SIEMENS

FS720

Fire detection system

Configuration

MP1XS

Building Technologies

Fire Safety & Security Products

Technical specifications and availability subject to change without notice.

Table of contents

1 About this document

Goal and purpose

This document describes the configuration of an FS720 fire detection system with Cerberus-Engineering-Tool FX7230.

Scope

The information in documents A6V10211076, operation and A6V10210416, commissioning is prerequisite for configuration of the fire detection system with Cerberus-Engineering-Tool FX7230.

This document is valid for market package MP1XS.

Target groups

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

Target group	Activity	Qualification
Commissioning personnel	● Configures the product at the place of installation according to customer-specific requirements. ● Checks the product operability and releases the product for use by the operator. ● Searches for and corrects malfunctions.	● Has obtained suitable specialist training for the function and for the products. ● Has attended the training courses for commissioning personnel.
Maintenance personnel	● Carries out all maintenance work. ● Checks that the products are in perfect working order. ● Searches for and corrects malfunctions.	● Has obtained suitable specialist training for the function and for the products.

Document identification

Position	Information
Title page	● Product type ● Product designation ● Document type
Last page, bottom left	● Document ID ID_ModificationIndex_Language_COUNTRY ● Edition date
Last page, bottom right-hand side	● Manual ● Register

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
'Text'	Quotation, reproduced identically
<Key>	Identification of keys

Supplementary information

The  symbol identifies supplementary information such as a tip for an easier way of working.

Supplementary information is labelled with the 'i' symbol.

Technical terms

Term	Explanation
ES	Product version
C-NET	Addressed detector line

Reference documents

Document ID	Title
A6V10210355	FS720, Fire Detection System, Description
A6V10210416	FS720, Fire Detection System, Commissioning, Maintenance, Troubleshooting
009122	Input/output module FDCIO223 in, technical manual

History of changes

Document ID	Edition date	Brief description
A6V10210424_c_en_--	08.2009	Chapter 8.2.2 restructured Chapter 8.4.3.1 and 8.5.6.4 new
A6V10210424_b_en_--	05.2009	Adaptations for MP1XS
A6V10210424_a_en_--	08.2008	First edition

2 Safety

2.1 Safety notices

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.
NOTICE	*NOTICE* identifies possible damage to property that may result from non-observance.

How risk of injury of presented

Information about the risk of injury is shown as follows:

⚠ WARNING
Nature and origin of the danger Consequences if the danger occurs ● 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 ● 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

- 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 alarming control 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 layout and 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

Disclaimer

We have checked that the content of this document matches the hardware and software described. Despite this, we cannot rule out deviations and cannot therefore assume liability for them matching completely. The details in this document are checked regularly and any corrections needed included in subsequent editions.

We are grateful for any suggestions for improvement.

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.

- 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.

- 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 Installation

3.1 System requirements

Hardware

Component	Minimum requirements
Processor	Pentium M1.6
Main memory	512 MB
Hard disk	400 MB, better still 1 GB of free memory
CD drive R/W	present
Network connection	Ethernet RJ45
Screen resolution	1024 x 768
Colours	65535

Software

Operating system	Windows 2000, Windows XP, Windows Vista (32-bit version only)
Acrobat Reader	Version 6 or higher
Browser	Internet Explorer or similar browser

Administrator rights to the OS of the PC are required for the installation of the software.

3.2 Installation of the Cerberus Engineering Tool set

The following components are installed with the installation of the Cerberus Engineering Tool set FX7230:

- FXS7211 (firmware package)
- FXS7212 (Cerberus Engineering Tool)
- FXS2004 (Basic data variant for set-up of new systems)
- FXS7216 (Help documentation)

FX7230 Installing Cerberus Engineering Tool set

1. Insert the program CD into the drive.

   ⇨ The installation routine starts and guides you through the installation.

2. Follow the instructions of the installation routine and observe the installation paths.

If the installation routine does not launch automatically, proceed as follows:

1. Click "Start" > "Run" in the Windows task bar.
2. Enter the following command in the "Run" dialog box: D:\FX7230_"Version"
   "D" is the letter assigned to the CD drive.
   "Version" is the sequence of characters after "FX7230_".

Installation paths

During installation, you can change the standard installation paths offered.
You can change various paths subsequently within the program, but you must then move the respective folder manually to the new location.
We do not recommend that you change the program path after successful installation in the program.

You can change the following standard installation paths during installation:

- Target directory

  C:\Program Files\Siemens\FX7230\"VersionID" (*)

- Common data directory

  C:\Documents and Settings\All Users\Application Data\Siemens\FX7230\"VersionID"

- Log file directory

  C:\Documents and Settings\"User name"\Application Data\Siemens\F-FX7230\\"VersionID" (*)\Logfiles
  The path for the log files cannot be changed afterwards.

(*) "VersionID" = Name of the program and version

3.3 Starting the program

You can start the program as follows:

- Click the program symbol on the desktop.
- In the task bar click "Start" > "Programs" > "Siemens" > "FX7230" > XX_xx_Version > "F-FXS7212".

3.4 Exit the program

You can exit the program as follows:

- In the menu bar, click on 'File' > 'Exit'.
- Click on the 'X' button in the title bar.

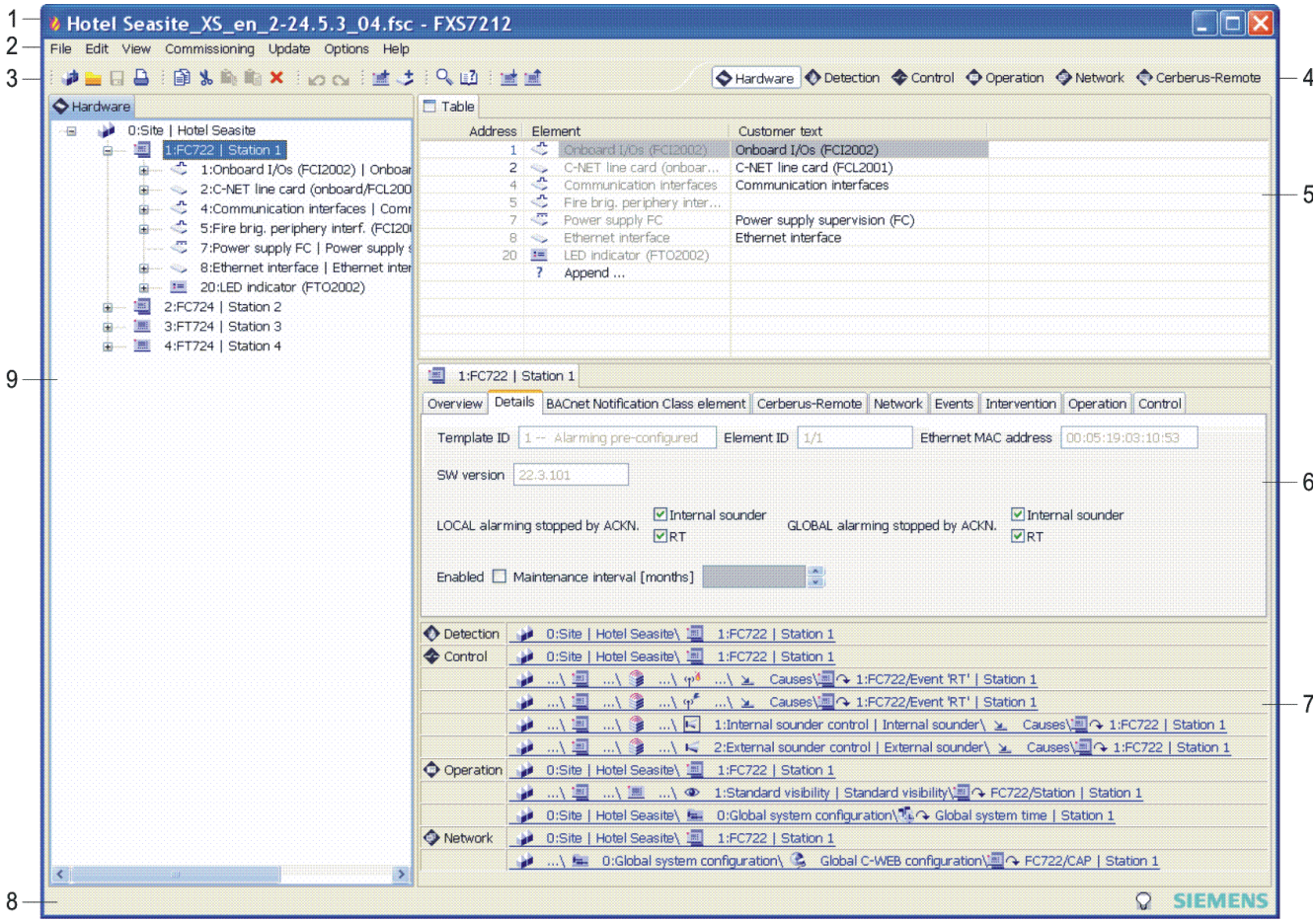
If you have made changes in the program and not saved these, a window opens asking 'Do you want to save the changes?'.

4 GUI

The Cerberus Engineering Tool distinguishes between normal BDV mode and expert BDV mode.

The detailed explanations of the buttons relate to expert BDV mode. For details of normal BDV mode, please refer to document A6V10244705, Normal BDV mode vs. expert mode.

4.1 Overview of the program window



Program window

1 Title bar
2 Menu bar
3 Tool bar
4 Task cards
5 Table
6 Detail editor
7 Hyperlinks
8 Status bar
9 Tree

4.2 Menu bar

The menu structure and menu items are fixed for each task card. Individual menu items may be shaded out depending on the task card selected. Menu items that can not be run are shaded gray.

There are the following main menus and submenus:

Main menu	Submenu	Description
File	New site	Opens the 'Create new site' window
	Open	Opens the existing site configuration
	Save	Saves the current site configuration
	Save as ...	Saves the current site configuration under a new name
	Site properties	Opens the 'Site properties' window
	Import new FW package	Imports new firmware
	Import new BDV	Imports a new BDV
	Import new help	Imports new Help file
	SiB-X export	Exports configuration data definitions in SIB-X format
	Compare configurations	Compares site configurations and BDVs
	Reports	Opens the 'Reports' window
	Site export (XML)	Exports system data in XML format
	Recently opened sites	Opens one of the recently opened sites
	Exit	Exit Cerberus-Engineering-Tool
Edit	New station	Opens the 'New station' window
	New station with address	Opens the 'New station with address' window
	New element	Opens the 'New element' window
	Undo	Undoes the last action
	Redo	Restores actions that have been undone
	Copy	Copies selected elements/subtrees
	Cut	Cuts selected elements/subtrees
	Paste	Pastes (inserts) copied elements/subtrees
	Paste without children	Pastes copied elements without children elements
	Delete	Deletes selected element
	Replace element	Replaces element template
	Change element address: $(NUMBER)	Decreases the address of the selected element as well as all higher elements by one
	Change element address: $(NUMBER)	Increases the address of the selected element as well as all higher elements by one
	Convert site configuration	Converts the site configuration
	&Show conversion log	Opens the 'Conversion log' window
View	Find	Opens the 'Find' window
	Find and replace	Opens the 'Find and replace' window
	Find next	Jumps from one hit to the next
	Show problems	Opens the 'Problems' window
	Show all problems	Opens the 'All problems' window

Main menu	Submenu	Description
Commissioning	Assign	Opens and closes the 'Assign' window
	Unassign	Cancels link
	Disconnect	Interrupts the communication with the station
	Initialize station	Initializes networked station
	Download site configuration	Loads site configuration into station
	Upload site configuration	Loads site configuration into PC
	Upload site event memory	Loads the event memory of the site into the PC
	Upload site log files	Loads log files from selectable stations to the PC
	Upload diagnostics data	Loads diagnostics data of the site into the PC
Update	FW update main CPU	Updates the firmware of the main CPU
	FW update additional CPUs	Updates the firmware of additional CPUs
	FW update standard peripheral device	Updates the firmware of peripherals
	FW update FDUZ221 update box	Updates the firmware of the MCL-USB adapter
	FW update FDUL221 line tester	Updates the firmware of the line tester
	FW update serial FDUL221 line tester	Updates the firmware of the line tester with serial interface
Network	Convert to CAP	Converts a SAFEDLINK station or Ethernet station into a CAP station
	Convert to Safe D-Link host	Converts a CAP station into a SAFEDLINK station
	Convert to ethernet host	Converts a CAP station into an Ethernet station
	Create CAP configuration	Configures a standalone station as a CAP station for remote access with Cerberus-Remote or Cerberus-Engineering-Tool
Options	Preferences	Opens the 'Preferences' window
Help	Help	Opens the documentation overview
	View additional documents	Opens a file selection window for additional documents
	About	Opens the 'FXS7212' window with details on the installed version

4.3 Tool bar

The toolbar allows the operator to access functions quickly.

The following functions can be run directly via the toolbar:

Symbol	Menu Item	Description
	'New site'	Opens the 'Create new site' window
	'Open'	Opens existing Site
	'Save'	Saves current configuration of Site
	'Reports'	Opens the 'Reports' window
	'Copy'	Copies selected elements/subtrees
	'Cut'	Cuts selected elements/subtrees
	'Paste'	Pastes (inserts) copied elements/subtrees
	'Paste without children'	Pastes copied elements without children elements
	'Delete'	Deletes selected element
	'Undo'	Undoes the last action
	'Redo'	Restores actions that have been undone
	'New station'	Opens and closes the 'New station' window
	'New element'	Opens and closes the 'New element' window
	'Help'	Opens the documentation overview
	'Find'	Opens the 'Find' window
	'Download site configuration'	Loads site configuration into station
	'Upload site configuration'	Loads site configuration into PC
	'Assign'	Opens and closes the 'Assign' window

4.4 Help and tooltips

When working with the software, there are two information sources available:

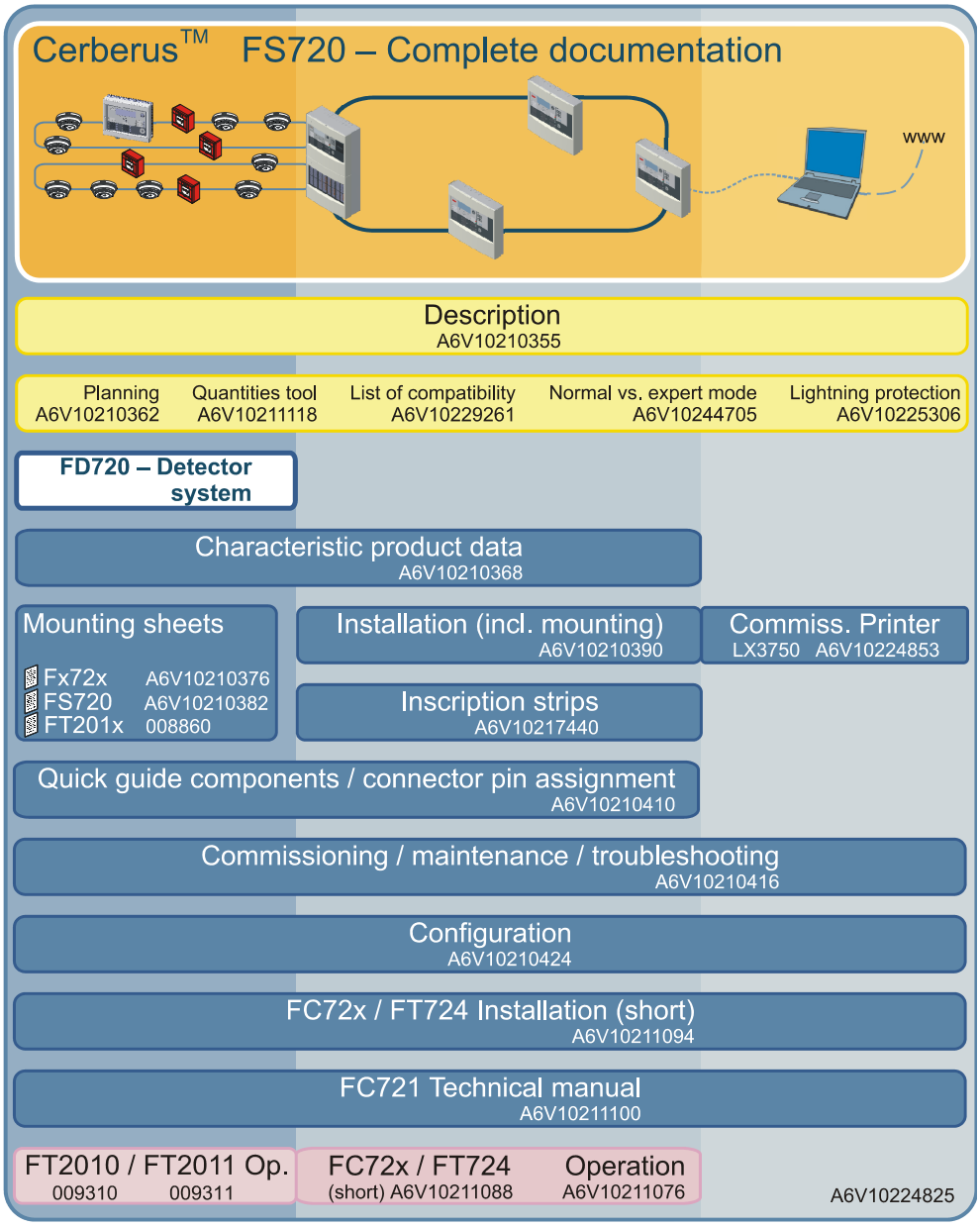
- Help
- Tooltips

Help

There are three ways of calling up the Help:

- Press <F1>.
- Select 'Help' > 'Help' from the menu bar.
- Click on the symbol in the toolbar.

A PDF document containing an overview of the documentation opens. To open a document, click on its name in the overview.



Graphic with an overview of the documentation

Tooltips

Tooltips are windows within the program with context-sensitive detail information. Tooltips are shown when the mouse pointer is moved over a panel or name of a register in the detail editor.

4.5 Pre-settings

Clicking on the 'Options' > 'Preferences' menu item opens the 'Preferences' window. This window contains the site and BDV directories as well as pre-settings.

The 'Preferences' window has the following views:

- 'Editing preferences'
- 'Firmware package preferences'
- 'LRC Server preferences'
- 'Periphery update tool preferences'
- 'Preferences'
- 'Site preferences'

In the 'Preferences' window you may change program paths to the folders from the master directory.

In addition, you may perform other settings regarding the language selection and program behavior.

If you change program paths then you must move the respective folder manually to the new location.

The name "VersionID" in the following is the wildcard for the name of the currently installed program version, e.g.: EN_en_1-V1.

