW241

You must update the firmware of the radio gateway FDCW241 with a SWING-Tool and the MCL-USB adapter FDUZ227. You will find information on this in document A6V10227639. See chapter 'Applicable documents'.

See also

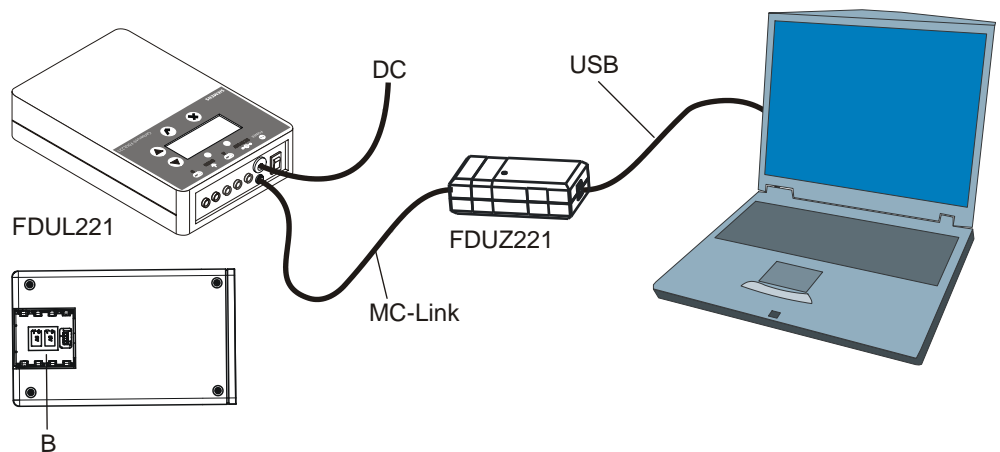
- 📄 Applicable documents [→ 8]

21.6 Updating firmware on the line tester FDUL221

This chapter relates to the line tester FDUL221, device version with MC link connection, order no. A5Q00022100

Preparation

- ▷ The driver for the MCL-USB adapter FDUZ221 is installed on the PC.
- ▷ The line tester is fed either internally with batteries or via a mains adapter.
- 1. Select 'File' > 'Import new FW package'.
- 2. In the selection window open the most recent file with the corresponding language F-FXS2007-XX_x_x_...zip.
- 3. Connect the device to the PC via the MCL-USB adapter.



Connect the PC to the line tester

FDUZ221	MCL-USB adapter (interface USB/MC-LINK)
FDUL221	Line tester
DC	Supply with network adapter DC 24 V / 625 mA
B	Battery compartment 2 x 9 V



If the device has no MC link connection, it is an older device version with an RS232 connection. You will find more information on this in the next chapter.

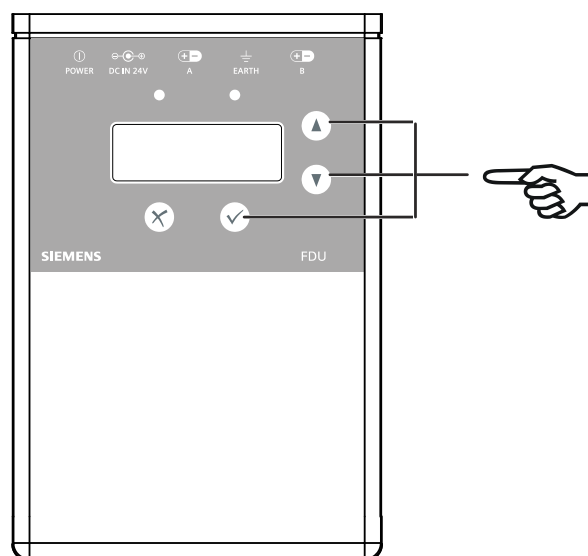
Updating the firmware

1. Select 'Update' > 'FW update FDUL221 line test device'.
 - ⇒ The 'FW update FDUL221 line test device' window opens.
 - ⇒ Cerberus-Engineering-Tool establishes the connection to the device and sets the device to update mode.
 - ⇒ The latest firmware package and the latest firmware version are suggested.
2. Click on 'Start'.
 - ⇒ If the hardware version is not compatible, click on 'Cancel' and check the hardware version. Replace the hardware and start again at point 1.
 - ⇒ The status bar indicates the update progress.
 - ⇒ The 'FW update FDUL221 line test device' window is closed after updating.
 - ⇒ The device is restarted.
 - ⇒ A success message is indicated.
3. Remove the MCL-USB adapter.
 - ⇒ The firmware is updated.

Manually setting device to update mode

Proceed as follows if you are prompted to manually set the device to update mode in step 1:

1. Simultaneously press the '▲', '▼' and '√' buttons on the device while in the 'FW update FDUL221 line test device' window pressing 'OK'.
⇒ Another 'FW update FDUL221 line test device' window is opened and you are prompted to release the buttons.
2. Only release the '√' button.
⇒ The device is set to update mode.
3. Release the '▲' and '▼' buttons.
4. Click on the 'OK' button in the 'FW update FDUL221 line test device' window and go to 'Update firmware', step 2.