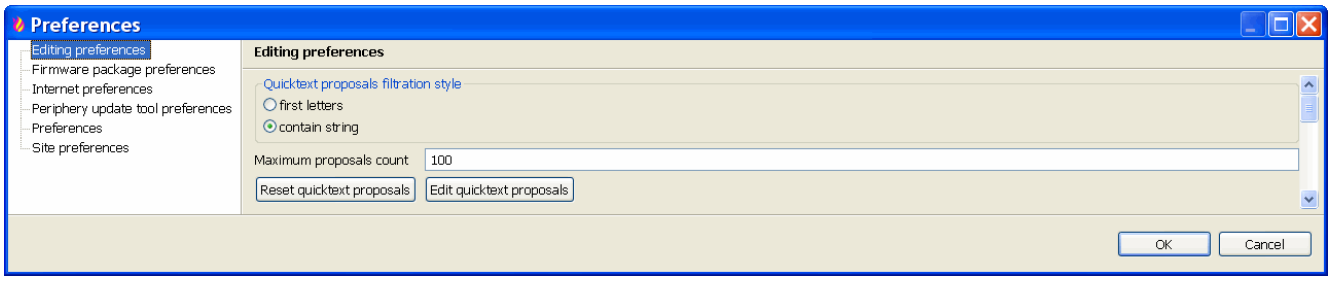
If, during installation of the software, no other path has been entered, then the root directory or the "VersionID" folder is in the following path:

C:\Documents and Settings
All Users\Application Data\Siemens\FX7230\"VersionID"

The common master directory contains the following subfolders:

- 'Additional documents directory:'
- 'BDV'
- 'FS720_SW'
- 'Help'
- 'Logfiles'
- 'Sites'
- 'Technical files' (trace reports)

4.5.1 Editing preferences

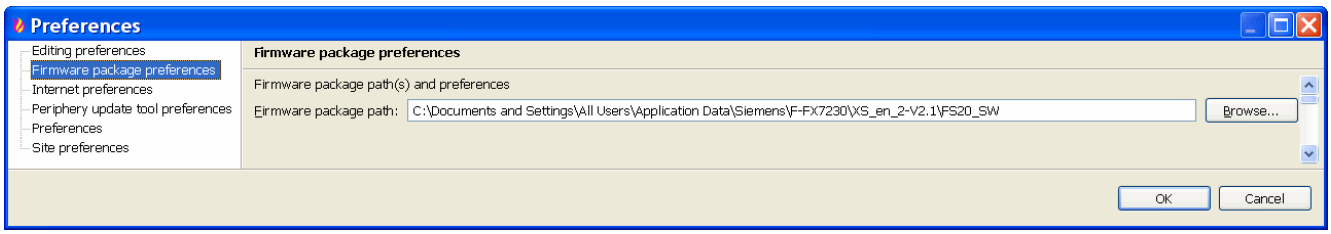


Editing preferences

The 'Editing preferences' view contains pre-settings for predictive text entry of customer texts and counter-measures texts:

- Number of proposed texts which Cerberus-Engineering-Tool saves.
- The proposals are listed by one of two selections:
  - by comparison of initial letters
  - by comparison of the letter sequence at any position in the word
- The 'Reset quicktext proposals' button is used for deleting the proposed texts.
- The 'Edit quicktext proposals' button is used for editing the proposed texts.

4.5.2 Firmware package preferences

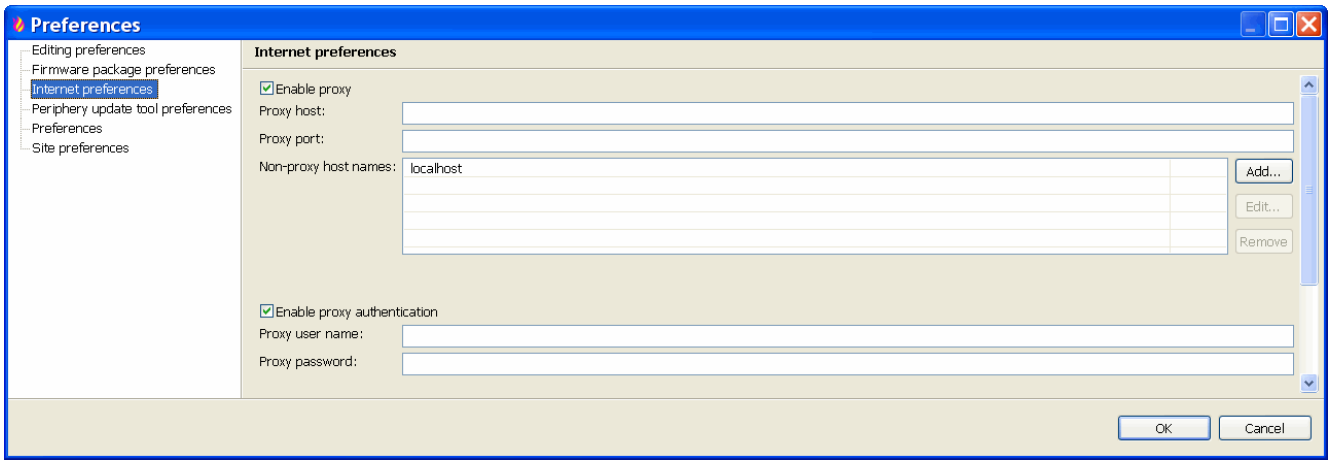


Firmware package preferences

The 'Firmware package preferences' view contains the path to the 'FS720_SW' folder, in which program-specific data can be found once the program has been installed.

In addition, files that are made available to the program by the 'Import new FW package' function are stored here. These files serve for the firmware update of the relevant devices.

4.5.3 Internet preferences



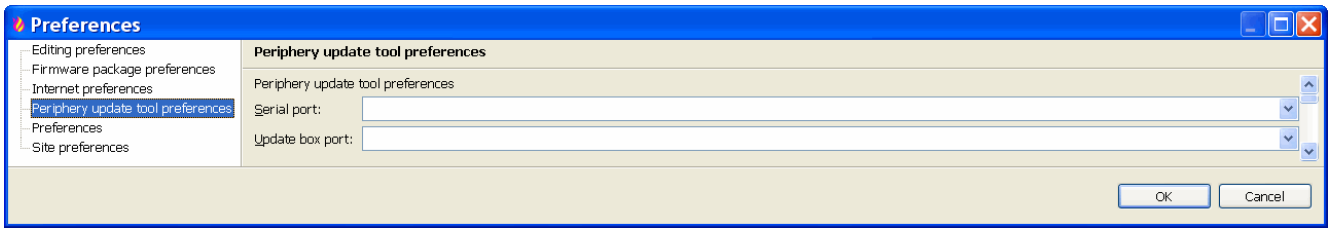
Internet preferences

The 'Internet preferences' view contains Internet access details. There are three ways in which the user can access the Internet:

- Direct: The user is granted Internet access without proxy. The box for 'Enable proxy' is not checked.
- Via proxy: The user is granted Internet access with proxy. The information on proxy host and proxy port is provided by the IT administrator. The 'Enable proxy' must contain a checkmark in order to enter it.
- Via proxy with authentication: If, in addition to the proxy, a user name and a password are requested, there must be a checkmark in the box for 'Enable proxy authentication' as well.

Please ask you IT administrator about the access method you should use.

4.5.4 Periphery update tool preferences

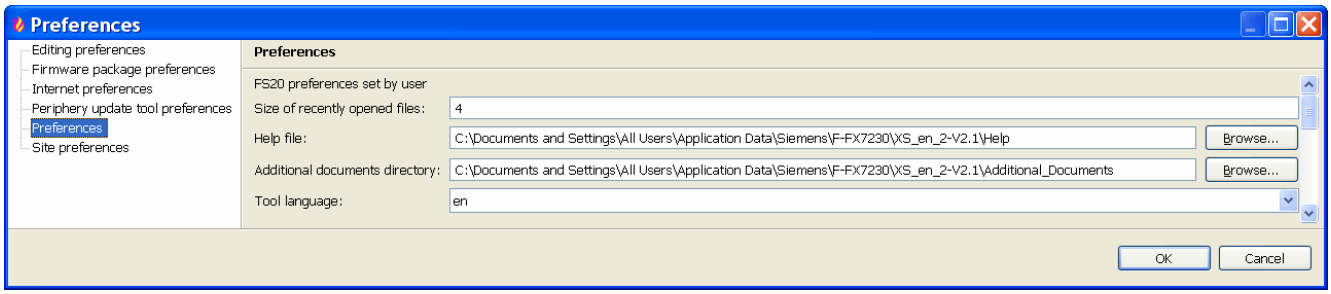


Periphery update tool preferences

In the 'Periphery update tool preferences' view, the PC outputs are defined for the following:

- serial port
- MCL-USB adapter

4.5.5 Preferences

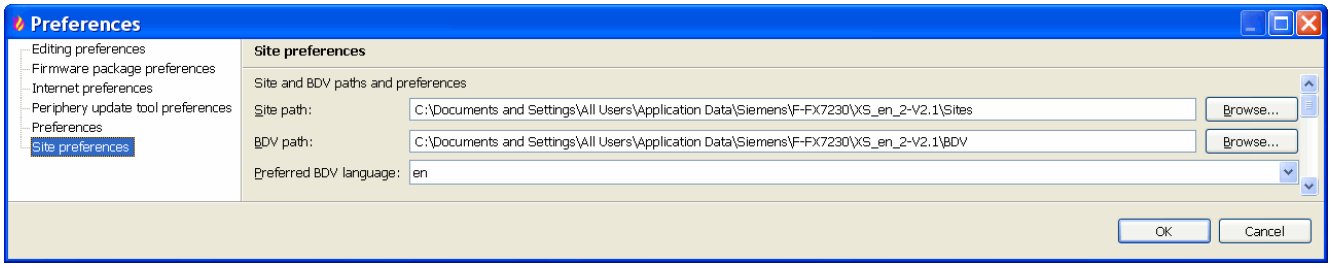


Preferences

The 'Preferences' view includes FS720 pre-settings that can be adapted by the user:

- The number of files that were recently opened and that are displayed in the 'File' menu for opening.
- The path to the 'Help' folder. This folder includes the online help files with sub-folders.
- A defined storage location where additional documents can be stored, e.g. country-specific information, application guidelines or product information.
- Selection of the tool language for menu, dialogs and Help.

4.5.6 Site preferences



Site preferences

The 'Site preferences' view includes the following pre-settings:

- The path to the 'Sites' folder, which includes all sites saved by the program.
- The path to the 'BDV' folder. This contains the BDV that was included when the program was installed, or that has been made available to the program by the 'Import new BDV' function. This folder may contain more than one BDV.
- Selection of the BDV language. This selection determines which language of the BDV is indicated, provided that several languages are included in the BDV. If the preferred language is not available in the current BDV, English is used as standard.

4.6 Task cards

The task cards show different perspectives of a 'Site' in the program window. The 'Site' is configured in the perspectives.

Every task card has a name and its own icon. When clicking a task card the perspective in account is indicated.

The task cards enable a free, logical configuration. There is no binding work sequence.

The program has the following task cards:

- 'Hardware'
  - Configuration and display of all hardware components of a 'Site'.
- 'Detection'
  - Configuration and display of detection applications.
- 'Control'
  - Configuration and indication of the control applications such as fire control, alarming control, evacuation control and extinguishing control.
- 'Operation'
  - Configuration and indication of the visibility of stations and any devices that are visible in the operation.
- 'Network'
  - Configuration and display of the network.
- 'Cerberus-Remote '
  - A station connected to the PC via Ethernet can be visualized and operated with 'Cerberus-Remote'.

4.7 Task Card Components

Each task card has the following components:

- Tree
- Table
- Detail editor
- Hyperlinks

Tree

The display and function of the tree corresponds to the tree in the Windows Explorer. Each element is shown by a symbol and text.

The elements contain configuration data.

The tree shows the structure of the site.

The root element of each tree is always the 'Site' element.

Various elements are displayed by various icons for identification.

A linked element has a link symbol on the element symbol.

Problems and special instructions are shown with red and yellow exclamation marks in the tree.

Additional information can be found in the chapter 'Problem identification and error indication'.

Table

The child elements of the highlighted element in the tree is shown in the table. If a highlighted element in the tree has no child element that the table remains empty.

The table provides a selection of the most important properties of the child elements.

Elements that are read-only but can not be edited are shaded gray.

Detail editor

The detail editor shows properties of an element or several elements highlighted within the table or the tree. If no element in the table is marked then the properties of the element marked in the tree are shown.

The detail editor includes tabs to select the most important property categories of an element.

The number of tabs shown depends on the link status of an element. In displaying an element that is linked or referenced to another element, specific properties of the linked element are shown in a new tab with the designation of the task card.

Hyperlinks

Hyperlinks are shown in the lower part of the detail editor, provided that the selected element is linked to other elements.

The view changes to the linked element of the corresponding task card by clicking a hyperlink.

4.8 Roll bars and window separating lines

Control elements in the program such as, e.g. roll bars and window separating lines, correspond to the Windows standard.

Roll bars are automatically displayed as required and each window can be zoomed in or out at a window separating line.

4.9 Expanding and reducing the tree elements

Corresponding to the functionality in the Windows Explorer, an element may be extended by a partial tree or reduced.

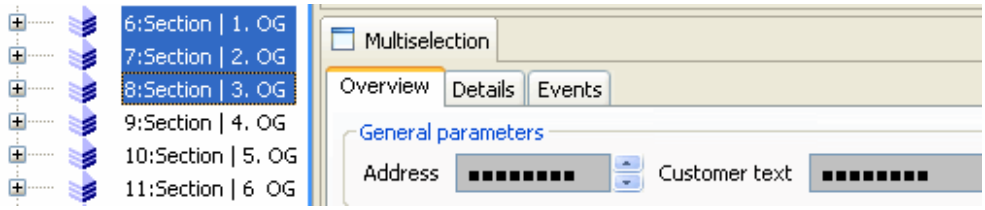
You can expand and collapse tree elements as follows:

- Click on the buttons '+' or '-' on a tree element.
- Double-click on a tree element.
- Highlight the tree element and press the right or left arrow key.
- To expand or collapse all elements of the element highlighted, highlight a tree element and press the buttons **<*>** or **</>** on the numeric keypad.

4.10 Multiselection

Multiselection allows, e.g. entry of a customer text for several elements in one procedure. Multiselection is possible in the table and in the tree view. Selecting one or more lines corresponds to the Windows standard.

If several elements are selected in the tree view, nothing is indicated in the table. The intersection of selected elements is displayed in the detail editor. If the properties of the selected elements are different then the appropriate panel in shown in the detail editor by quadrates. Following multiselection, the tab name in the detail editor is 'Multiselection'.



Multiselection

4.11 Navigating within the program window

Navigation in the program window functions according to the Windows standard.

Navigation between the task cards or the perspectives of a site depend on the program. Opening a perspective or changing from one perspective to the other is possible using the following control elements:

- Task cards
- Hyperlinks
- Shortcut

4.11.1 Navigating with task cards

Click on a task card to change to another perspective.

4.11.2 Navigating with hyperlinks

You can use hyperlinks to navigate between the task cards. An element that is contained in more than one perspective is shown by a hyperlink. Hyperlinks are shown in the lower part of the detail editor.

The perspective of the corresponding task card changes by clicking on a hyperlink.

When navigating between task cards, a selected element remains highlighted.

4.11.3 Navigating with shortcuts

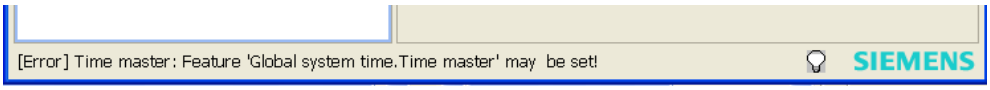
The shortcuts are listed in the following table.

Description	Shortcut
Changing between task cards	<Ctrl> + <F8> + Up or down arrow keys + <Enter>
Changing between windows of a task card	<Ctrl> + <F7>
Navigating between Parent/Child nodes	Left or right arrow keys
Navigating between nodes in the tree	Up or down arrow keys
Navigating between columns of the table	• Tab • Left or right arrow keys (apart from in editing mode; then only if the entire field is highlighted)
Navigating between lines of the table	• <Enter> or <Shift> + <Enter> • Tab in the last column • Right arrow key in the last column (apart from in editing mode; then only if the entire field is highlighted) • Up or down arrow keys (apart from in editing mode)
Navigating between the tabs in the detail editor	• <Ctrl> + <Page Up> or <Ctrl> + <Page Down> • Arrow keys if the tabs are highlighted
Navigating between the parameters of a tab in the detail editor	<Tab> or <Shift> + <Tab>

4.12 Status bar

The following information is displayed on the status bar:

- The error description of a selected element.
- A symbol for information on the connection status between the station and the PC.



Status bar

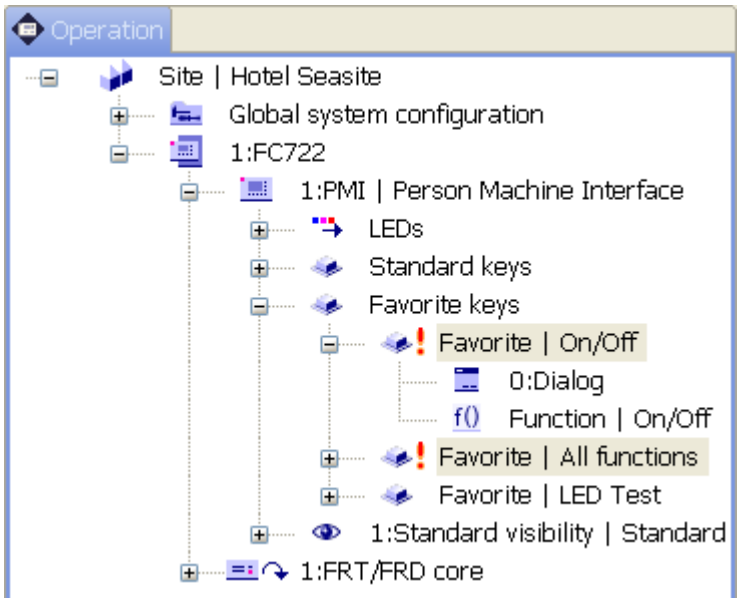
4.13 Designation of problems and displaying errors

If errors have occurred during configuration, these errors are marked in the tree view with a red exclamation mark.

A yellow exclamation mark next to an element indicates a warning, e.g. a missing link.

An error prevents the download to a station.

A site can even be stored on the PC with an error.