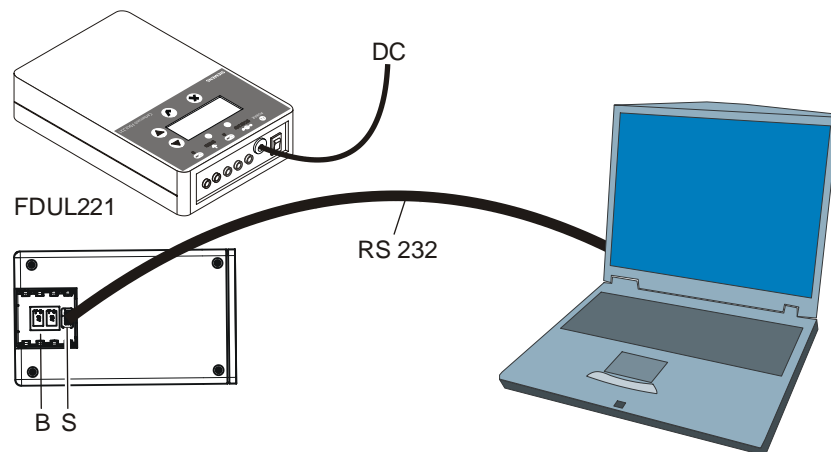


21.7 Updating firmware on the line tester with serial interface FDUL221

This chapter relates to the line tester FDUL221, device version with RS-232 connection, order no. up to A5Q00004397 02

Preparation

- ▷ The line tester is supplied via a mains adapter.
- ▷ An RS232 port is available on the PC.
- 1. Select 'File' > 'Import new FW package'.
- 2. In the selection window open the most recent file with the corresponding language F-FXS2007-XX_x_x_...zip.
- 3. Connect the device to the PC via the RS232 interface in the battery compartment.



Connect the PC to the serial line tester

FDUL221	Line tester
RS 232	Serial port for the direct connection to the PC
S	Serial interface RS 232
DC	Supply with network adapter DC 24 V / 625 mA
B	Battery compartment

Updating the firmware

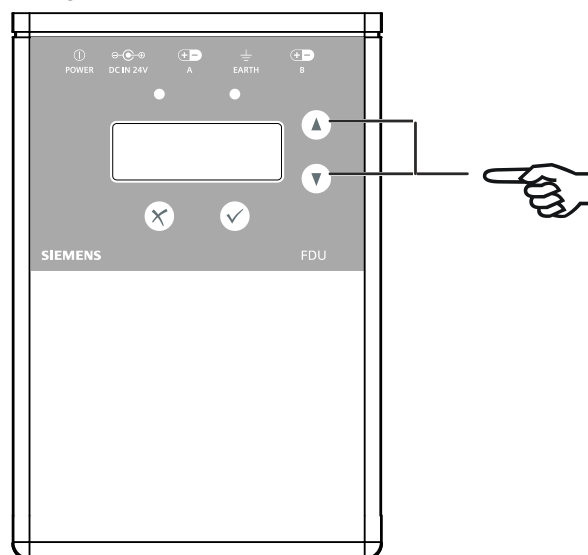
1. Select 'Update' > 'FW update serial FDUL221 line test device'.
 - ⇒ The 'FW update serial FDUL221 line test device' window opens.
 - ⇒ Cerberus-Engineering-Tool establishes the connection to the device and sets the device to update mode.
 - ⇒ The latest firmware package and the latest firmware version are suggested.
2. Click on 'Start'.
 - ⇒ The status bar indicates the update progress.
 - ⇒ The 'FW update serial FDUL221 line test device' window is closed after updating.
 - ⇒ The device is restarted.
 - ⇒ A success message is indicated.
3. Disconnect the connection with the PC.
 - ⇒ The firmware is updated.

Manually setting device to update mode

Proceed as follows if you are prompted to manually set the device to update mode in step 1:

1. Keep the '▲' and '▼' buttons on the device pressed and click on 'OK' in the 'FW update serial FDUL221 line test device' window.
 - ⇒ Another 'FW update serial FDUL221 line test device' window is opened and you are prompted to release the buttons.
2. Release the buttons.
 - ⇒ The device is set to update mode.

Click on the 'OK' button in the 'FW update serial FDUL221 line test device' window and go to 'Update firmware', step 2.



22 Commissioning external printer

The external FUJITSU DL3750+ printer can be installed and commissioned using the operating manual. The operating manual is on the CD delivered with the printer.

To operate the printer on the fire detection system FS720 settings that differ from the default values must be made in the following functions.

- 'MENU 1': Assignment of print functions to MENU1 in the printer Person Machine Interface.
- 'MENU 2': Assignment of print functions to MENU2 in the printer Person Machine Interface.
- 'HARDWRE': Changing the printer hardware options.
- 'ADJUST': Changing the setting options for the print position.
- 'CONFIG': Changing the configuration options.

The printer must be set to configuration mode in order to do this. You will find information on this in document A6V10224853. See chapter 'Applicable documents'. The following table shows the options to be set.

	Function	Value
MENU 1		
	EMULATE	XL24E
	FONT	COUR 10
	QUALITY	LETTER
	PITCH	10 CPI
	LINE SP	6 LPI
	CHAR-W	NORMAL
	CHAR-H	NORMAL
	ATTRIB	NONE
	PAGE LG	12.0 IN
	LFT-END	1 COLM
	TOP-MRG	1 LINE
	LANGUAGE	LATIN-9
	CHR-SET	SET1
	AGM	OFF
	PRF-SKP	NO-SKIP
	ZEROFNT	NO-SLSH
	CR-CODE	CR ONLY
	LF-CODE	LF & CR
	RGHTEND	WRAP
	==END==	

	Function	Value
MENU 2		
	EMULATE	DPL24C+
	FONT	COUR 10
	QUALITY	LETTER
	PITCH	10 CPI
	LINE SP	6 LPI
	CHAR-W	NORMAL
	CHAR-H	NORMAL
	ATTRIB	NONE
	PAGE LG	11.0 IN
	LFT-END	1 COLM
	TOP-MRG	1 LINE
	LANGUAGE	PAGE437
	CHR-SET	SET2
	PRF-SKP	NO-SKIP
	ZEROFNT	NO-SLSH
	DC3-CDE	ENABLE
	CR-CODE	CR ONLY
	LF-CODE	LF & CR
	RGHTEND	WRAP
	==END==	
HARDWRE		
	PPR-OUT	DETECT
	PRT-DIR	BI-DIR
	BUZZER	ON
	WORD-LG	8 BIT
	BUFFER	NONE
	INTRFCE	SERIAL
	FORMAT	8NONE 1
	BAUD-RT	9600
	PROTOCL	XON/XOF
	DSR	IGNORE
	DUPLEX	FULL
	CTS	IGNORE
	CD	IGNORE
	==END==	

	Function	Value
ADJUST		
	CNT-ORG	1 /6 IN
	CNTFINE	1 /180
	CUT-ORG	1 /6 IN
	CUTFINE	1 /180
	CNT-LFT	0 /90
	CUT-LFT	0 /90
	CUT-ADJ	0 /360
	CNT-ADJ	0 /360
	CNTADJL	0 /360
	==END==	
CONFIG		
	TEAROFF	AUTO
	TEARPOS	VISIBLE
	TEAR-EN	4 SEC
	CUTLOAD	BUTTON
	DECODE	DIRECT
	AREACNT	DISABLE
	ON-LOAD	ONLINE
	LOCK	NONE
	// S //	DISABLE
	CONT-PE	EDGE
	GATHER	DISABLE
	CUT-CTL	SPEED
	SKIP-PR	ENABLE
	STATUS	ENABLE
	BANDCTL	ENABLE
	TOF-CTL	DRIVER
	==END==	

Settings required

23 Maintenance


23.1 General

General rule

It is assumed that the 'Site' was commissioned in accordance with the existing directives, i.e. all functions have been tested and the system data have been saved and archived.

Protocol

The measuring values (according to specifications) to be recorded belong to the technical documentation in the system file.


	<p>NOTICE</p> <p>Non-observance of rules during maintenance work</p> <p>Insufficient maintenance and damage to the 'Site' or parts thereof.</p> <ul style="list-style-type: none"> • Always de-energize the 'Station' first before connecting, fitting or removing components. • Prevent electrostatic discharge. • If undertaking work on components, you must use an EMC mat. • Do not touch the modules unnecessarily with your bare hands. • Do not unnecessarily switch off the 'Site' or parts thereof for long periods of time.
---	---

23.2 Spare parts

- You will find details for ordering spare parts for 'Stations' in document A6V10227652.
- You will find details for ordering Detectors and accessories in document A6V10225323.

See chapter 'Applicable documents'.

See also

 Applicable documents [→ 8]

23.3 Testing and measuring instruments

The following table shows an overview of the test devices and measuring instruments used.

Test	Required auxiliaries	Comment
Voltage, current and resistance measuring	Universal measuring instrument	Measuring ranges: <ul style="list-style-type: none"> ● Voltage: AC/DC 1...500 V ● Current: DC 100 mA...5 A ● Resistance: 10 Ω...10 MΩ Measurement error: ≤ 2 % Internal resistance: ≥ 20 k Ω
Testing batteries	Battery tester	Load resistance: 5 Ω
Poll diagnosis data	Maintenance PC with Cerberus-Engineering-Tool	For requirements, see document A6V10210424. See chapter 'Applicable documents'.
Insert and remove FD720 point detectors	Detector exchanger DX791 Adapter for detector exchanger FDUD491	Compatible with all FD720 point detectors Some detectors also require the adapter for detector exchanger FDUD491.
Test FD720 point detectors	Test gas REF 8-S (recommended), REF 8, hot air fan	
Test manual call points, line devices and alarm devices		
Test linear smoke detector FDL241-9	Adjustment kit FDLU291	Adjustment device and black alarm test filter
Test flame detector FDF2x1-9	LE3 Test lamp	
Test C-NET detector line	Line tester FDUL221	

23.4 Preparatory work

Inform the system owner

Inform the system owner of the scope and expected duration of work and also that 'Site' operation will be restricted.

For large-scale systems fill out the system shutdown notification sheet and have this signed by the system owner.

Block system components

Block the following system components:

- Remote alarm (log out on the receiving centre)
- 'Fire controls' and alarm equipment
- Extinguishing stations

Specify the procedure

Stipulate the times for the following test sequences with the system owner:

- Test alarms (including remote transmission)
- Performance check for 'Fire controls'
- Additional instructions (if required)
- Clarifications (if required)

23.5 Test system data

System test manual

Ensure that the system test manual is available and up to date.

Remote transmission

Check that the phone numbers and the names of the remote transmission receivers are up to date.

Data backup for 'Site'

1. Check that the system data are saved.
 - ⇒ Two copies must be archived with the 'Site', one copy with the technical department.
2. Update the system data when the configuration is changed.
3. Note the date of execution in the system test manual.

Firmware

1. Read out the firmware version from the 'Station': To do this, select 'Topology' > 'Hardware tree' > 'Station' > 'More Options' > 'Show details' in the main menu.
2. Do not replace current firmware versions with the current version if this is not necessary to correct faults or add functions.

'Event memory'

Check the content of the 'Event memory' and take the necessary measures.

Change in use

Verify whether a change of use or changes to the building have an effect on the configuration and perform the necessary corrections.

Pending modification applications

Check that all pending modification applications such as corrections to the diagrams or modifications to the fire brigade orientation plans have been completed.

23.6 Testing the 'Station'

Check the hardware

- Check the condition of the housing and the components.
- Check the fixture of screws, terminals and plug connections.
- Check that the batteries are not leaking (inspection).

Check labeling

Check that the inscription strips are correct and still easily legible.