Display of a problem in the tree view of the 'Operation' task card

You can display more information about a problem as follows:

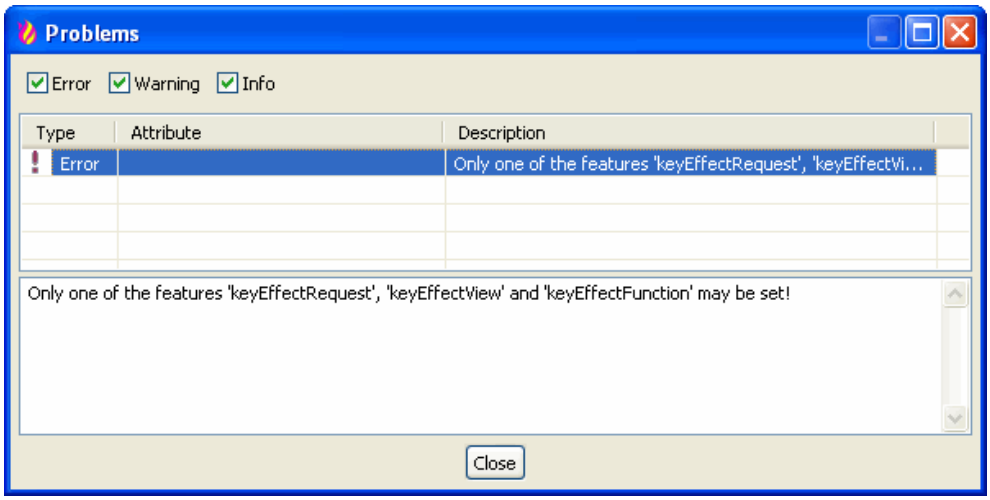
1. Right-click on an element with a red or yellow exclamation mark.
2. In the shortcut menu, select the 'Problems' menu item.

- OR -

1. Highlight the element you want.
2. Select 'View' > 'Show problems' from the menu bar.

⇨ The 'Problems' window opens.

In the 'Problems' window, an 'Error', 'Warning', or 'Information' entry concerning the problem selected is displayed.



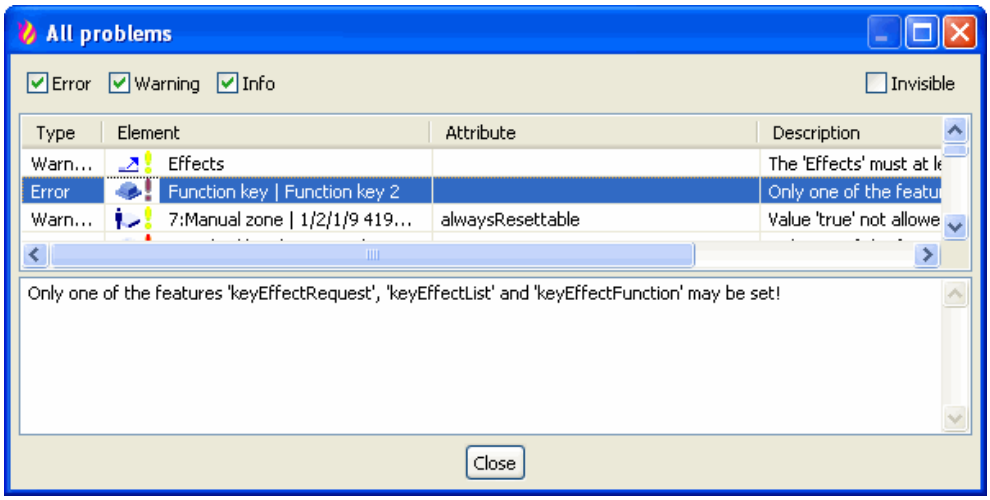
'Problems' window

You can display more information about the configuration of the entire site as follows:

- Select 'View' > 'Show all problems' from the menu bar.

⇨ The 'All problems' window opens.

The 'All problems' window displays 'Error', 'Warning', and 'Information' entries relating to the configuration of the entire site.



Window 'All problems' with the entries 'Error', 'Warning' and 'Info'

4.14 Cerberus Remote

Cerberus-Remote is software for the PC which can be used to display the Person Machine Interface of a 'Station' on the PC. For example it can be used to access the fire detection system remotely for maintenance purposes.

Depending on the operating mode, Cerberus-Remote can either be used for display purposes or for display and operation purposes.

The link between Cerberus-Remote and a 'Station' can be structured as follows:

- Local connection via any 'Station' in the fire detection system
- Connection via the Central Access Point ('CAP')
  - Local
  - Via remote access

Cerberus-Remote is an integrated part of Cerberus-Engineering-Tool but may also be installed on a PC as a stand-alone application 'FX7220'.

You will need an installed licence key (at least L1) and appropriate approval for the 'Station' in order to use Cerberus-Remote. The licence key need only be installed in the 'Station' whose PMI is to be displayed in Cerberus-Remote.

The connection to a 'Station' with a licence key is also possible via a 'Station' without a license key.

Cerberus-Remote receives the visibility which is configured on the 'Station' displayed using Cerberus-Remote.
You can use Cerberus-Remote in a fire detection installation with networked 'Stations' to gain global visibility. Just one licence key is needed for this per network if the licence key is installed in a 'Station' with global visibility.

Cerberus-Engineering-Tool is opened via the 'Cerberus-Engineering-Tool' task card in the program window.

Example for CerberusRemote in 'View and Operate' operation mode (red frame)

The button with the loudspeaker symbol (bottom right in the figure) serves for switching an activating buzzer off/on.

However, the buzzer is switched off/on only on the PC and not on the connected station.

The connection with a 'Station' is shown by the Person Machine Interface (display, LEDs, keys) transmitted.

The 'Cerberus-Remote access' operation mode is indicated by a red frame around the Person Machine Interface.

An enable granted for Cerberus-Remote is retained when a 'Station' restarted.

Cerberus-Remote has the following operation modes:

- Indicators
- Indications and operation

For both operation modes, Cerberus-Remote must be enabled on the 'Station'. In addition, a license key (minimum L1) must be installed.

Indicators

In this operation mode Cerberus-Remote indicates the same as the 'Station' connected to it, but you cannot operate the linked 'Station'.

Cerberus-Remote indicates the display with all indicated texts, all LEDs in their current state and all buttons.

Indications and operation

In this operation mode the connected 'Station' is visualised as in the Indications operation mode. Additionally, the 'Station' can be operated with Cerberus-Remote, while operation on the 'Station' itself is limited.

As operation on a 'Station' must have priority, this restriction (blocking) on the 'Station' can be cancelled at any time.

Each time an attempt is made to operate on the 'Station', a dialog is indicated with the option to abort the connection with Cerberus-Remote.

The display test is not performed on Cerberus-Remote.

5 Program administration

5.1 BDV import

A BDV can be made available in the program by clicking on the 'File' > 'Import new BDV' menu item. During this import process, the BDV is saved into the standard BDV path from a selectable location.

All imported BDVs are kept in a list which indicates the BDVs permitted for producing a new site or changing an existing site.

When you import a new BDV, you will be asked if you want to delete the old BDV. Existing sites have saved the BDV used with the site data and do not need access to the BDV in the aforementioned standard BDV path.

5.1.1 BDV name and versioning

The following information can be found in the BDV name:

- Country
- Language (and variant if required) or languages
- Meta data version
- Sales channel
- BDV version

The name of the BDV must not be changed by the user.
BDVs with names which do not correspond to the following arrangement cannot be used by the software.

Example

F-FXS2004-XS_en_2-24.4.0_01.eBDV

The arrangement for the name format is as follows:

<prefix>-<country>_<national code(s)>_<sales channel>-<metadata version>_<BDV version>[Variant].eBDV

Designation	Coding
Prefix	F-FXS2004
Country	double digit, ISO 3166-1 alpha-2 codes
Language code	double digit, ISO 639-1:2002 codes
Sales channel	single digit, numerical (1-4)
Meta data version	three levels (major, minor, bugfix), separated from each other by dots, numerical, any number of positions per level
BDV version	double digit, numerical with leading zero when applicable
Variants	optional, single digit, only CAPS
.eBDV	extension of every BDV, capital letters or lower-case letters

5.2 Firmware import

Clicking on the 'File' > 'Import new FW package' menu item enables the firmware to be provided in the Cerberus-Engineering-Tool. During this import process, the firmware is saved into the standard firmware path from a selectable location.

5.2.1 Firmware name and versioning

The following information can be found in the firmware name:

- Country
- Language (and variant if required) or languages
- Meta data version
- Sales channel
- Firmware version

The name of the firmware must not be changed by the user.
Firmware with names which do not correspond to the following arrangement cannot be used by the software.

Example

F-FXS7211-XX_xx_x-24.5.9_00.zip

The arrangement for the name format is as follows:

<prefix>-<country>_<national code(s)>_<sales channel>-<meta data version>_<Firmware version>[variant].ZIP

Designation	Coding
Prefix	F-FXS7211
Country	double digit, ISO 3166-1 alpha-2 codes
Language code	double digit, ISO 639-1:2002 codes
Sales channel	single digit, numerical (1-4)
Meta data version	three levels (major, minor, bugfix), separated from each other by dots, numerical, any number of positions per level
Firmware version	double digit, numerical with leading zero when applicable
Variants	optional, single digit, only CAPS
.ZIP	extension of every firmware, capital letters or lower-case letters

6 Operation for configuration

6.1 Creating a site

You can either configure an existing site or a new one. To do this, you first need to create a site.

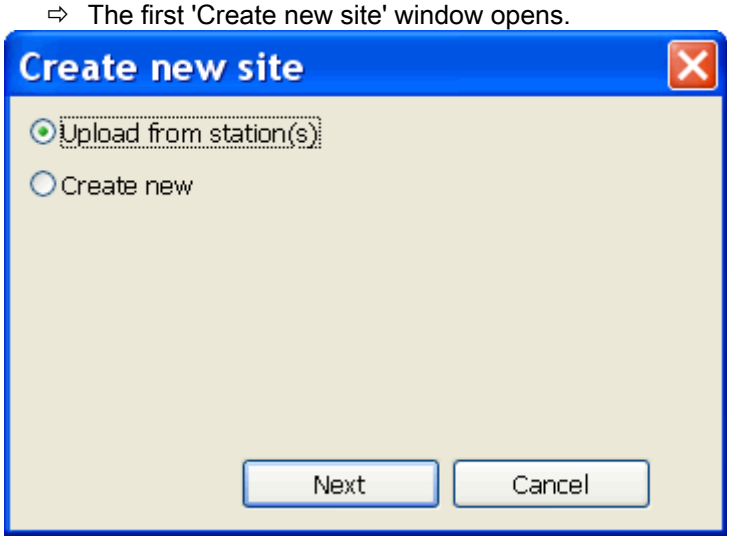
Creating existing site

▷ The station already contains configuration.

▷ The PC has a connection to the station.

1. Select 'File' > 'New site' from the menu bar or click on the  symbol in the toolbar.

   ⇨ The first 'Create new site' window opens.



Window 'Create new site'

2. Select the 'Upload from station(s)' option.
3. Click on the 'Next' button.

   ⇨ Cerberus-Engineering-Tool starts communication with the station.
   ⇨ The whole configuration is loaded into Cerberus-Engineering-Tool.

⇨ The second 'Create new site' window opens once the upload has successfully completed.

The progress of the upload is shown in the status bar.

If communication between the PC and station is interrupted, a message indicating that the upload has been aborted is displayed.

Creating new site

▷ A new site needs configuring.

1. Select 'File' > 'New site' from the menu bar or click on the  symbol in the toolbar.

   ⇨ The first 'Create new site' window opens.

2. Select the 'Create new' option.

3. Select the BDV.

4. Click on the 'Next' button.

⇨ The second 'Create new site' window opens.

When a newly created site is saved, a backup file is produced automatically and given the name of the site and the supplement '_bac.fsc'

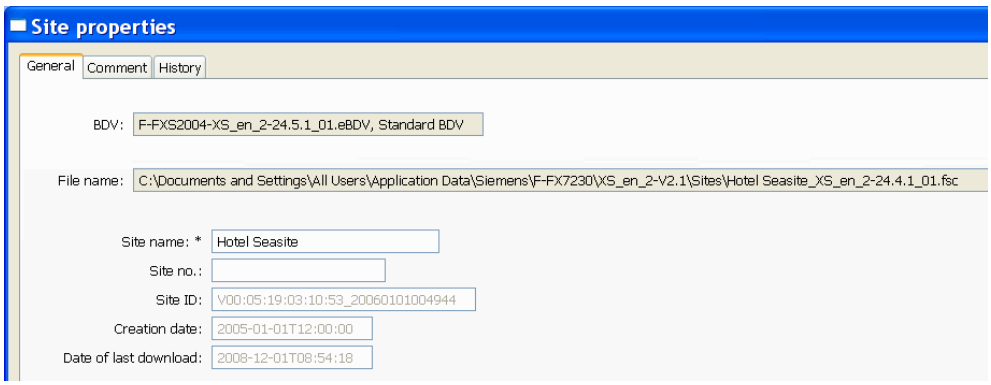
6.1.1 Editing the site properties

When a site is loaded, the site properties can be edited.

Editing properties

- Click on the 'File' > 'Site properties' menu item or use the shortcut <Ctrl> + <I>.

  ⇨ 'The 'Site properties' window opens.



'Site properties' window

The site name and assigned BDV are shown in the 'Site properties' window. Additional information can be found or entered in the 'Creator:', 'Customer:', and 'Contact:' text fields. The fields marked with '*' must be completed.

Comments can be entered on the 'Comment' tab.

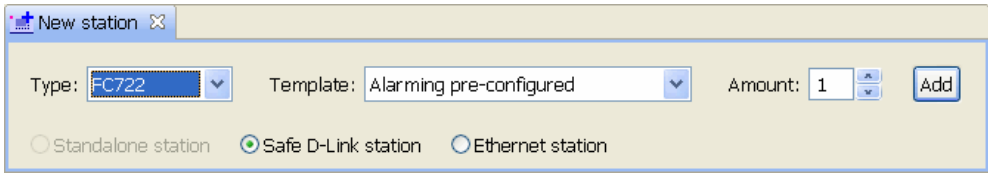
The 'History' tab contains a log file for the site.

!	*NOTICE*
	The following characters are not permitted in 'Site name' or in the path: < > / \ | : ? * " If these characters are entered, the following error message appears: 'Error: file:/V:/F-FX7230/XX_xx_Version/Sites/Test>Name.fsc or Test>Name.fsc is not a valid path or file name.'

!	*NOTICE*
	The following characters are not permitted in 'Site name' or in the path: % # If these characters are entered, Cerberus-Engineering-Tool cannot load the site.

6.2 Creating a station

When creating the first station, you can choose between 'Standalone station' and networked stations of types 'Safe D-Link station' and 'Ethernet station'. Any additional stations you create may only be networked types.



Window 'New station'

Creating station

▷ A site is created.

1. Open the 'New station' window. You can do this in the following ways:
   Select 'Edit' > 'New station' from the menu bar.
   Click on the symbol in the toolbar.
   Right-click in the tree view and select the symbol in the context menu.
   ⇨ The 'New station' window opens above the table.
2. Select a station from the 'Type:' selection list.
3. Select a template from the 'Template:' selection list.
4. Select the corresponding network for networked stations.

5. Select the number of new stations in the 'Amount:' field.
6. Click on the 'Add' button.

⇨ A new station or new stations are created.

You can close the 'New station' window using the '**X**' button on the tab in the 'New station' window or by clicking on the  symbol.

Networked stations

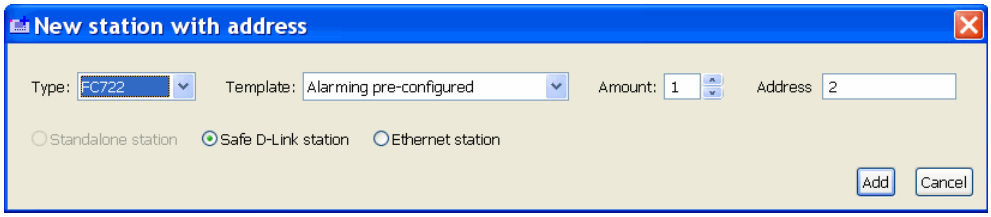
For details of how to create and configure networked stations, see [→ 187]

Creating station with individual address input

This function is normally called up when migrating from old systems if a particular address is to be assigned to a station.

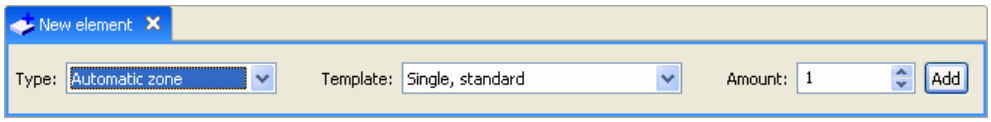
- Select 'Edit' > 'New station with address' from the menu bar.

⇨ The 'New station with address' window opens.



Window 'New Station with address'

6.3 Creating an element



Window 'New element'

Create element

▷ A station is created.

▷ An element is selected for which a sub-element can also be displayed.

▷ The site node is not selected.

1. Open the 'New element' window. You can do this in the following ways:
   Select 'Edit' > 'New element' from the menu bar.
   Click on the symbol in the toolbar.
   Right-click in the tree view and select 'New element' in the context menu.

   ⇨ The 'New element' window opens above the table.
2. Select an element from the 'Type:' selection list.
3. Select a template from the 'Template:' selection list.
4. Select the number of new elements in the 'Amount:' field.
5. Click on the 'Add' button.

⇨ A new element or new elements are created.

Close the 'New element' window using the '**X**' on the tab in the window, or by clicking on the symbol again.

Creating an element in the table

▷ A station is created.

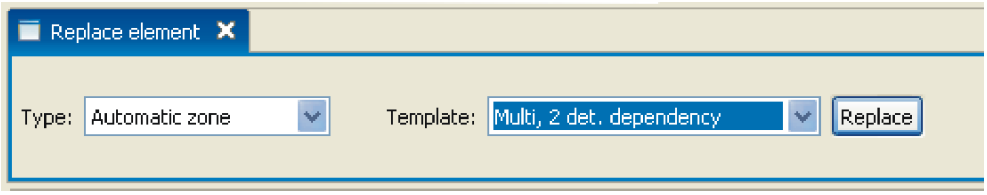
▷ An element is selected for which a sub-element can also be displayed.

1. Double-click on the 'Append ...' field in the table.
2. Select the element type with the corresponding template from the selection list.

⇨ A new element is created.

6.4 Replacing an element

Replacing an element means assigning another template of the same type to the element.



Window 'Replace element'

Replacing element

1. Highlight the element to be replaced in the tree view.
2. Select 'Edit' > 'Replace element' from the menu bar.
   ⇨ The 'Replace element' window opens above the table.
3. Select another template for the type indicated and click on the 'Replace' button.

⇨ The template is replaced accordingly.

6.5 Deleting an element

An element can be deleted in the tree or in the table. The subtree of the element is also deleted when an element is deleted. If the element that is to be deleted is referenced in other elements, for example in a link to 'Causes' in a control, a message appears indicating that the references will be deleted at the same time. If a linked logical channel is deleted then the physical channel is no longer assigned.

You can delete an element as follows:

- Using the button  in the toolbar
- Using 'Edit' > 'Delete' in the menu bar
- Via the context menu
- With <Delete>

6.6 Editing an element

Elements can be edited in the table or detail editor. Editing in the tree is not possible.

The same parameters of various elements can be edited and changed in one process in the detail editor. To do this, the corresponding lines of the element must be highlighted in the table, or several elements in the tree Changing the parameter in the detail editor then changes these parameters in all highlighted elements.

Editing elements

- Highlight an element in the tree or table

⇨ The details of the highlighted element are indicated in the detail editor.

⇨ Editable properties can be changed.

6.7 Copying properties in the table

In the table, you can copy editable properties of an element, such as customer text, into any number of adjacent cells of other elements.

Copying property

1. Click the cell with the property that you want to copy.
   ⇨ The cell is marked by a frame.
2. Guide the mouse pointer to the bottom right corner of the highlighted cell.
   ⇨ The mouse pointer changes to a white cross.
3. With the left mouse button pressed, drag the white cross over the cells in the same column into which you want to copy the property.
   ⇨ Highlighted cells have a gray background.
4. Release the pressed left mouse button.

⇨ The copying process is complete.

With the multiselection feature you can also copy properties for several elements in one go.

6.8 Predictive text input

When writing customer texts and counter-measures texts in the detail editor, as in the table, texts that have already been used are displayed in a list when the first letter or a matching sequence of characters is entered. You can navigate through the list by scrolling, using the mouse, or using the Up/Down arrow keys and <Enter>. The list is updated continually as text is entered.

For settings see [→ 22]

6.9 Copying, cutting and pasting an element

The functions for copying, cutting and pasting elements correspond to the Windows standard and can be used in the tree and the table as well as between the tree and the table.

When copying and cutting, the entire subtree of an element, if it exists, is placed on the clipboard. Copied and cut elements can be pasted in one after another at various positions.

When pasting, the customer text and other data are transferred. Attributes, for example the element's address, are updated depending on the new position.

Conditions

- Elements can only be copied/cut if they can be created separately.
- Elements that are generated automatically when creating parent elements can not be copied/cut separately.
- Cross links and reference links are not copied.
- Copying/cutting is only possible within a 'Site'.

Copying element

You can copy an element as follows:

- Using 'Edit' > 'Copy' in the menu bar
- Using the button  from the toolbar
- Using the shortcut <Ctrl> + <C>

Pasting copied element with subtree

You can paste a copied element with subtree as follows:

- Using 'Edit' > 'Paste' in the menu bar
- Using the button  from the toolbar
- Using the shortcut <Ctrl> + <V>

Pasting copied element without subtree

You can paste a copied element without subtree as follows:

- Using 'Edit' > 'Paste' in the menu bar
- Using the button  from the toolbar

Cutting element

You can cut an element as follows:

- Using 'Edit' > 'Cut' in the menu bar
- Using the button  from the toolbar
- Using the shortcut <Ctrl> + <X>

Pasting cut element

You can only paste a cut element with subtree:

You can paste a cut element as follows:

- Using 'Edit' > 'Paste' in the menu bar
- Using the button  from the toolbar
- Using the shortcut <Ctrl> + <V>

6.10 Moving an element

You can move an element using the standard Windows function 'Drag and drop' or with 'Cut' and 'Paste'.

When dragging an element, the mouse pointer shows whether the element can be placed at the respective position or on the respective element. An element with child elements cannot be dragged and dropped without its child elements. If a subtree is moved then various attributes of the parent element are automatically updated, such as the address of the element in the zone.

If you press the 'Ctrl' key when dragging, the mouse pointer indicates a '+' and copies the element when dropping.

Handling links when moving

Moving elements inside a station:

- The links to the hardware are also moved.
- The links to the control are also moved.

Moving elements between different stations:

- The links to the hardware are deleted.
- The links to the control and detection elements are also moved.

6.11 Re-addressing elements

Elements in the tree view can be provided with another address, e.g. to close gaps in the sequence or to paste elements into particular positions. This application is mainly of use in the 'Detection' task card, at 'Zone' level.

The addresses are re-addressed within the same level, e.g., 'Zone', over the entire 'Site'.

Closing gaps

Gaps are produced in the address sequence when you delete, cut/paste or move elements or when re-addressing elements throughout stations.

Procedure:

1. Highlight the element after the gap in the tree view.
2. Click on the 'Edit' > 'Change element address: $(NUMBER)' menu item.
   ⇨ The 'Move address confirmation' window opens.
3. Confirm the message by clicking on the 'Yes' button.

⇨ The address of the element selected and all elements of the same level with higher addresses are decreased by one counter across the system to close the gap.

Inserting element

An element, e.g. another zone, can be inserted into the address sequence at a particular place.

Procedure:

1. Highlight the element before which you want to insert an element in the tree view.
2. Click on the 'Edit' > 'Change element address: $(NUMBER)' menu item.
   ⇨ The 'Move address confirmation' window opens.
3. Confirm the message by clicking on the 'Yes' button.
   ⇨ The address of the element selected and all elements of the same level with higher addresses are increased by one counter across the system to produce a gap in the address sequence.
4. Highlight the parent element and create a new element using the 'New element' function.
5. In the detail editor, change the address to the number corresponding to the gap.

⇨ The new element is moved to the position of the gap.

The two functions can only be used when the address is editable.
When the address of an element in the site is unambiguous, the elements of other parent elements are also adapted. A warning message appears and the function can be cancelled.

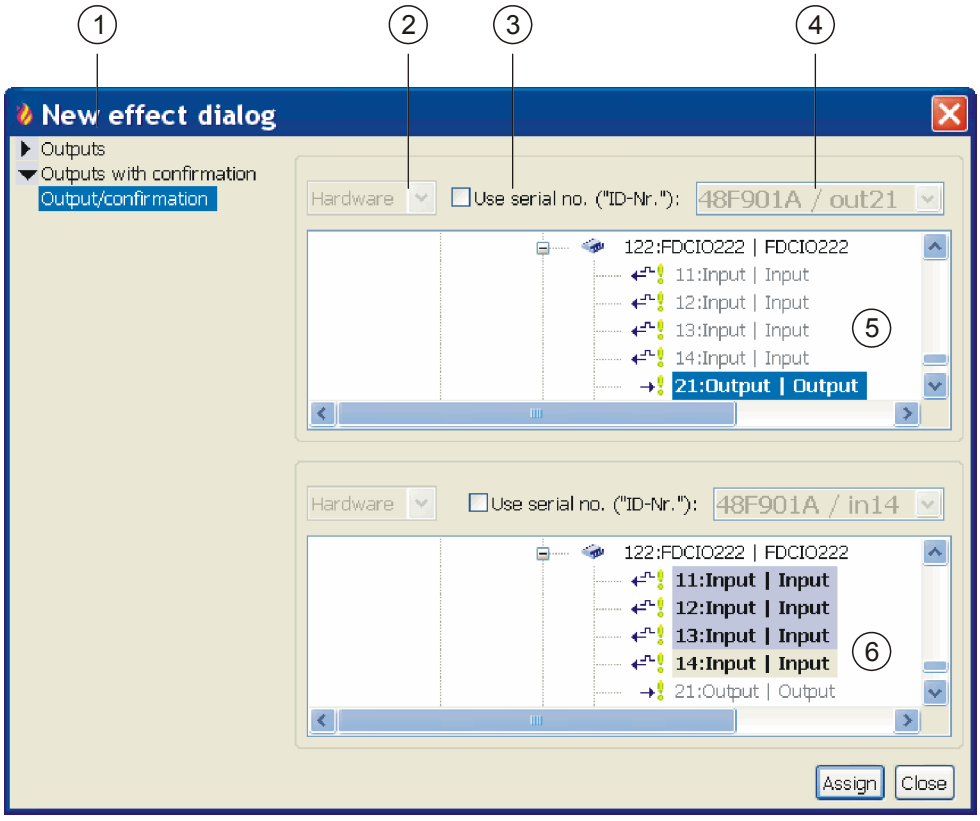
6.12 Linking elements

Elements from the same task card as well as those from different task cards can be linked using the Assign function. When this is done, a physical channel is linked with a non-linked logical channel.

The 'Assign dialog' window is opened using the 'Commissioning' > 'Assign' menu item, the shortcut menu, the button in the toolbar, or <Ctrl> + <L>.

The opened 'Assign dialog' window can remain open when changing perspectives.

The Assign function cannot be called up in the 'Hardware' task card.



'Assign Dialog' window, example 'Outputs with confirmation'

1 List with linkable event categories, inputs and outputs
2 Dropdown list field to select the task card
3 Option field to activate search by ID no. (4)

4 Dropdown list field to select the element to be linked by search by ID no.

5 Tree view of the linkable elements:
- Light gray text: the path leads to an element that cannot be linked
- Bold text: the path leads to an element that can be linked
- Bold text, grayed out: element that can be linked
- Inverted text, blue: highlighted element

6 Tree view of linkable elements (can only be seen with an output with confirmation input)

Linking elements

1. Highlight the element to be linked in the tree view of the task card.
2. Open the 'Assign dialog' window.
3. Select the category from the list (1).
4. Select the task card in the dropdown list field (2).
5. Search for the element to be linked using the ID no. (4) or by opening the path in the tree view (5).
6. Highlight the element in account.
7. Click on the 'Assign' button.

⇨ Elements are linked.

6.13 Finding

This function allows you to perform a different kind of search for:

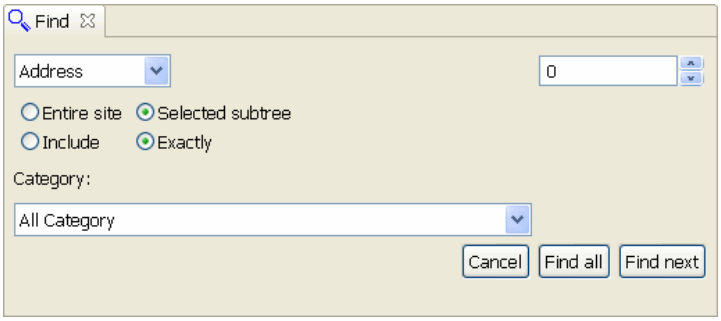
- 'Element ID'
- 'Address'
- 'Customer text'
- 'Problem' (labeling: exclamation mark, red = error, yellow = warning)
- 'Not linked': one possible reason for a yellow exclamation mark or Element ID. The search can be restricted to 'Sensor' and 'Sounder'.

The search criteria available depend on the selected task card.

The 'Find' function is limited to the selected task card.

Clicking on the 'View' > 'Find' menu item opens the 'Find' window via the tree view.

The window is closed with the button 'X' in the tab. The window can also be opened and closed with the symbol  in the toolbar.



'Find' window with search criteria 'Address'

Options:

- 'Entire site': The search is undertaken throughout the entire 'Site'.
- 'Selected subtree': The search is undertaken in the subtree highlighted.
- 'Include': The search function searches for all values which include the value entered in the top right field.
- 'Exactly': The search function searches for exactly the value matching the one entered in the top right field.

'Category:'

In this list field, the search can be limited to one element category, e.g., to 'Area', 'Section', or 'Zone' in the 'Detection' task card. All element categories are always listed, regardless of the task card selected. If an element category is highlighted that is not present in the task card selected, the search will be fruitless.

Search process:

1. Select a search criterion and enter the corresponding search value in the top right field.
2. Select the options and category.
3. Click a button.

⇨ The 'Find all' button searches for and highlights all elements which correspond to the search criterion.

⇨ The 'Find next' button jumps from one hit to the next hit.

⇨ <F3> corresponds to the 'Find next' function.

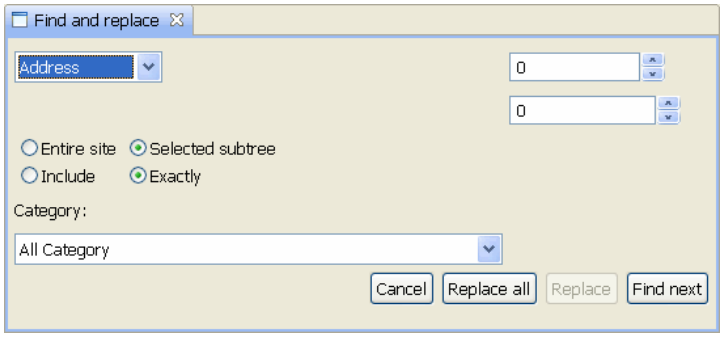
⇨ The 'Cancel' button stops the current search and removes the highlighting on elements found following a search.

6.14 Finding and replacing

This function allows you to perform a different kind of search than with the 'Find' function. See [→ 48]

Clicking on the 'View' > 'Find and replace' menu item opens the 'Find and replace' window via the tree view.

The window is closed with the button 'X' in the tab.



'Find and replace' window with search criteria 'Address'

Search process:

1. Select a search criterion and enter the corresponding values. The search values can be seen in the top right and the replacement values under them.
2. Select the options and category.
3. Click a button.

- The 'Find next' button jumps from one hit to the next hit.
  - <F3> corresponds to the 'Find next' function.
- The 'Replace' button replaces the search value of the 'Find next' hit with the replacement value.
- The 'Replace all' button replaces the search value of all the hits found with the replacement value.
- The 'Cancel' button stops the current search and removes the highlighting on elements found following a search.

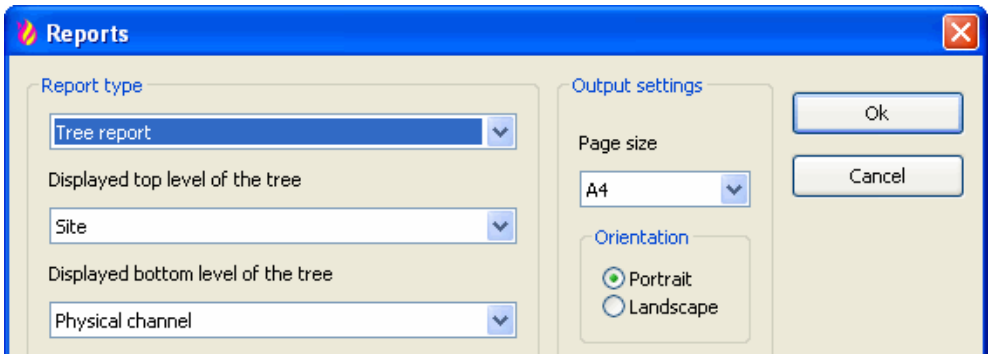
6.15 Reports

Clicking on the 'File' > 'Reports' menu item opens the 'Reports' window. This makes it possible to generate and print different types of reports on the application functionalities. The reports are generated in accordance with the task card that is active - 'Hardware', 'Detection', 'Control', 'Operation', 'Network'. The following identifications are supported:

- 'Tree report'
- 'Node report'
- 'Device report'
- 'Diagnostics report'

The reports are output in PDF file format. Each report has various output options the user may select according to his requirements. The paper format may be selected as well. For the output the user must select a path and enter a file name. The report can be printed with the corresponding program.

Tree report



Tree report

In the Tree report, the task card elements displayed in the tree view are listed in tabular format. The elements include the same properties as in the tree view: address, symbol, element type and customer text.

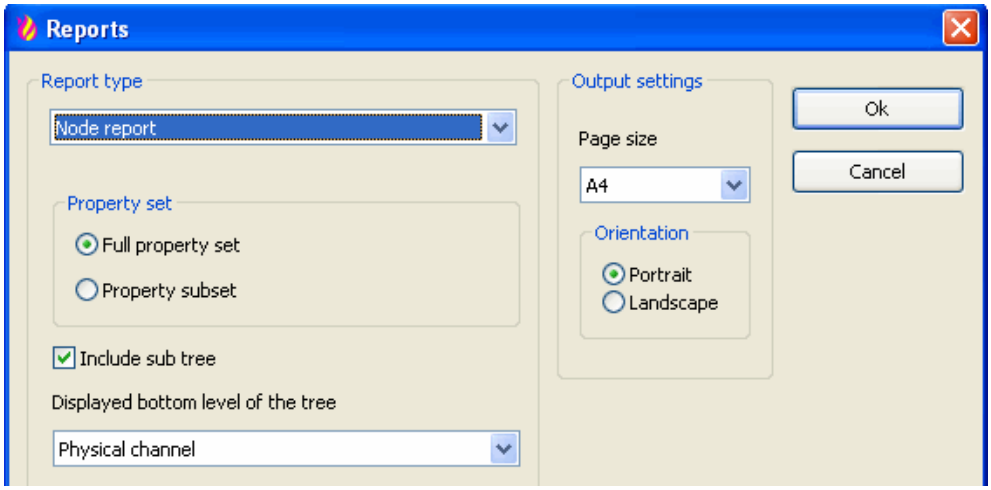
The very top and very bottom levels in tree view that are to be output can be selected.

The properties of the elements are listed in the table columns. The following table shows which properties are output in each task card.

Features	**Task card**				
	Hardware	Detection	Control	Operation	Network
'Use serial no. ("ID-Nr."):'	X	X			
'Customer text'				X	
'S-LINE parameter set 'manned''	X	X			
'S-LINE parameter set 'unmanned''	X	X			
'C-LINE parameter set'	X	X			
'Template ID'		X			
'Hyperlink'	X	X	X		

Properties output

Node report



Node report

In the Node report, the task card element selected in the tree view is listed in tabular format.

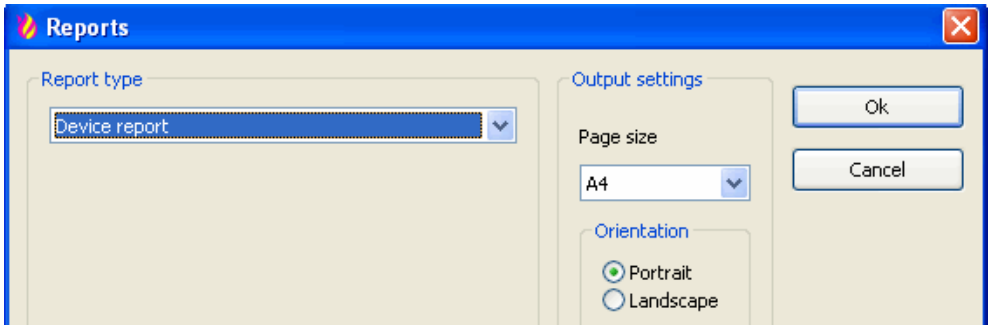
The following selection is available:

- 'Full property set': All visible properties of the highlighted element.
- 'Property subset': All individually specified properties.

You can also determine whether the highlighted elements are output alone or the subtree is output too.