Check the function

1. Enter the password.
2. Initiate the lamp test.
3. Check switchover of operating modes from 'Manned operation' to 'Unmanned operation' and vice versa.
4. Switch an 'Area' off and on again.
5. Check the operation of an alarm.
6. Check the operation of a 'Fault'.
7. Block operation.

Clean the operating unit

Clean the display and the front plate with a wet cloth. Do not use any caustic solvents!

23.7 Check the power supply

Check the current consumption

1. Measure the current consumption during 'Emergency power operation' and for alarms with the highest alarm level (local alarm and global alarm).
2. Compare the measurement values with the calculation value for emergency current capacity.

Checking the batteries

1. Measure the battery voltage (23 V min., max. asymmetry 1 V).
2. Measure the charging current.
3. Check the battery load capacity. The load test should only be performed if the battery charge current is below 50 mA.
4. Disconnect the batteries from the charger. Do not subject the connections to strain unnecessarily.
5. Connect the battery tester to both batteries (load resistance 5 Ω).
6. Test duration for battery 7 Ah: 20 minutes.
7. Test duration for battery 12 Ah: 30 minutes.
8. Measure the battery voltage (when the tester is connected). During the test the battery voltage should not drop below 11 V per battery and not below 23 V for both batteries. Always replace both batteries!

Checking for power supply faults

1. Disconnect the mains supply cable.
⇒ The following message is displayed: 'Mains failure'.
2. Disconnect the battery supply cable.
⇒ The following message is displayed: 'Supply failure'.

Checking the mains supply cable

1. Check whether the site mains supply cable is correctly fuse-protected and labeled (fire detection system).
2. Check whether installed overvoltage dischargers are in order.

23.8 Testing the printer

1. Check the roll of paper in the printer and ensure that there are spare rolls available.
2. Initiate the printer test and check the print-out for legibility and correct printing.
3. Check whether the events are correctly printed out.

You will find more information about the printer in document A6V10211076. See chapter 'Applicable documents'.

See also

📄 Applicable documents [→ 8]

23.9 Checking 'Site' function

Test the functions of the 'Site' in the various test modes:

You will find information about testing a 'Site' in the chapter 'Testing' in document A6V10211076. See chapter 'Applicable documents'.

See also

📄 Applicable documents [→ 8]

23.10 Intervals for testing the system function

'Self test' for the 'Detectors'

The 'Self test' is an automatic performance check for FD720 'Detectors'. The function of the 'Detectors' must be checked regularly on site despite this.

Detector inspection

- Annual visual check of all 'Detectors'.
- Replace 'Detectors' that are badly soiled or mechanically damaged.

Function test

The following table shows the intervals recommended for the function check. National specifications always take priority.

Function	Activity	Interval (years)		
		1	2	5
Software	Check date and time.	X		
Detector lines: C-NET	Activate an 'Automatic detector' and a 'Manual call point' per 'Line'.	X		
	Activate all 'Manual call points'.		X	
	Trigger all automatic fire detectors.		X	
	Check all 'Detectors' for soiling and application.	X		
	Check the function of the input/output modules.		X	
	<ul style="list-style-type: none"> • On each 'Line' check whether a short-circuit or open line triggers a 'Fault'. • Check the loop line function. • During short-circuit also check the separator function. 			X

Function	Activity	Interval (years)		
		1	2	5
'Fire controls'	Check activation of the 'Controls' up to and with the interface.		X	
	Check the effects of the 'Controls' owned by the customer. Arrange a time with the customer.		X	
'Mains failure'	Check how long it takes until the 'Emergency power operation' fault message is displayed during power failure.			
Alarm devices	In 'Emergency power operation' check all alarm devices taking the following event category into account: <ul style="list-style-type: none"> • 'Pre-ALARM' • 'ALARM' • 'Fault' 	X		
	Check the remote transmission equipment in accordance with the manufacturer's instructions.	X		
Alarm organization	Check the function of the delay times t1 and t2.	X		
	Activate a global alarm with an 'Automatic detector' in the 'Unmanned operation' operating mode.	X		
	Activate a local and global alarm by setting a 'Manual call point' to the 'Manned operation' and 'Unmanned operation' operating modes.	X		
	Check automatic switchover from 'Manned operation' to 'Unmanned operation' on the basis of the event memory entries.	X		
	Check activation of the remote transmission equipment with 'ALARM'.	X		

Intervals for the function test


23.11 Completion work

1. Activate a test alarm through the system operator with remote transmission.
2. Issue subsequent instructions if necessary.
3. Ensure that the system file is available and up to date.
4. Update the system data when the central configuration is changed. Archive a copy with the 'Site' and a copy in the office.
5. Check the master data sheet (phone no., contact person, etc.).
6. Replace all used material.
7. Cancel all blockings and 'OFF' statuses.
8. Have the revision confirmed by the system owner.

24 Repair

24.1 Disconnecting 'Station' from the power supply

Work on an open 'Station', e.g. changing components, cabling, etc. must only be performed when the 'Station' is current-free. For this purpose the batteries must be disconnected and the mains connection must be interrupted. The 'Station' cannot be shut down.

	NOTICE
	Connecting or removing components during operation Damage to components <ul style="list-style-type: none"> Do not connect or remove components during operation.



You will find information about installing and uninstalling the components in document A6V10210390. See chapter 'Applicable documents'.

1. First disconnect the negative battery terminals, then the positive terminals.
2. Remove the disconnect terminal block that is mounted on a DIN rail in the housing.
 - ⇒ The mains connection is interrupted.
3. Exchange the components.
4. Re-insert the disconnect terminal block.
 - ⇒ The mains connection is intact.
 - ⇒ The 'Station' starts.
5. First connect the negative battery terminals, then the positive terminals.
6. Enter the date and time. To do this, select the 'Settings/administration' > 'System commands' > 'Set system time' menu items.
7. If need be, carry out partial commissioning.