- 'Include sub tree' highlighted: the subtree including properties is output, the very bottom level to be output can be selected.
- 'Include sub tree' not highlighted: only the properties of the element highlighted in the tree view are output.

Device report



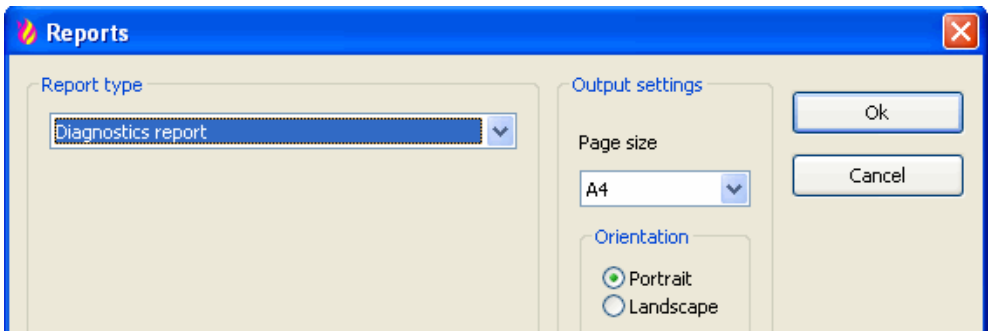
Device report

Regardless of which task card is selected, the Device report lists the number of elements available in the hardware tree, detection tree, and control tree. On the one hand, the elements are listed as in the tree view, with the number of elements in the parent element. On the other hand, each element type is listed with the total number of elements.

The output elements are:

- Detection tree: Elements 'Area', 'Section', and 'Zone'.
- Control tree: Elements 'Control group' and 'Control'.
- Hardware tree: Element 'Site'

Diagnostics report



Diagnostics report

The Diagnostics report lists the Site info properties and the software and firmware versions of the hardware in the entire site. Only the properties existing in the elements are listed here, i.e. only some of the following possible properties:

- Hardware version
- Software version
- Firmware version
- Firmware revision
- Product version
- Series number
- Hardware name
- Hardware type
- Ethernet MAC address

6.16 XML export

The Site configuration can be exported into an XML file to create country-specific reports. This file can be edited with any XMl-compatible program, so that reports with different criteria and representation forms can be output.

Exporting XML file

1. Open a Site using the 'File' > 'New site' or 'Open' menu item.
2. Click on the 'File' > 'Site export (XML)' menu item.
   ⇨ The 'Save site export (XML) as ...' window opens.
3. Select the path, enter a file name, and click on the 'Save' button.

6.17 SiB-X export

With the SIB-X export the definitions of the configuration data can be exported in SIB-X format (a special XML file). SIB-X is the exchange format for configuration data between various products of Siemens Building Technologies, e.g. to the Management System MM8000.

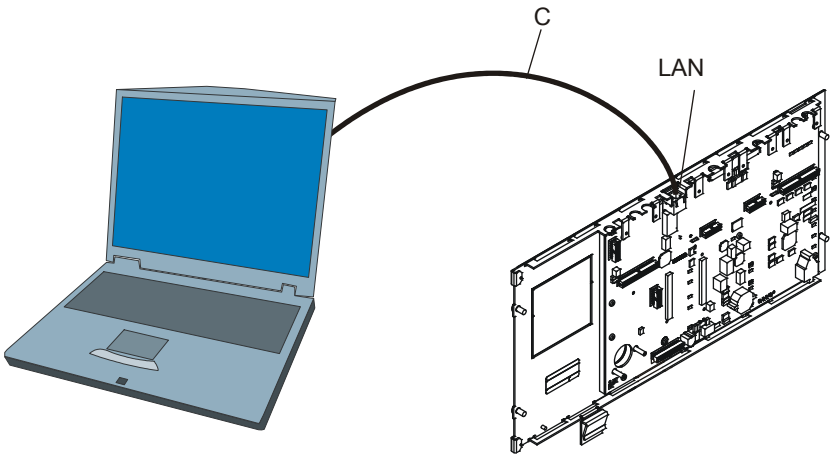
Exporting configuration data

1. Open a site using the 'File' > 'New site' or 'Open' menu item.
2. Click on the 'File' > 'SiB-X export' menu item.
   ⇨ The 'Save SIB-X export as ...' window opens.
3. Select the path, enter a file name, and click on the 'Save' button.

7 Operation for communicating with station

7.1 Connect the PC to the station

For most commissioning, maintenance and repair work a PC with installed Cerberus-Engineering-Tool is required. The following figure shows how the PC is connected to the station.



PC and rear panel of operator unit

LAN	Ethernet connection	C	Cable, type CAT 5 or CAT 7, crossover, max. 100 m

7.2 Disconnecting link between Cerberus Engineering Tool and station

In order to remove the connection between the Cerberus-Engineering-Tool and the control panel in a defined way, the Cerberus-Engineering-Tool must be used to remove the LAN connection first, via 'Commissioning' > 'Disconnect' in the menu bar. Only then can the cable be removed.

7.3 Initializing the station

The 'Commissioning' > 'Initialize station' menu item can be used to transfer the configuration of the station selected in Cerberus-Engineering-Tool to the connected station. This incorporates the station in the network. The pre-configuration and the BDV are loaded into the station when initializing. Doing this overwrites the site ID.

A detailed description of initialization can be found in the document A6V10210416, commissioning.

7.4 Downloading configuration of a 'Site'

You can use the 'Download site configuration' function to load the configuration of one site from the Cerberus-Engineering-Tool on the PC into the station. In networked stations, the entire site is downloaded via a station.

▷ The site is opened in the Cerberus-Engineering-Tool.

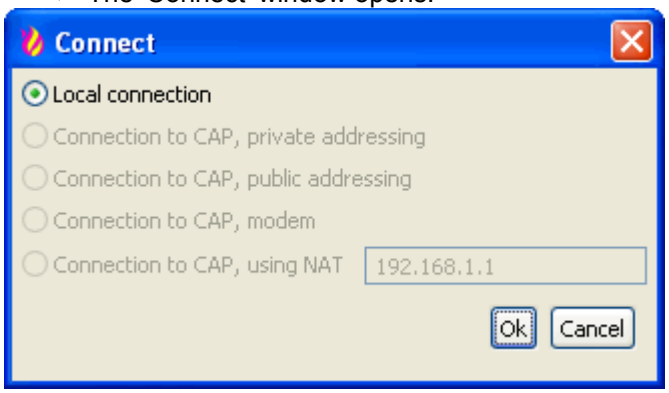
▷ The PC is linked to the station via an Ethernet cable.

▷ Networked stations must be initialized.

▷ The station and Cerberus-Engineering-Tool must have the same site ID and belong to the same organizational unit.

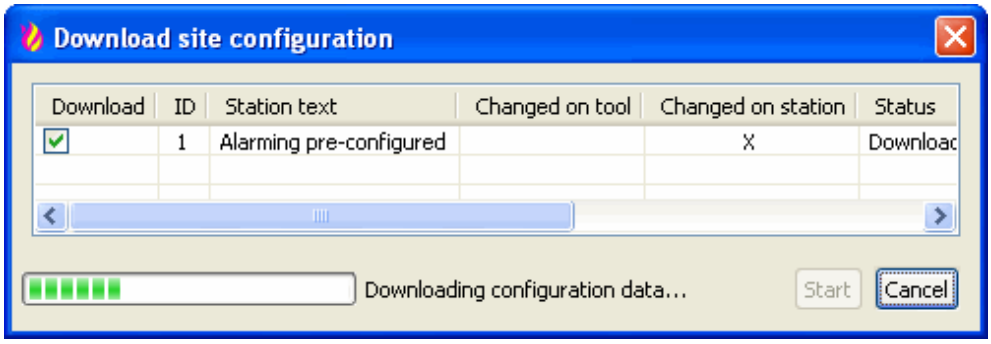
1. In the 'Commissioning' menu, select the 'Download site configuration' menu item.

   ⇨ The 'Connect' window opens.



2. Select the connection setting and confirm with 'OK'.

   ⇨ The selection window opens.
   ⇨ Establishment of a connection is started and indicated.



3. Select the stations whose configuration you want to download and click on the 'Start' button.

⇨ The download is carried out.

⇨ The status of the transfer is shown in the status bar.

A detailed description of the download can be found in the document A6V10210416, commissioning.

7.5 Uploading configuration of a 'Site'

The 'Upload site configuration' function can be used to upload the entire 'Site' configuration from a station into the Cerberus-Engineering-Tool on the PC.

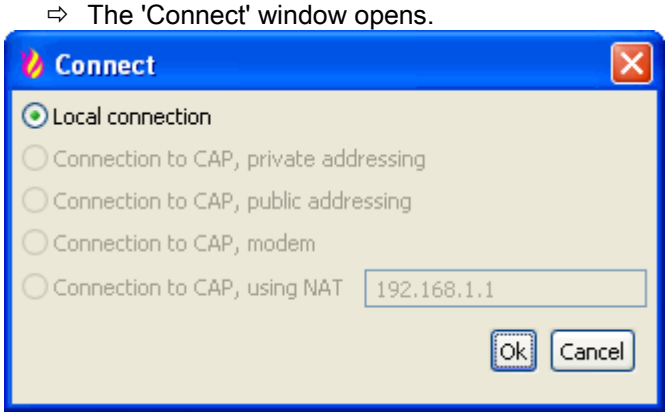
▷ The 'Site' is opened in Cerberus-Engineering-Tool.

▷ The PC is linked to the station via an Ethernet cable.

▷ Station and Cerberus-Engineering-Tool must have the same 'Site' ID and belong to the same organizational unit.

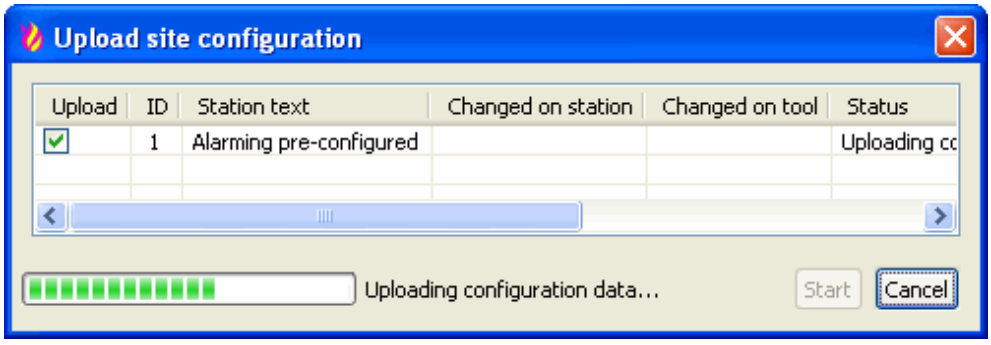
1. In the 'Commissioning' menu, select the 'Upload site configuration' menu item.

   ⇨ The 'Connect' window opens.



2. Select the connection setting and confirm with 'OK'.

   ⇨ The selection window opens.
   ⇨ Establishment of a connection is started and indicated.



3. Select the stations whose configuration you want to upload and click on the 'Start' button.

⇨ The upload is carried out.

⇨ The status of the transfer is shown in the status bar.

A detailed description of the upload can be found in the document A6V10210416, commissioning.

7.6 Uploading event memory

The 'Upload site event memory' function can be used to upload the event memories of all the site's stations into the Cerberus-Engineering-Tool on the PC, while working on any station.

▷ A valid 'Site' is loaded.

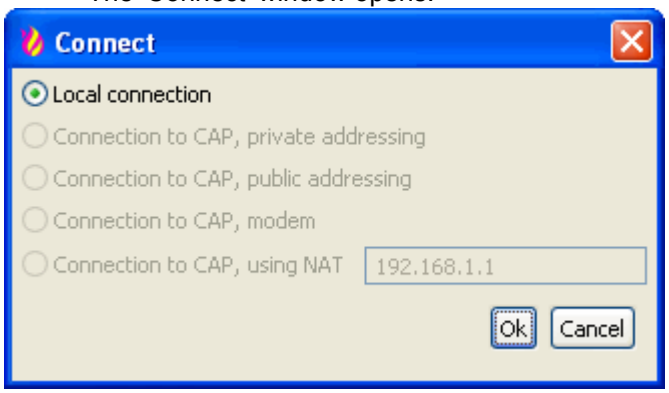
▷ All stations have the same BDV version and the same global configuration so that site-wide communication is supported.

▷ Station and Cerberus-Engineering-Tool must belong to the same organizational unit.

▷ The PC is linked to a station of the site via an Ethernet cable.

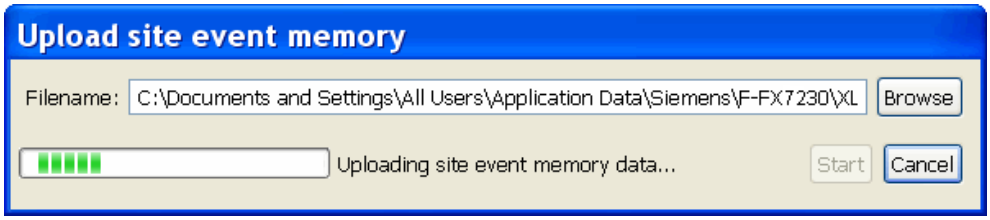
1. In the 'Commissioning' menu, select the 'Upload site event memory' menu item.

   ⇨ The 'Connect' window opens.



2. Select the connection setting and confirm with 'OK'.

   ⇨ In the following dialogue, the system proposes a file name for saving the data.



3. Leave this or change the file name and click on the 'Start' button.

⇨ The upload is carried out.

⇨ The status of the transfer is shown in the status bar.

⇨ The data is saved in the specified file.

7.7 Uploading 'Site' log

To receive support in diagnosing the site, the 'Upload site log files' function can be used to upload log files to the Cerberus-Engineering-Tool on the PC from selectable stations. The log files are saved in a compressed archive determined by the user. This archive contains one folder for each station.

Example:

LogFilesArchiveExample.zip
- \Station1\
  - Syslog
  - Syslog.1
  - Syslog.2
- \Station2\
  - Syslog
  - Syslog.1

▷ A valid 'Site' is loaded.

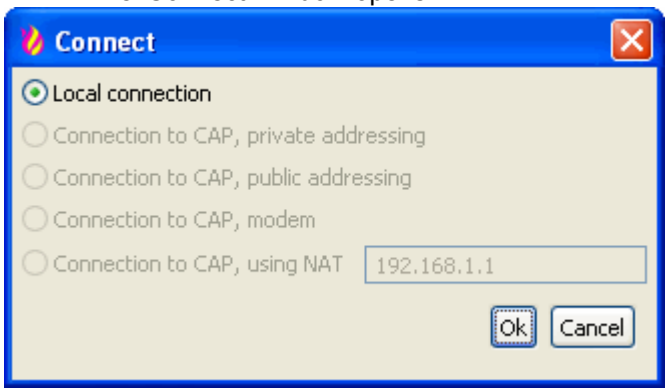
▷ All stations have the same BDV version and the same global configuration so that site-wide communication is supported.

▷ Station and Cerberus-Engineering-Tool must belong to the same organizational unit.

▷ The PC is linked to a station of the site via an Ethernet cable.

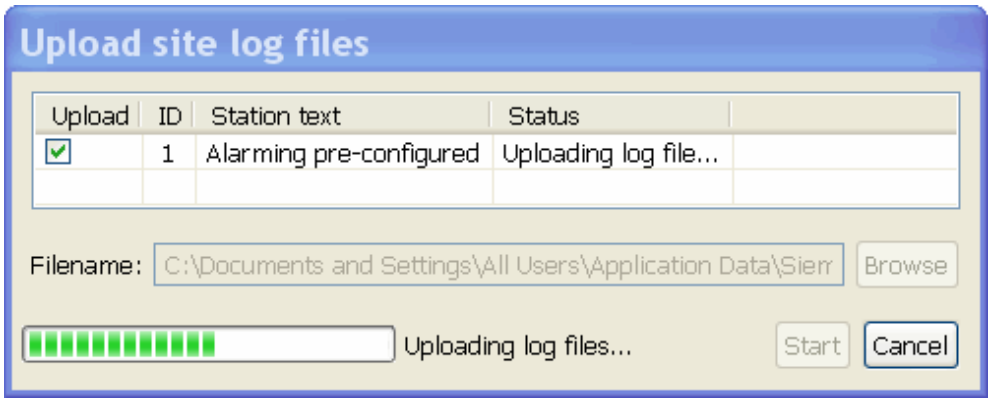
1. In the 'Commissioning' menu, select the 'Upload site log files' menu item.

   ⇨ The 'Connect' window opens.



2. Select the connection setting and confirm with 'OK'.

   ⇨ The selection window opens.
   ⇨ Establishment of a connection is started and indicated.



3. Select the stations whose log files you want to upload and click on the 'Start' button.

⇨ The upload is carried out.

⇨ The status of the transfer is shown in the status bar.

⇨ The data is saved in the specified file.

7.8 Firmware update for station

A firmware update on the station can be carried out in two ways:

- 'FW update main CPU' enables the main processor to be updated.
- 'FW update additional CPUs' enables additional CPUs, such as the periphery boards, to be updated.

A detailed description of the firmware update can be found in the document A6V10210416, commissioning.

7.8.1 'Site' conversion

The Cerberus Engineering Tool distinguishes between normal BDV mode and expert BDV mode.

Conversions from normal BDV mode to expert BDV mode are also possible but not the other way round.

During a firmware update, the existing site is converted on the basis of the new base data variant (BDV). The conversion is done automatically or manually. Manual conversion is called up in the Cerberus-Engineering-Tool via the 'Edit' > 'Convert site configuration' menu item.

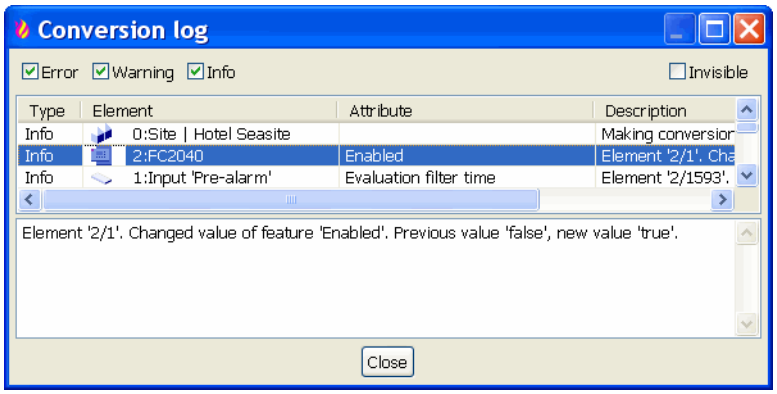
Properties of the conversion

- Only the configuration data is converted.
- The process data of the station is not converted. The default values of the new software are transferred and the station recalculates the process data.
- The critical conversions are logged for the complete site. The logs can be viewed in the 'Conversion log' window or printed from the log file.