Date and time are not saved in the 'Station'. The date and time must be reset to restart the 'Station'.

24.2 Spare parts

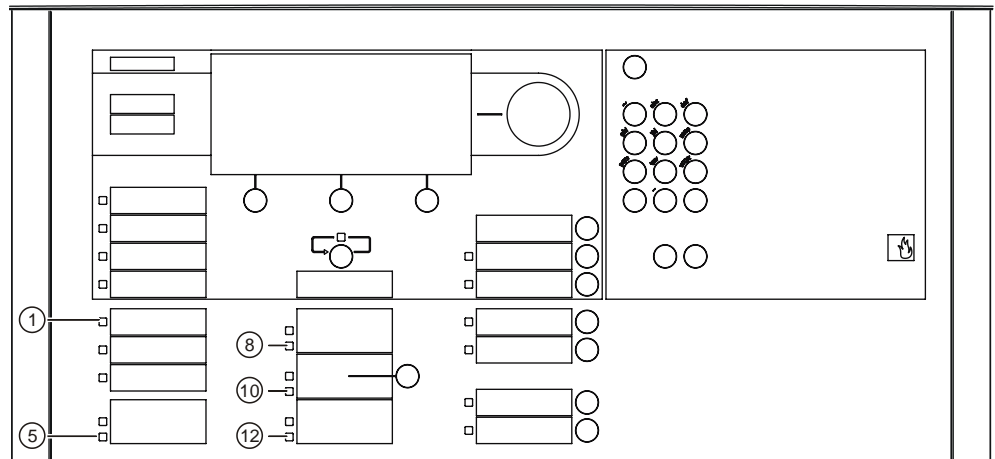
- You will find details for ordering spare parts for 'Stations' in document A6V10227652.
- You will find details for ordering Detectors and accessories in document A6V10225323.

See chapter 'Applicable documents'.

See also

 Applicable documents [→ 8]

24.3 Fault messages on the Person Machine Interface



Fault messages on the Person Machine Interface


The table below shows the causes and measures should a fault be displayed.

LED	LED flashes	Cause	What must be done
1	FAULT	The 'Site' has a fault	<ul style="list-style-type: none"> Check whether another fault LED is flashing, if not: <ul style="list-style-type: none"> Check the display Check whether the 'Fault' control input is activated
5	System Fault	Failure of the main CPU	<ul style="list-style-type: none"> Visual check of the cable connections Check whether the red LED H37 on the operating unit FCM72xx is on: <ul style="list-style-type: none"> Exchange PMI & mainboard
		'Fault of a component	<ul style="list-style-type: none"> 'Restart 'Station' <ul style="list-style-type: none"> When the 'Fault' is still indicated: exchange the module
		Communication fault of a networked 'Station'	<ul style="list-style-type: none"> Check the transmission line Check the faulty 'Station'
8	Remote alarm Fault / Off	Transmission equipment has a 'Fault'	<ul style="list-style-type: none"> Check remote transmission
10	Alarm device Fault / Off	'Acoustic control line 'Fault'	<ul style="list-style-type: none"> 'Check the 'Line' for open line/short-circuit or end-of-line element (EOL) is missing or defective
12	Control function Fault / Off	'Fire control line 'Fault'	<ul style="list-style-type: none"> 'Check the 'Line' for open line/short-circuit Check the function of the external control devices Check the function, any existing feedback switch

24.4 Fault indicators on components

The components are equipped with LED indicating the status of the component. You will find the meaning of the indications in document A6V10210368. See chapter 'Applicable documents'.

See also

 Applicable documents [→ 8]

24.5 Communication problems in networked systems

Date and time are not permanently saved in the 'Station'. If this data is not defined correctly, it is not possible to communicate with the corresponding 'Station' in the network or via Cerberus-Engineering-Tool.

Date and time

The date and time must be checked regularly for the following reasons:

- The deviation of the internal clock is up to four minutes per month.
- When data is downloaded, and when a 'Station' is restarted, the internal clock does not continue working.
- If a 'Station' is de-energized, the date and time of the internal clock is lost.

Moving the network cable from one 'Station' to the next

Wait at least two minutes before inserting the cable into the next 'Station'.

If 'Stations' are fitted close to one another, you may be able to move the network cable from one 'Station' to the next without first having to execute the 'Commissioning' > 'Disconnect' command in Cerberus-Engineering-Tool. If this is done, a connection cannot be immediately re-established on the next 'Station'.

24.6 Non-stationary devices of the same type have been swapped over

When C-NET devices have been swapped over in their bases, e.g. while work is carried out, the 'Line' is not fault-free.

The following message is shown on the display of the Person Machine Interface for each C-NET device that has been swapped over:

'Zone', 'Serial no. ("ID-Nr.")', 'Device missing'

If the C-NET detector line was restarted, the following message is displayed for each swapped C-NET device:

'Zone', 'Serial no. ("ID-Nr.")', 'Dev.location fault'

To enable the 'Station' to become fault-free again, at least the device types in the corresponding bases must be correct. 'Faults' of C-NET devices of the same type that have been swapped over can then be rectified using the Person Machine Interface without having to find the original base.