The site is converted as part of a firmware update. More information can be found in document A6V10210416, commissioning.

7.8.2 Conversion log

The log of the site conversion from an older BDV to a new BDV is shown in the 'Conversion log' window along with the 'Error', 'Warning', and 'Info' entries. With the aid of the log, errors in the converted configuration can be found and corrected.



'Converter log' window with the 'Error', 'Warning', and 'Info' entries

The site is converted as part of a firmware update. More information can be found in document A6V10210416, commissioning.

7.9 Firmware update of peripherals

The following functions are available:

- 'FW update standard peripheral device' enables the floor repeater terminal FT2010, the floor repeater display FT2011, and the mimic display driver FT2001-A1 to be updated.
- 'FW update FDUZ221 update box' enables the MCL-USB adapter to be updated.
- 'FW update FDUL221 line tester' enables the line tester to be updated.
- 'FW update serial FDUL221 line tester' enables the serial line tester to be updated.

The MCL-USB adapter must be used for the connection between the periphery device and the PC.

A detailed description of the firmware update can be found in the document A6V10210416, commissioning.

7.10 Connecting Cerberus Remote

Cerberus-Remote can only ever be connected with one station at a time. The connection can be established locally or remote via the 'Central Access Point' (CAP). For this purpose, there must be a license key (at least L1 or L2) installed in the station that is to be displayed with Cerberus-Remote.

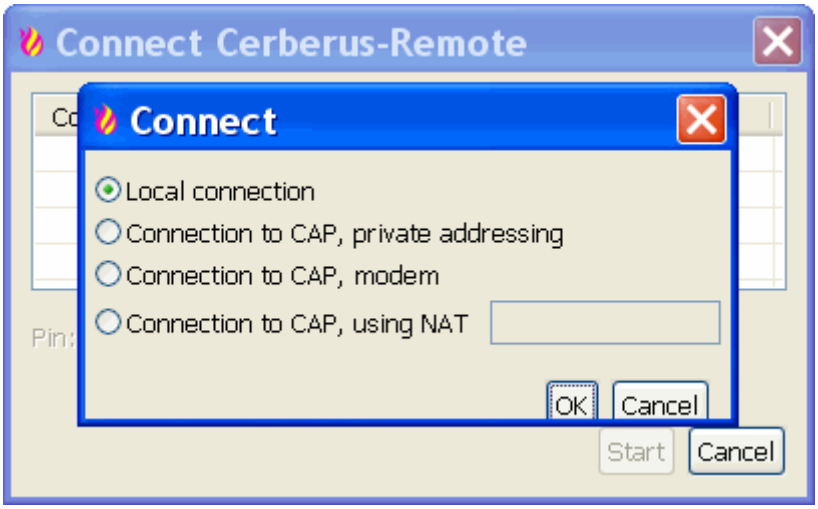
Cerberus-Remote receives the visibility which is configured on the 'Station' displayed using Cerberus-Remote.

You can use Cerberus-Remote in a fire detection installation with networked 'Stations' to gain global visibility. Just one licence key is needed for this per network if the licence key is installed in a 'Station' with global visibility.

The possible 'Cerberus-Remote viewer' or 'Cerberus-Remote access' operation modes must be enabled before connecting to the station. The possible operation modes can also be permanently enabled in the configuration with Cerberus-Engineering-Tool.

Establishing connection

1. Click on the 'Cerberus-Remote' task card.
   ⇨ The Person Machine Interface of a station is shown.
2. In the menu bar, click on the 'Cerberus-Remote' menu item.
   ⇨ The submenu 'Connect' (and 'Disconnect') is indicated.
3. Select 'Connect'.
   ⇨ A window showing the selection of connection type is indicated.



4. Select the required type of connection and confirm with 'OK'.
   ⇨ A window with the list of all stations of the site is indicated.
5. Mark the corresponding station.
6. Enter your PIN.
7. Click the 'Start' button.

⇨ The connection is established.

The connection with a 'Station' is shown by the Person Machine Interface (display, LEDs, keys) transmitted.
The 'Cerberus-Remote access' operation mode is indicated by a red frame around the Person Machine Interface.
An enable granted for Cerberus-Remote is retained when a 'Station' restarted.

See also

Establishing connection between PC and C-WEB [→ 201]

8 Configuration

A fire detection system is comprised of the following components: control panels, detectors, operating terminals, control elements, etc. To enable the components to communicate with each other, and to ensure that the events and the functions of the system are correctly detected/reported and controlled, the system must be configured.

For the configuration, the installation is divided into a physical and a logical structure. These structures are represented in the task cards in the Cerberus-Engineering-Tool. The following table shows an overview.

Structures	Trees	Task cards
Physical structure	Hardware tree	'Hardware'
Logical structure	Detection tree Control tree Operation tree Network tree	'Detection' 'Control' 'Operation' 'Network'

The physical structure is read in by the station. The logical structure can be created either manually during the pre-configuration or automatically on the station by automatic configuration. Some parts of the logical structure are already pre-configured in the station template.

Below you will find a rough overview of the possible configurations:

- Configuring the components of the station
- Creating detector zones
- Setting the detector parameter sets
- Multi-detector dependency
- Alarm organization
- Controls (alarming, fire, evacuation)
- Networking control panels and operating panels (stations)
- Visibilities of events and functions
- Service intervention
- Customer texts
- Intervention texts

There are two basic procedures used in configuring the fire detection system:

- With pre-configuration
- Without pre-configuration

With pre-configuration

- In Cerberus-Engineering-Tool, the system is primarily configured in its logical structure (preconfigured) based on the planning documents, the layout plan, etc.
- During the later commissioning, the pre-configuration must be loaded into the station.
- After downloading, the station is re-started and the modules and the C-NET devices/periphery of the station are read in. The resulting physical structure is loaded into the Cerberus-Engineering-Tool together with the logical structure.
- The logical and physical structure are linked in Cerberus-Engineering-Tooland loaded back into the station.

Without pre-configuration

During commissioning, first the modules and the station periphery are read in. There are two ways of reading in the periphery:

- The C-NET lines are read in individually. The resulting physical structure is loaded into Cerberus-Engineering-Tool.
  The logical structure is then created in Cerberus-Engineering-Tool and is linked with the physical structure.
- The C-NET lines are read in by automatic configuration. The physical structure and the logical structure are created (a section is created for the detector line and a zone for each C-NET device). The two structures are loaded into Cerberus-Engineering-Tool.

  The automatic configuration can be carried out at the station or related to single detector lines.

Customer text

All components may be provided with a customer text. The customer text is shown in the operating terminal display. However, not all elements require inscription. The length of the customer text is checked when inscribing in Cerberus-Engineering-Tool.

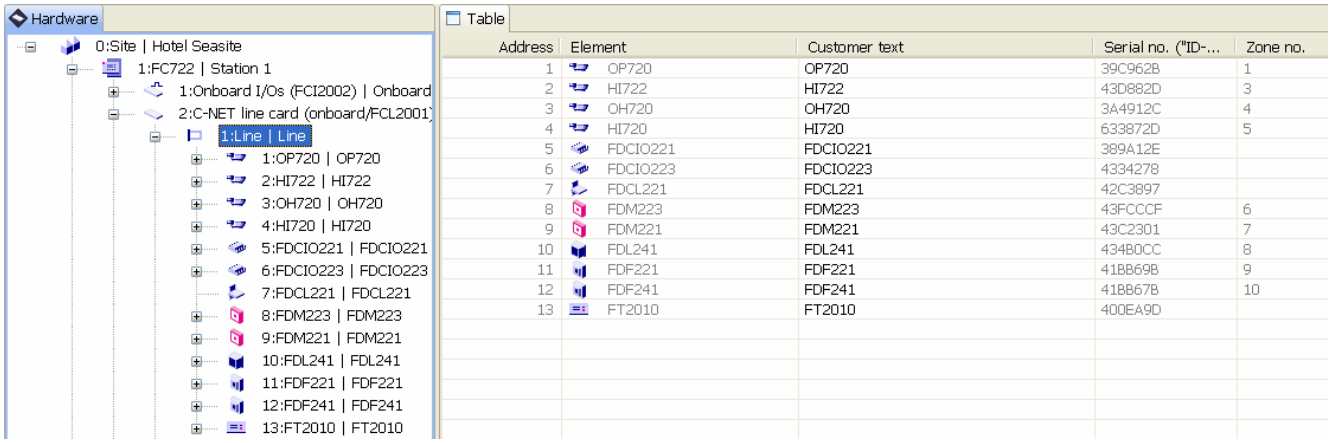
For the indication on the display of the PMI, the following rules must be taken into account:

- All elements except 'Zone' element:

  If a message associated with an element appears, the corresponding customer text is displayed. If no customer text is assigned to that element, the customer text of the next higher-level element is displayed, e.g. when a detector has no customer text, the text for the line is displayed.
- 'Zone' element:

  If an alarm message for a 'Zone' appears, the customer text of the detector sensor linked to it is displayed. If no customer text is assigned to it, the customer text for the 'Zone' appears. If no customer text is assigned to the 'Zone' either, the customer text of the next higher-level element appears, and so on.

8.1 'Hardware' task card



Hardware task card with the hardware tree and the window 'Table'

The station components and the peripheral devices in the Hardware tree are displayed in the 'Hardware' task card.

The components are automatically read in when starting the station.

The C-NET devices are read in via the station's Person Machine Interface upon the user's command.

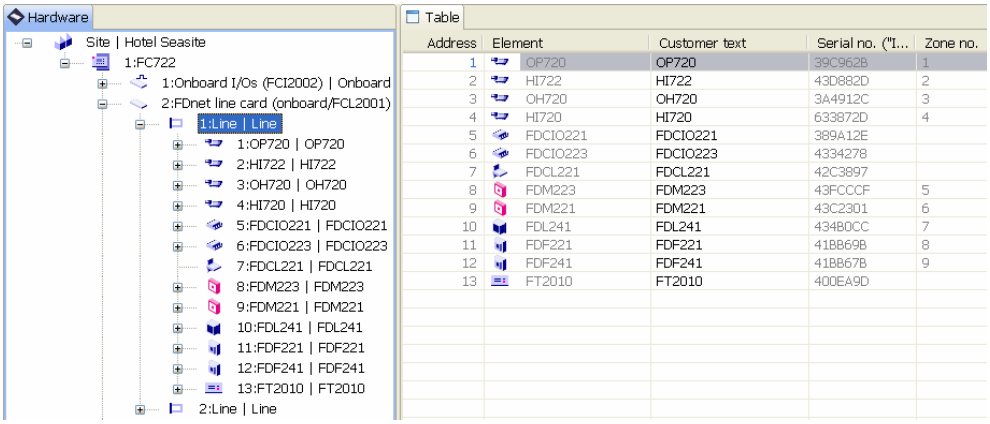
Once the data has been uploaded into the Cerberus-Engineering-Tool, the station components and the C-NET devices/peripherals are visible in the Hardware tree.

The structure of the C-NET devices cannot be edited.

Elements that are not produced automatically can, however, be added or removed, e.g., the 'LED indicator (FTO2002)' element.

8.1.1 Station

Features



Detail editor 'Station', 'Details'

For the station, the following properties can be set:

- In the detail editor ('Intervention'): 'Immediate intervention type 'manned''/'Immediate intervention type 'unmanned'' and 'Service intervention type 'manned''/'Service intervention type 'unmanned'' configuration
- In the detail editor ('Details'):
  - Stopping the local and global alarming equipment by means of 'Acknowledge', which is activated by 'Immediate intervention type 'manned''/'Immediate intervention type 'unmanned'' or 'Service intervention type 'manned''/'Service intervention type 'unmanned''.
  - Activation of a message so that the end-user is reminded to perform the maintenance work. 'Maintenance interval [months]' can be set in months.
- In the detail editor ('BACnet Notification Class element'), see [→ 214]
- In the detail editor ('Operation'): Visibility on the event categories. By default visibility is set to all event categories. As an alternative, the visibility can be selected for individual event categories:'ALARMS', 'Pre-ALARMS', 'Faults', 'Isolations', 'Test messages', 'Technical messages', 'Activations', 'Information'.

See also

BACnet Notification Class Element [→ 214]

8.1.1.1 Intervention concept (IC)

The intervention concept (IC) is a standard configuration for immediate intervention and service intervention.

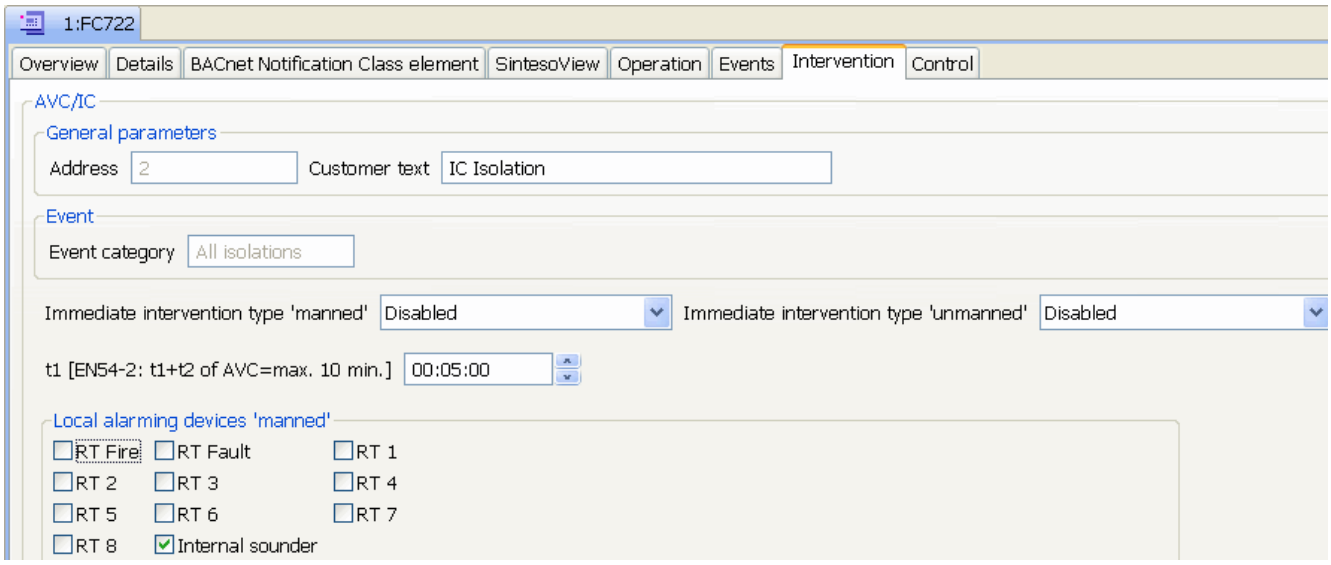
Events such as a fault caused by a soiled detector are monitored during a preconfigured period of time. If the normal operation conditions are not re-established within this period of time, the maintenance personnel is informed (service intervention). In this way, it is possible to rectify a fault locally before informing the maintenance personnel.

You will find a detailed description of the intervention concept in the document A6V10210355, system description.

The intervention concept verifies the following event categories:

- 'All faults'
- 'All isolations'
- 'All test messages'
- 'All technical messages'
- 'All activations'
- 'All information messages'

Configuring intervention concept



Detail editor 'Station', 'Intervention'

1. Select the 'Hardware' task card.
2. Highlight 'Station' in the tree view.
3. In the 'Station' detail editor ('Intervention'), set the properties for the intervention types.

Immediate intervention

For immediate intervention the following properties can be set:

- Separately for 'Manned operation' and 'Unmanned operation':
  - 'Disabled'
  - 'Delayed intervention'
  - 'Global intervention only'
  - 'Local intervention only'
- Time t1 for (intervention) attendance check:

  A new event must be acknowledged within this period, otherwise the intervention concept switches to global alarming.
- Alarming equipment

Service intervention

For service intervention the following properties can be set:

- Separately for 'Manned operation' and 'Unmanned operation':
  - 'Disabled'
  - 'Delayed intervention'
  - 'Direct intervention'

- Service intervention time ts:

  Within this time period, the cause of an event must be remedied/must disappear, otherwise the intervention concept activates the alarming equipment of the service intervention.

- Alarming equipment:

  'RT Fire', 'RT Fault', 'RT 1' - 'RT 8', 'Internal sounder'

8.1.2 Power supply

Operation modes

The power supply concept of the stations distinguishes between the following types of operation:

- Operation with battery backup
  - The power supply unit feeds the hardware with system voltage, continuously charging the batteries. In case of a mains failure, the batteries take over the power supply of the station without interruption.
- Operation without battery back-up
  - The power supply unit feeds the hardware with system voltage. In this case, the emergency power supply is ensured via an externally buffered network.
- Operation with an external DC power supply unit
  - The supply comes directly via a 24 V DC feed line. This is the normal operating mode for the fire terminal FT724.
- Operation with redundant supply
  - The fire terminal can be fed with 24 V DC by a fire control panel. In accordance with EN 54, a redundant supply source is required in this case. The fire terminal board is therefore provided with two independent DC supply inputs.

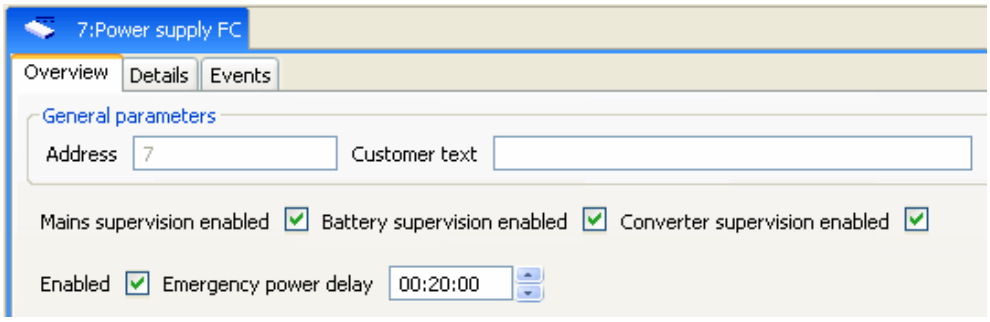
Features

For the power supply, the following properties can be set:

- Mains supervision
  - Monitoring for power loss.
- Battery supervision
  - Monitoring switched on or off.
- Converter supervision
  - Monitoring switched on or off.
- Emergency power operation
  - Delay time for the display of a fault in case of power loss; can be set when switched on.

Setting properties

Depending on the operation mode, certain monitorings must be deactivated. Normally when the station is equipped with a power supply unit and batteries, no monitorings need deactivating. The configuration of the delay time for the fault indication in case of a power failure is independent from the operation mode.