Procedure

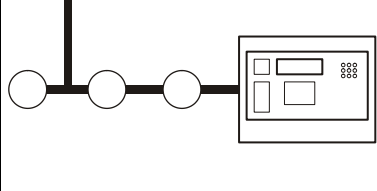
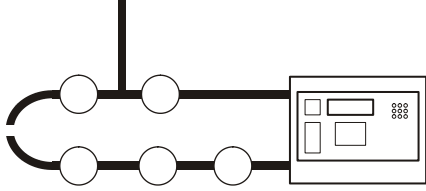
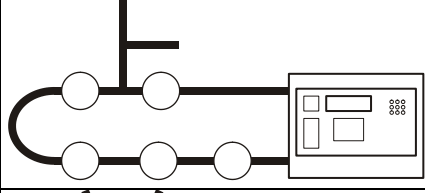
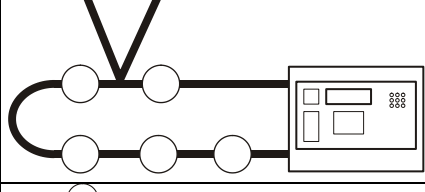
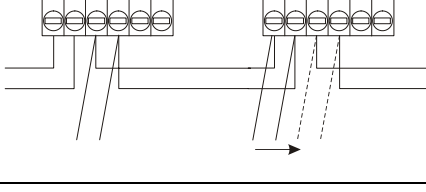
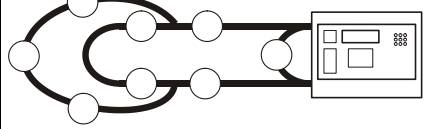


You will find additional information about the individual steps on the specified pages.

1. Rectify localization errors. Link [→ 33]
2. Connect the PC to the 'Station'. Link [→ 20]
3. Load the configuration from the 'Station' to the PC. Link [→ 24]
4. Disconnect the PC from the 'Station'. Link [→ 20]

24.7 Error message 'Topology is invalid'

If the topology of a C-NET detector line is invalid, after the detector line has been read in, the error message 'Topology is invalid' is displayed. The table below shows invalid topologies.


Stub on stub or loop interrupted		
Stub on stub on loop		
Several stubs starting from same location on loop		
Loop on loop		

Invalid topologies

Troubleshooting

1. Check the detector line with the line tester FDUL221. You will find information on this in document 008250. See chapter 'Applicable documents'.
2. Create a valid topology:
 - Rectify the fault by changing over the wiring or plan the detector line again.
 - If there are several stub outputs between two C-NET devices, change over the wiring or add a line separator FDCL221 between each stub.
3. Read in the C-NET detector line again.

See also

 Reading in devices [→ 31]

24.8 Restart 'Station'



The configuration of the 'Station' remains the same.

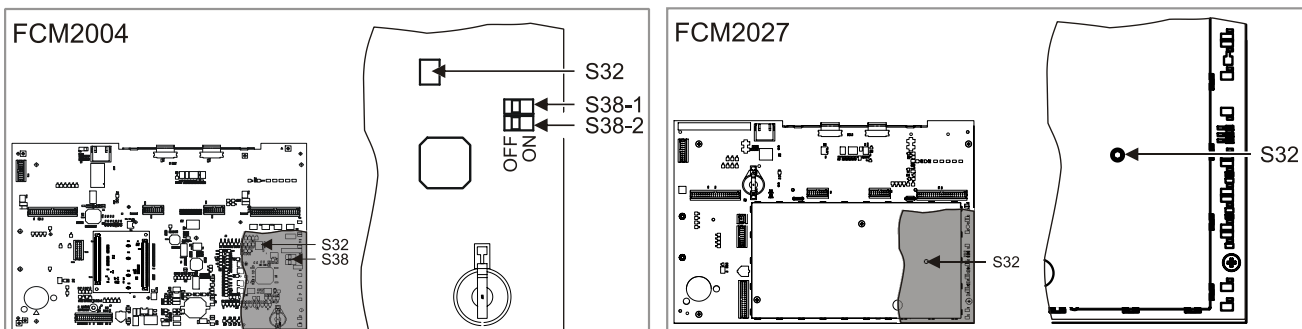
There are the following ways in which to restart the 'Station':

- Via the menu on the display
- With the 'S32' button

Via the menu on the display

1. Press <MENU>.
 - ⇒ The PIN input dialog is indicated.
2. Enter a valid PIN and confirm with <ok>.
 - ⇒ The 'User successfully logged in' message is displayed.
 - ⇒ The main menu is displayed.
3. Select the 'Topology' > 'Hardware tree' > 'Station' menu items.
 - ⇒ The elements of the 'Station' are listed.
4. Select module 101 or module 102 'CPU (FCM20xx)'.
5. Press the 'More Options' softkey and select 'Execute commands'.
6. Select the 'Reset module' command.
 - ⇒ The 'Station' restarts.
 - ⇒ After a few minutes, the 'Buzzer' sounds twice.
7. Press <Acknowledge> on the Person Machine Interface to switch off the 'Buzzer'. Do not perform any more actions on the 'Station' until the 'Buzzer' has sounded for the second time.

With the 'S32' button




- ▷ The switches S38-1 and S38-2 are set to the 'OFF' position on the PMI & mainboard FCM2004.
1. On the PCB of the operating unit, press and hold down the 'S32' button for < 2 s.
 - ⇒ The 'Station' restarts.
 - ⇒ After a few minutes, the 'Buzzer' sounds twice.
 2. Press <Acknowledge> on the Person Machine Interface to switch off the 'Buzzer'. Do not perform any more actions on the 'Station' until the 'Buzzer' has sounded for the second time.