Detail editor 'Power supply FC', 'Overview'

To set the properties, proceed as follows:

1. Select the 'Hardware' task card.
2. Open 'Station' in the tree view.
3. Highlight 'Power supply FC' or 'Power supply FT'.
4. In the detail editor ('Power supply FC' or 'Power supply FT' > 'Overview'), check the boxes as indicated in the table below.

Operation mode	'Mains supervision enabled'	'Battery supervision enabled'	'Converter supervision enabled'	Display delay 'Emergency power delay', 'Enabled '
with battery backup	√	√	√	√ or –
without battery backup	√	–	√	–
with an external DC power supply unit	–	–	–	–
with redundant supply	√	√	–	√ or –

Configuration of the power supply

√ Checkmark set

– Checkmark removed

You will find the hardware configuration in document A6V10210416, commissioning.

8.1.3 Onboard I/Os

The following inputs and outputs are available on the periphery board:

- 'I/O': Configurable inputs/outputs (24 V)
- 'RT fire/NOT monitored': Connection of an RT channel for RT alarm
- 'RT fire/monitored': Monitored output for RT alarm
- 'RT fault/NOT monitored': Connection of an RT channel for RT fault
- 'RT fault/monitored': Monitored output for RT fault
- 'Sounder/monitored': Monitored sounder output

These inputs and outputs are shown in the Hardware tree under the 'Onboard I/Os' element.

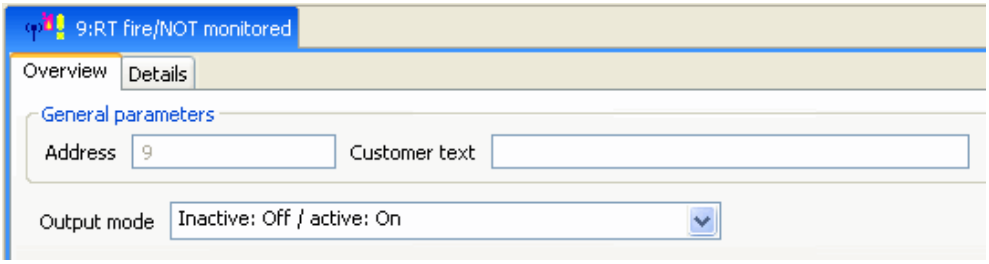
In the detail editor the following properties can be set:

- 'Output mode'
- 'Input inverted'
- 'Open/short circuit monitoring enabled'

To set the properties, proceed as follows:

1. Select the 'Hardware' task card.
2. Open 'Station' > 'Onboard I/Os' in the tree view.
3. Highlight the corresponding input/output.
4. In the detail editor select the properties described below.

Output mode



Output mode in the detail editor, 'Overview'

For each output, ten output modes are possible.

Output mode	Inactive	Active	Always
1			Off
2	Off	Intermittent, slow	
3	Off	Intermittent, fast	
4	Off	Intermittent, pulse	
5	Off	On	
6			On
7	Intermittent, slow	Off	
8	Intermittent, fast	Off	
9	Intermittent, pulse	Off	
10	On	Off	

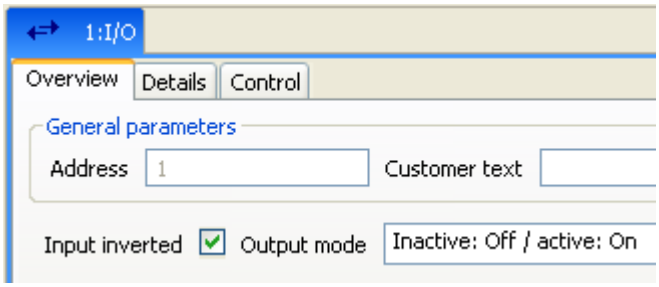
Output modes in the detail editor, 'Overview'

The output mode defines the behaviors of the output signal in active or inactive status of the logic.

Examples:

- 'Inactive: Off / active: On' = The output signal is switched off when the logic is in an inactive status and switched on when it is in an active status.
- 'Inactive: Off / active: Intermittent, fast (0.25s/0.25s)' = The output signal is switched off when the logic is in an inactive status. When the logic is in an active status, it is 0.25 s HIGH and 0.25 s LOW (alternating).
- 'Always Off' = The output signal is switched off when the logic is in both an inactive and active status.

Invertible input



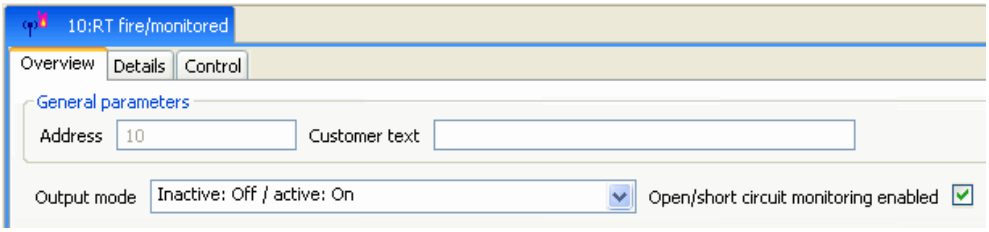
Invertible input in the detail editor, 'Overview'

The inputs can be inverted.

Checkmark set	Active when signal is changing from HIGH to LOW
Checkmark removed	Active when signal is changing from LOW to HIGH

Input inverted in the detail editor 'Onboard I/Os', 'Overview'

Monitored outputs



Open/short circuit monitoring in the detail editor, 'Overview'

The monitoring of monitored outputs can be inactivated. This includes:

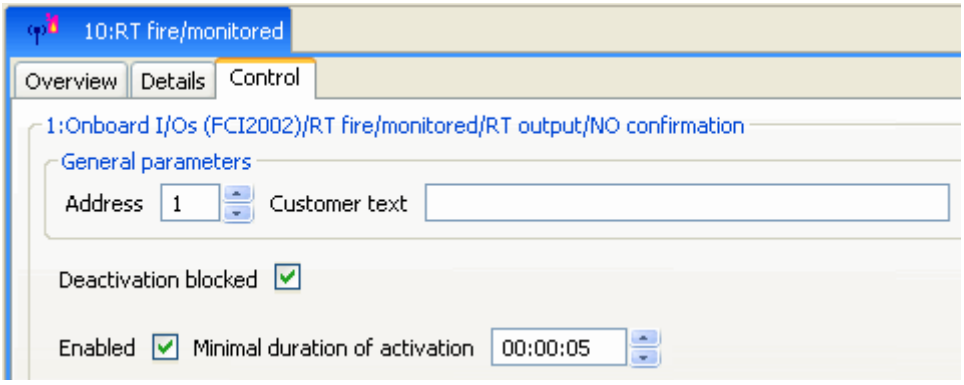
- 'RT fire/monitored'
- 'RT fault/monitored'
- 'Sounder/monitored'

Duration of activation and deactivation

When the output is linked to the effect of a control, the minimal duration of activation can be set and the deactivation can be blocked.

The following outputs are affected by this:

- 'RT fire/monitored'
- 'RT fault/monitored'



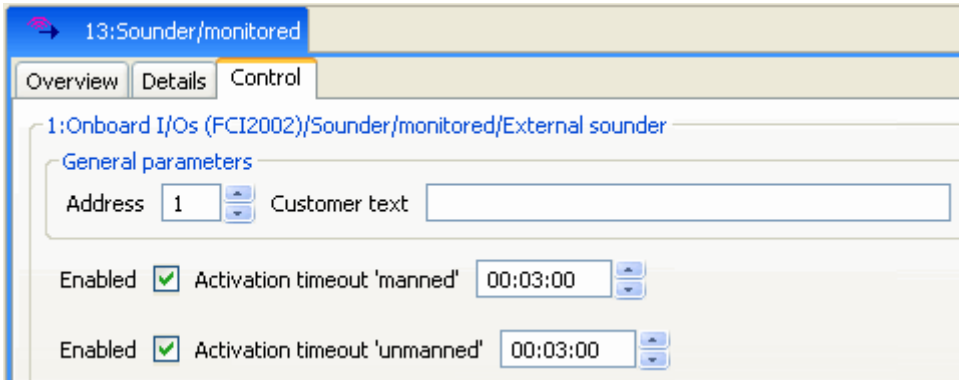
Deactivation blocked and Minimal duration of activation in the detail editor 'RT/monitored', 'Control'

Activation timeout

When the output is linked to the effect of a control, 'Activation timeout 'manned'' and 'Activation timeout 'unmanned'' can be activated or deactivated separately and the duration selected.

The following output is affected by this:

- 'Sounder/monitored'



Activation timeout in the detail editor 'Sounder', 'Control'

8.1.4 Detector parameter sets

The detection behavior of the automatic fire detectors is influenced by the parameter sets, so that it can be very specifically adjusted to the fire phenomena and environmental conditions to be expected in the environment to be monitored.

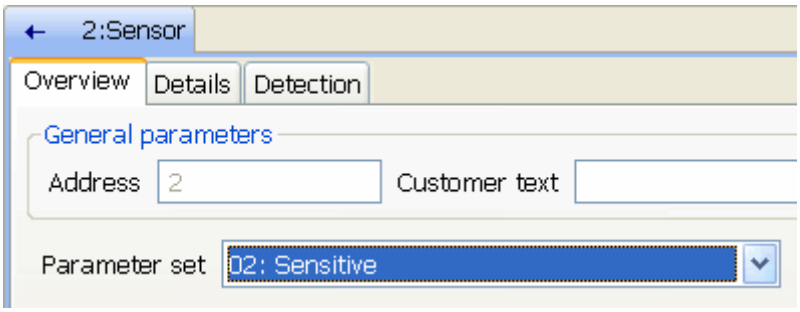
Examples:

- When a smoke detector is placed in a production hall, a parameter set must be selected that has a high immunity to deceptive phenomena.
- When the smoke detector is placed in a hospital room, however, a parameter set must be selected ensuring the earliest possible alarming.

Setting detector parameter sets

The detector parameter sets are visible in the detail editor of the 'Hardware' task card if the detector sensor to be parameterized is highlighted in the tree view.

If the detector sensor is linked to the logical channel of an automatic zone, the parameter sets for the detectors in the detail editor of the 'Detection' task card are also visible under the 'Hardware' button.



Detail editor 'Sensor', 'Parameter set'

To set the parameter sets, proceed as follows:

1. Select the 'Hardware' task card.
2. Open 'Station' > 'C-NET line card (onboard/FCL2001)' > 'Line' > 'Detector' in the tree view.
3. Highlight 'Sensor '.
4. In the detail editor ('Sensor' > 'Overview'), define the parameter sets for 'Manned operation' and 'Unmanned operation'.

A detailed description of the parameter sets that can be selected can be found in the corresponding documentation FD720, Cerberus detector system.

8.1.5 External alarm indicator

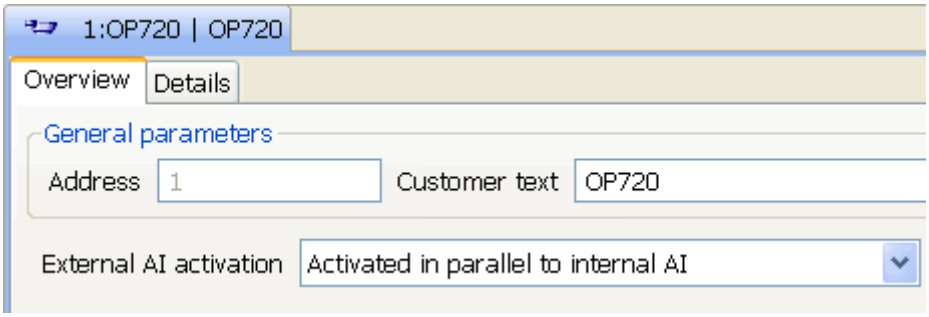
Some C-NET devices have an external alarm indicator output.

The output can be used to actuate an external alarm indicator and for controls.

Editing properties

There are three ways to activate the external alarm indicator output:

- 'Activated by the zone of the detector'
- 'Activated in parallel to internal AI'
- 'Activated by a control (independent output)'



External AI activation in the detail editor of a detector, 'Overview'

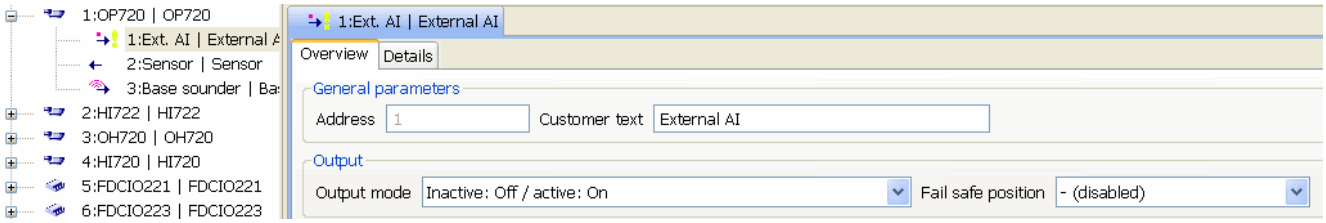
Proceed as follows:

1. Open the 'Hardware' task card.
2. Highlight the relevant C-NET device in the tree view.
3. In the detail editor ('Detector' > 'Overview'), select the activation mode in the 'External AI activation' box.

When the 'Activated by a control (independent output)' activation mode is selected, the external alarm indicator output can be used for an evacuation control or fire control.

For the external alarm indicator output it is possible to select the following properties for certain detectors, depending on their product version:

- 'Fail safe position'
- 'Output mode'



Fail safe position and Output mode in the detail editor 'Ext. AI', 'Overview'

Proceed as follows:

1. Open the relevant C-NET device in the tree view.
2. Highlight 'Ext. AI '.
3. In the detail editor ('Ext. AI' > 'Overview'), define the 'Fail safe position' and 'Output mode'.

8.2 'Detection' task card

The following logical elements of the detection tree are shown in the 'Detection' task card:

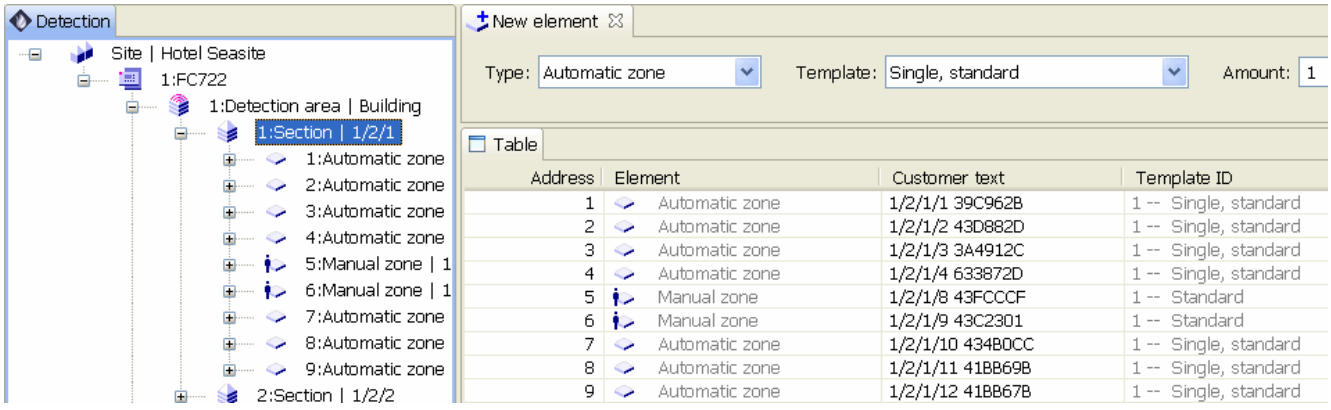
- 'Area'
  - The 'Area' element is also created when creating a control panel.
  - Other 'Area' elements can be produced for each control panel.
- 'Section'
  - If included in the BDV, the 'Section' element can be produced manually.
- 'Zone'
  - The 'Zone'element can be produced manually.
- 'Physical channel'
  - The 'Physical channel' element can be produced manually during pre-configuration. But this is not usually necessary because this element is produced when linking with the corresponding hardware element. If a link is deleted, the channel is retained.

If the control panel is configured using the 'Auto-configure line' or 'Auto-configure station' function, the Section', 'Zone', and 'Physical channel' elements are created automatically. The physical and logical channels are linked automatically.

See also

Document A6V10210416, commissioning, Definition of terms.

8.2.1 Detection tree



Task card 'Detection' with the tree view and window 'New element'

To create the Detection tree, proceed as follows:

1. Create a 'Site' and the Station (Stations) if a Site is not yet available.
2. Select the 'Detection' task card.
3. Open a control panel.
   ⇨ The 'Detection area' sub-element is visible.
4. Open the 'New element' window.
5. If you need to create other 'Detection area' elements, highlight the control panel in the tree view.
   ⇨ The 'Detection area' element is displayed in the 'Type:' field of the 'New element' window.
6. Enter the number of elements required in the 'Amount:' field and click on the 'Add' button.
   ⇨ Other Areas are created.
7. Enter the customer text(s).
8. Highlight 'Detection area '.
9. If required, and if provided in the BDV, select the 'Section' element in the 'Type:' field.
10. Enter the number of elements required in the 'Amount:' field and click on the 'Add' button.
    ⇨ The elements are created.
11. Enter the customer text(s).
12. Highlight 'Section' in the tree view.
13. In the 'New element' window, select a Zone (e.g., 'Automatic zone') and the appropriate 'Template:' in the 'Type:' field.
14. Enter the number of elements required in the 'Amount:' field.
15. Click on the 'Add' button.
    ⇨ The elements are created.
16. Enter the customer text(s).

8.2.2 Area

Each control panel contains the following Areas:

- 'Detection area'

  is the uppermost element in the Detection tree. Several 'Detection area' are possible per control panel:
  – FC722, FC724: up to four
    The 'Detection area' has an alarm verification concept (AVC) and can be configured and linked to the controls independently of other areas.

- 'Station area'

  occurs just once and unites the alarm verification (AVC) functionality for hardware-related elements which are not in the Detection area. This includes e.g. collective line alarms and emergency operation. The Station area can be displayed and navigated just like any other Detection area. It has no child elements and is identical to the Detection area in terms of alarm verification.

Properties of the area

The following properties can be set for the Area:

- In the detail editor ('Overview')
  – 'UNMANNED switching time 1' to 'UNMANNED switching time 4':
    Times of the day at which the alarm organization is automatically switched to 'Unmanned operation' for the first, second, third, or fourth time. This is required if, for example, the alarm organization is manually switched back to 'Manned operation' after being automatically switched over to 'Unmanned operation'.