24.9 Restoring factory setting on the 'Station'

There are the following ways in which to restore the factory setting on the 'Station':

- Via the menu on the display
- With the 'S32' button

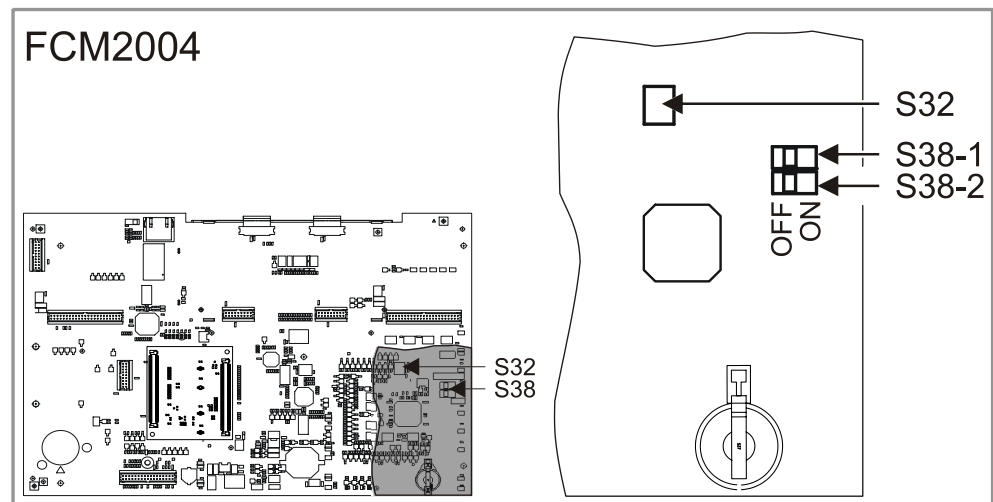
	NOTICE
	<p>Restoring factory setting on the 'Station'</p> <p>The configuration of the 'Station' is deleted!</p> <ul style="list-style-type: none"> • Save the configuration data for the 'Station' before restoring the factory setting.

Via the menu on the display

1. Press <MENU>.
 - ⇒ You are prompted to enter a PIN.
2. Enter a valid PIN and confirm with <ok>.
 - ⇒ The 'User successfully logged in' message is displayed.
 - ⇒ The main menu is displayed.
3. Select the 'Topology' > 'Hardware tree' > 'Station' menu items.
4. Press the 'More Options' softkey and select 'Execute commands'.
5. Select the 'Factory reset' command.
 - ⇒ The 'Station' restarts.
 - ⇒ After a few minutes, the 'Buzzer' sounds twice.
6. Press <Acknowledge> on the Person Machine Interface to switch off the 'Buzzer'. Do not perform any more actions on the 'Station' until the 'Buzzer' has sounded for the second time.
7. Enter the date and time. To do this, select the 'Settings/administration' > 'System commands' > 'Set system time' menu items.

PMI & mainboard FCM2004

1. Set the 'S38-1' switch to 'ON' on the rear of the operating unit.
2. Press the 'S32' button for > 2 s until the 'Station' restarts.



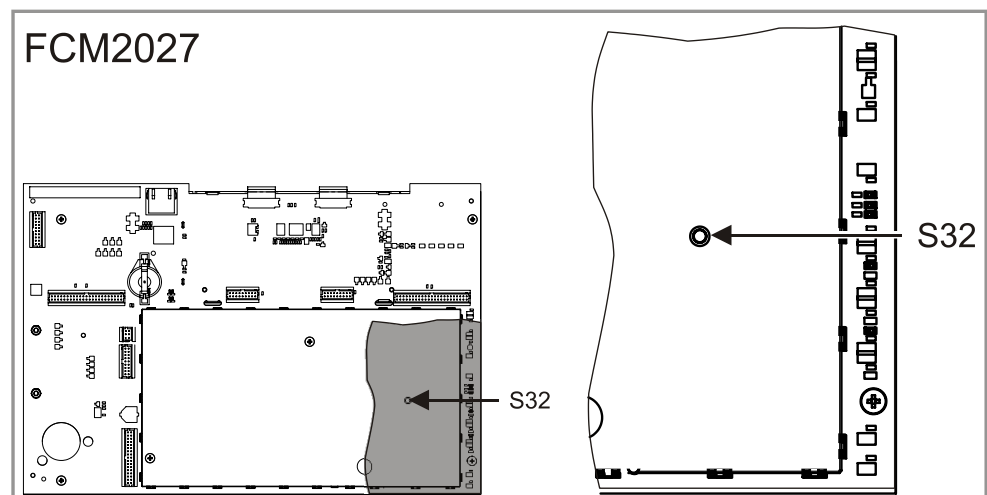
⇒ The 'Station' restarts.

3. Set the 'S38-1' switch to 'OFF' after the restart.

⇒ After a few minutes, the 'Buzzer' sounds twice.
4. Press <Acknowledge> on the Person Machine Interface to switch off the 'Buzzer'. Do not perform any more actions on the 'Station' until the 'Buzzer' has sounded for the second time.
5. Enter the date and time. To do this, select the 'Settings/administration' > 'System commands' > 'Set system time' menu items.

PMI & mainboard FCM2027

1. Keep the 'S32' button on the rear of the operating unit pressed and simultaneously press <Reset> on the Person Machine Interface at the same time until the 'Station' restarts (>2 s).



⇒ The Station restarts.

⇒ After a few minutes, the 'Buzzer' sounds twice.

2. Press <Acknowledge> on the Person Machine Interface to switch off the 'Buzzer'. Do not perform any more actions on the 'Station' until the 'Buzzer' has sounded for the second time.
3. Enter the date and time. To do this, select the 'Settings/administration' > 'System commands' > 'Set system time' menu items.

Index

A

Acceptance test, 16

Alarm counter, 71

Auto-configuration, 35

Definition of terms, 18

Detector line, 29

station, 28

B

Back-up, 25

C

Commissioning, 17

According to wiring sequence, 15

Auto-configuration, 35

Networked station, 40

Overview, 17

Standalone station with PC, with pre-configuration, 39

Standalone station with PC, without pre-configuration, 38

Standalone station without PC, 35

With serial number, 15

Without PC, 35

Communication problems, 110

Component

Indication of faults, 109

Configuration

Conversion, 77

Load to station, 21, 23

Loading to PC, 24

Connecting a sub-stub to a loop, 68

Connection to the station, 20

Connectivity, 20

Conversion, 77

Configuration, 77

Convert stubs into loops, 67

CPU

Updating the firmware, 79

CPU (other)

Updating the firmware, 84

Customer text, 36

D

Date/time, 110

Deleting

Device, 31

Detector

Test mode, 32

Testing, 59

Detector inspection, 106

Detector line

Auto-configure, 29

Expand, 66

Install, 15

ON, 30

Restart, 30

Switch off, 30

Testing, 15

Detector self-test, 106

Device

Remove, 60

Remove (base without loop contact), 62

Removing (stationary), 67

Removing for good, 65

Replace (base without loop contact), 62

Replacing (different types), 61, 63

Replacing (same type), 60

Replacing (stationary), 68

Swapped, 110

Temporarily remove, 64

Download, 21, 23

E

Error message

'Topology is invalid', 111

Ethernet switch (MM) FN2008 A1, 46

Event memory, 71

Expand

Detector line, 66

Site, 41

External printer, 99

F

Factory reset, 113

Factory setting, 113

Fault indicators, 109**FCI2007-A1 I/O card (RT), 58****FCI2009-A1 I/O card (horn/monitored), 58****FDUL221 line tester**

Updating the firmware, 95

FDUL221 serial line tester

Updating the firmware, 97

FDUZ221 MCL-USB adapter

Updating the firmware, 88

Fire brigade periphery module FCI2001-D1, 57**Firewall**

Security module (firewall) FN2009-A1, 49

Windows firewall, 71, 77

Floor repeater display

Updating the firmware, 91

Floor repeater terminal

Updating the firmware, 89

FN2008 A1

Ethernet switch (MM) FN2008-A1, 46

FN2009-A1 safety, 49**FT2001-A1 mimic display driver**

Updating the firmware, 93

FT2010 floor repeater terminal

Updating the firmware, 89

FT2011 floor repeater display

Updating the firmware, 91

FUJITSU DL3750+, 99**Function test, 33, 106, 106****Fuse, 25****H****Hardware reset**

station, 112

I**I/O card (horn/monitored) FCI2009-A1, 58****I/O card (RT) FCI2007-A1, 58****Indication of faults**

Component, 109

Initialize

station, 21, 21

Install

Detector line, 15

L**Line tester**

Updating the firmware, 95

Load

From PC to station, 21, 23

From station to PC, 24

Load data to PC

Site, 24

Load data to the station

Site, 23

Localization error, 33**M****Main CPU**

Updating the firmware, 79

Maintenance, 102**Manual call point**

Replace, 69

MCL-USB adapter

Updating the firmware, 88

Measuring instrument, 103**Merge**

Sites, 42

Mimic display driver

Updating the firmware, 93

N**Network cable**

Moving, 110

Networked station, 40**Normal operation, 32****O****ON**

Detector line, 30

P**Password, 79, 81, 84, 86****PC**

Connect to station, 20

Disconnecting from station, 20

PMI

Fault indicators, 109

Power supply

Configuring, 36

Testing, 105

Pre-configuration

Definition of terms, 18

Primary Setup Tool, 47

Printer

Testing, 106

R**Radio gateway FDCW221, 94**

Updating the firmware, 94

Radio gateway FDCW241, 94

Updating the firmware, 94

Read in

Definition of terms, 18

Device, 31

Remove

Device, 60, 65

Device (base without loop contact), 62

Device (stationary), 67

Device (temporary), 64

Replace

Device (base without loop contact), 62

Device (different types), 61, 63

Device (same type), 60

Device (stationary), 68

Manual call point, 69

Restart

station, 112

S**Scalance X204 2, 46****Security module (firewall) FN2009-A1, 49****Serial line tester**

Updating the firmware, 97

Series number, 15**Set parameter set**

Use Person Machine Interface, 37

Site

Expand, 41

Load data to PC, 24

Load data to the station, 23

Merge, 42

Test intervals, 106

Spare parts, 102, 108**Stand-alone station, 35, 38, 39****station**

Auto-configure, 28

Disconnect power, 108

Factory setting, 113

Hardware reset, 112

Initialize, 21, 21

Load data, 21

Mount and install, 16

Resetting, 113

Restart, 112

Switching off, 108

Swapped

Device, 110

Switch off

Detector line, 30

Switching off

station, 108

System data, 104**T****Test, 33, 106****Test intervals, 106, 106****Test mode, 32**

Detector, 32

Exit, 32

Test unit, 103**Testing**

Detector, 59, 59

Detector line, 15

Function, 106

Power supply, 105

Printer, 106

System data, 104

Time/date, 110**Topology is invalid, 111****U****Uninstalling**

Device, 31

Update BDV, 76**Updating the firmware**

Additional CPUs, 84

Main CPU and additional CPUs, 79

Periphery devices, 88

station, 71

Upload, 24

W

Windows firewall, 71, 77

Z

Zone

ON, 30

Switch off, 30



Issued by
Siemens Switzerland Ltd
Infrastructure & Cities Sector
Building Technologies Division
International Headquarters
Gubelstrasse 22
CH-6301 Zug
Tel. +41 41-724 24 24
www.siemens.com/buildingtechnologies

© 2008-2013 Copyright Siemens Switzerland Ltd
Technical specifications and availability subject to change without notice.