- In the detail editor ('Details')

  'Immediate global alarming': This configuration is used to determine under which of the following preconditions the alarm verification concept is directly and globally alarmed:
  – '- (disabled)'
  – 'Upon 2nd alarm within area'
  – 'Upon 2nd alarm within area OR fault within station'
  – 'Upon 2nd alarm within site'
  – 'Upon 2nd alarm OR fault within site'
  – 'Always (upon first alarm)'
  'Alarm organization mode': This configuration is used to determine which of the following statuses ('Manned operation', 'Unmanned operation') and functions (switchovers, indications) of the alarm organization are used in this area:
  – 'Always manned (no messages/no LED/no switching fct.)'
  – 'Always unmanned (no messages/no LED/no switching fct.)'
  – 'Manned/unmanned (with messages/with LED/with switching fct.)'

8.2.2.1 Alarm verification concept (AVC)

The Alarm Verification Concept (AVC) serves the purpose of delayed alarm transmission and takes into account the interaction of the operating personnel in the alarming sequence.

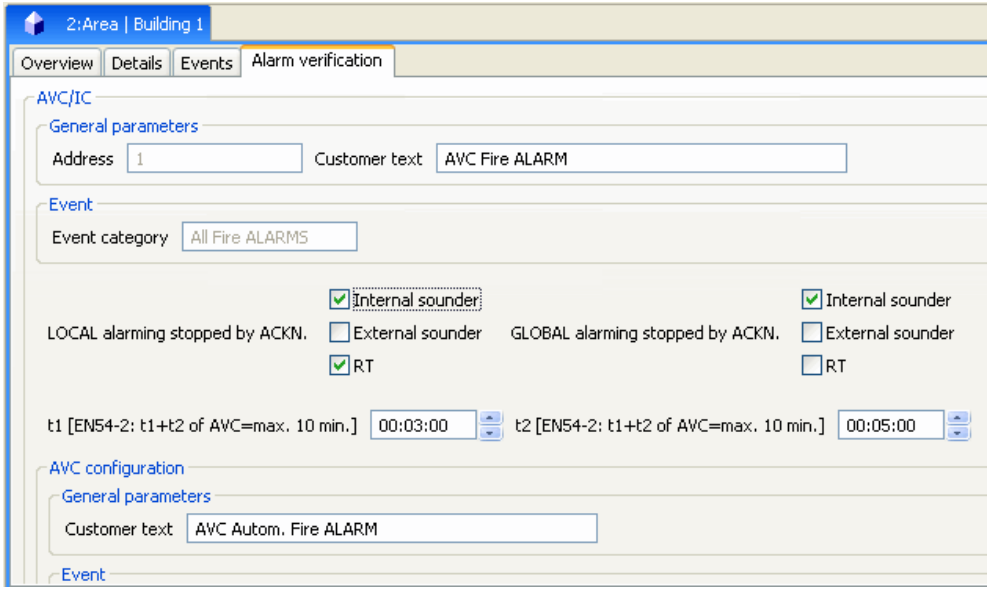
In the event of a fire, a local alarm is triggered. The operating staff have a certain amount of time to investigate the location given for the fire. In case of a false alarm or minor incident the intervention of the fire department (global alarm) can be avoided in good time.

You will find a detailed description of the Alarm Verification Concept in document A6V10210355, system description.

The Alarm Verification Concept verifies the following event categories:

- 'All Fire ALARMS'
- "--All autom. Fire ALARMS'
- "--Manual Fire ALARM'
- "--Degraded Fire ALARM'
- 'All Pre-ALARMS'
- 'Pre-ALARM, fire'

Configuring the Alarm Verification Concept



Detail editor 'Area', 'Alarm verification'

1. Select the 'Detection' task card.
2. Highlight 'Detection area' in the tree view.
3. In the 'Detection area' detail editor ('Alarm verification'), set the properties for the event categories.

'All Fire ALARMS', 'All Pre-ALARMS'

For these event categories, the following general properties can be set:

- Stopping the local and global alarming equipment by means of 'Acknowledge', which is activated by alarm verification
- Manned time t1

  A new event must be acknowledged within this period (max. 60 s), otherwise the alarm verification concept will switch to global alarming.
- Investigation time t2

  The cause of an event must be investigated within this period and the system reset, otherwise the alarm verification concept changes to global alarming. According to EN 54-2, the sum of t1+t2 must not exceed 10 minutes.

"--All autom. Fire ALARMS', "--Manual Fire ALARM', "--Degraded Fire ALARM', 'Pre-ALARM, fire'

Type of alarming when the alarm organization is in 'Manned operation' or 'Unmanned operation':

- 'Local alarming only'
- 'Delayed alarming'
- 'Global alarming only'

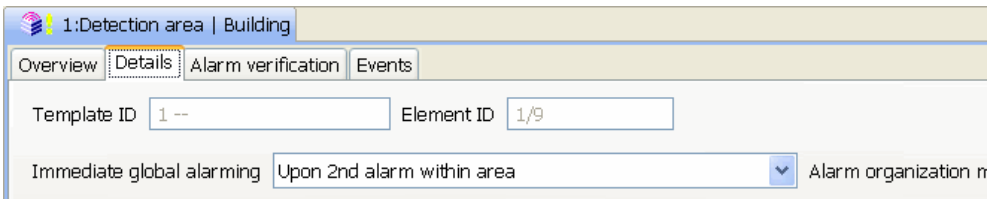
Selection of local and global alarming equipment when alarm organization (Area) is in 'Manned operation' or 'Unmanned operation':

- 'RT fire', 'RTfault', 'RT 1' - 'RT 8', 'Internal sounder', 'External sounder'

8.2.2.2 Immediate global alarming

this configuration is used to determine under which of the following preconditions the alarm verification concept is directly and globally alarmed:

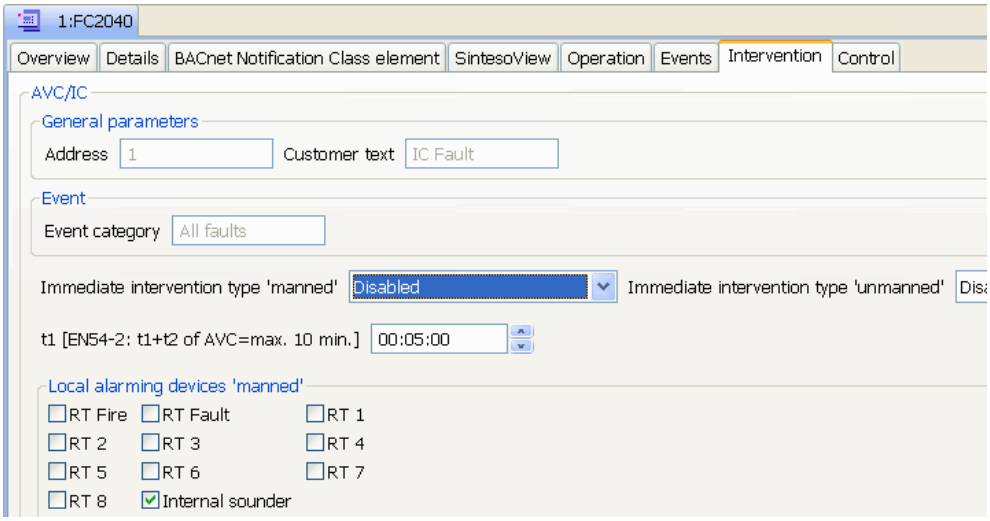
- "- (disabled)'
- 'Upon 2nd alarm within area'
- 'Upon 2nd alarm within area OR fault within station'
- 'Upon 2nd alarm within site'
- 'Upon 2nd alarm OR fault within site'
- 'Always (upon first alarm)'



Detail editor 'Detection area', 'Details'

Settings for intervention

If the setting 'Upon 2nd alarm within area OR fault within station' or 'Upon 2nd alarm OR fault within site' is selected for immediate global alarming, in the detail editor for intervention in the station, category 'IC Fault', the settings for 'Immediate intervention type 'manned'' and 'Immediate intervention type 'unmanned'' must never be 'Disabled'. Always select a defined setting.



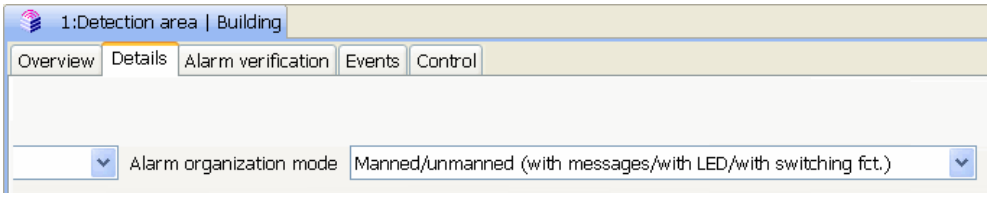
Detail editor, 'Station', 'Intervention'

If individual devices are not to be activated with 'IC Fault' , they can be deactivated by removing the check mark from the checkbox.

8.2.2.3 Alarm organization mode

This configuration is used to determine which of the following statuses ('Manned operation', 'Unmanned operation') and functions (switchovers, indications) of the alarm organization are used in this area:

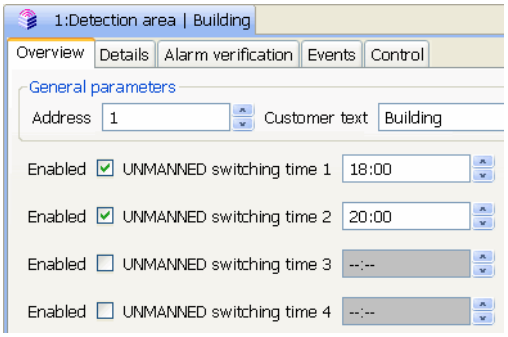
- 'Always manned (no messages/no LED/no switching fct.)'
- 'Always unmanned (no messages/no LED/no switching fct.)'
- 'Manned/unmanned (with messages/with LED/with switching fct.)'



Detail editor 'Detection area', 'Details'

8.2.2.4 UNMANNED switching times

If in the detail editors 'Detection area' and 'Overview' there are check marks 'Enabled' for 'UNMANNED switching time 1' to 'UNMANNED switching time 4', you can set the times of day at which the alarm organization automatically switches to 'Unmanned operation' for the first, second, third or fourth time. This is required if, for example, the alarm organization is manually switched back to 'Manned operation' after being automatically switched over to 'Unmanned operation'.



Detail editor 'Detection area', 'Overview'

8.2.3 Fire alarm zone

There are the following zone types:

- Automatic zone
- Manual zone
- Technical zone
- FSE zone
- Flow switch zone
- Flow switch zone

8.2.3.1 Automatic zone

Automatic detectors are combined in the automatic zone. The zone may, however, also be configured for other alarm inputs ('Input' and 'Collective') channels.

When creating an automatic zone in the 'Detection' task card, you can chose between 'Single' and 'Multi'. 'Single' is for single-detector dependence and 'Multi' is for multi-detector dependency. For both zone types you can select between various combinations that are defined such that several detectors must reach danger level 2 or 3 to trigger an alarm.

Template	Criteria for			
	Pre-stage		Main stage	
	Number of detectors with danger level 2	Number of detectors with danger level 3	Number of detectors with danger level 2	Number of detectors with danger level 3
'Single, standard'	1	0	0	1
'Single, ALARM sub-system'	1	0	0	1
'Single, Exting. discharged'	1	0	0	1
'Single, Exting. pre-alarm'	1	0	0	1
'Single, Gas alarm'	1	0	0	1
'Single, Gas warning'	1	0	0	1
'Single, door holders'	0	0	0	1
'Single, local ALARM'	1	0	0	1
'Multi, standard'	1	0	2	1
'Multi, garage'	0	0	0	2
'Multi, store'	1	0	2	1
'Multi, 2 det. dependency'	0	1	0	2
'Multi, ALARM sub-system'	0	1	0	2
'Multi, 2 det. dependency II' [AT]	0	1	0	2
'Multi, 2 det. dependency III' [CH]	0	1	0	2
'Two-zone dependency'	0	1	0	0

Template for the automatic zone

8.2.3.2 Manual zone

The manual call points are normally combined in the manual zone. The zone may however also be configured for other alarm inputs ('Alarm input' and 'Collective' channels). Danger signals are evaluated by means of an OR relation. Each manual call point in the zone can generate an alarm but not a pre-alarm.

Template	Criteria for main stage	
	Number of detectors with danger level 2	Number of detectors with danger level 3
Standard	0	1
ALARM sub-system	0	1
Local ALARM	0	1
Redundancy ALARM	0	1

Template for the manual zone

8.2.3.3 Technical zone

In the technical zone, inputs for technical messages, e.g. fault or danger by extraneous equipment, are evaluated.

Template	Criteria for main stage	
	Number of detectors with danger level 2	Number of detectors with danger level 3
Standard	0	1
Fault sub-system	0	1
Sub-system OFF	0	1
Fault extinguishing system	0	1

Template for the technical zone

8.2.3.4 FSE zone [DE]

A release element is assigned to the FSE zone. With the release element, a fire alarm is generated manually, which in turn unlocks the fire department key depot. A key which is held exclusively by the fire department is needed to operate the release element.

Template	Criteria for main stage	
	Number of detectors with danger level 2	Number of detectors with danger level 3
Standard	0	1

Template for the FSE zone

8.2.3.5 Flow rate indicator zone

In larger sprinkler systems, the piping system is distributed over several floors and the line network has an outlet on every floor. Flow rate indicators are built into these outlets. These signal where exactly the water runs to and generate an additional report for reporting to the sprinkler station.

The flow rate indicator is evaluated by means of an OR relation. Each flow rate indicator in the zone can generate an alarm.

Template	Criteria for alarm	
	Number of detectors with danger level 2	Number of detectors with danger level 3
Standard	0	1

Template for the flow rate indicator zone

See also

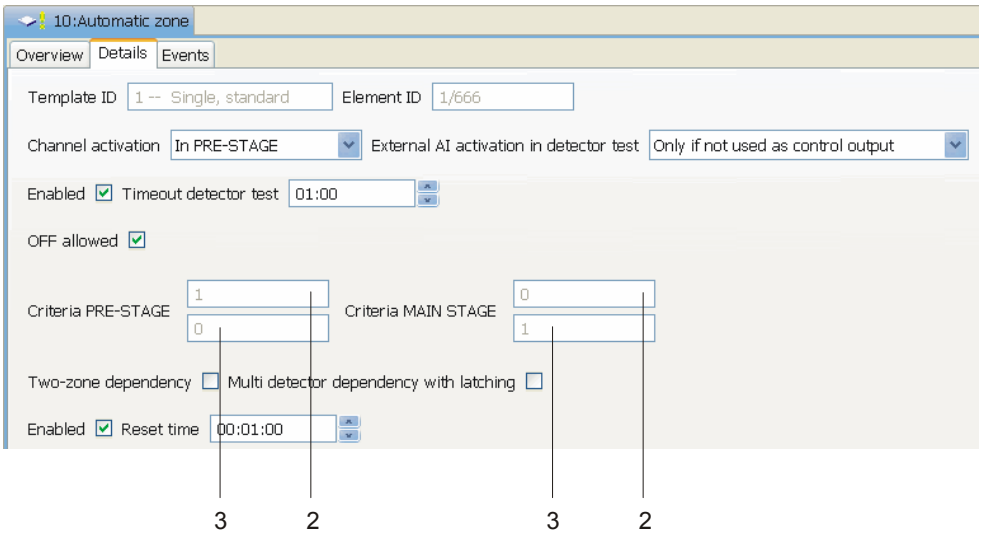
Sprinkler zone [→ 91]

8.2.3.6 Sub-system zone

Signals from sub-systems can be assigned to the sub-system zone by means of inputs and outputs. The zone contains inputs for pre-alarm, alarm, fault, and isolation, as well as outputs for acknowledging and resetting.

8.2.4 Configuring zone fire alarm

The settings of the zone and the pre-stage/main stage criteria described above are shown in the detail editor of the corresponding zone, under the 'Details' button.



Detail editor of the zone with settings and the criteria for the pre-stage and main stage

2 Number of detectors with danger level 2 3 Number of detectors with danger level 3

The properties shown in the following tables can be configured in the detail editor of the zone.

Channel activation

Selection	Effect
'In PRE-STAGE'	The contributing channels generate an activation message and activate their alarm indicators when the conditions for the pre-stage are met.
'In MAIN STAGE'	The contributing channels generate an activation message and activate their alarm indicators when the conditions for the main stage are met.

External AI activation in detector test

Selection	Condition	Effect
'No'	The external alarm indicator output is used as a control output for an application that is independent from the fire detection part.	The external alarm indicator output is not activated in test mode.
'Only if not used as control output'	The device (detector) option in the hardware tree is set so that the external alarm indicator is activated in parallel to the detector or zone.	The external alarm indicator output is activated in test mode.
	The external alarm indicator output is used as a control output and an external alarm indicator which is to be activated in test mode is connected (e.g. if several zones share an external alarm indicator).	In order to activate the external alarm indicator in the detector test, one cause for the criterion 'Test activation' must be added to the control per zone (using Configuring universal control).

Timeout detector test

Option	Effect
Checkmark removed for 'Enabled'	Timeout cannot be set.
1 h to 23 h 59 m	When this timeout expires, the detector test is ended automatically.

OFF allowed

Option	Effect
Checkmark set	The zone can be switched off by an operating command.
Checkmark removed	The zone cannot be switched off by an operating command.

Reset time

Option	Effect
Checkmark removed for 'Enabled'	Reset time cannot be set. In this case, the suitable reset time is set by the control panel.
1 s to 5 m	When the sub-systems are activated, the suitable reset time must be determined. The system attempts to reset the element within this time before the attempt is considered a failure.

Always resettable

This property is only available for the manual zone.

Option	Effect
Checkmark set	Zone can always be reset (message 'glass broken' from manual call points that are still active).
Checkmark removed	Zone can only be reset if all assigned manual call points are quiet.

Evaluation filter time

This property is only available for the sub-system zone. The time must be set for each input and output (1 s to 5 m). This is the time during which a signal must be present in order for the input or output to be evaluated as active.

8.2.4.1 Multi-detector dependency

!	*NOTICE*
	Use with collective line technology is not compliant with standards
	Multi-detector dependency may not be set up with collective lines.

The following elements are available in the automatic zone for configuring the multi-detector dependency:

- 'Multi, 2 det. dependency' and 'Multi, 2 det. dependency III' [CH]:

  There is no checkmark in the box for 'Multi detector dependency with latching'. The danger level of the detector is not stored. The multi-detector dependency is used for a stationary fire.

- 'Multi, 2 det. dependency II' [AT]:

  For 'Multi detector dependency with latching': the checkmark is set. The detectors linked to a zone are evaluated in multi-detector dependency with the signal being stored. If the zone reaches the pre-stage then the danger levels of the detectors that have reached the criteria of the pre-stage are stored as a criterion for the main stage. As soon as the required number of detectors have

stored the criteria for the main stage then the main stage is reached and signaled accordingly.
Typical application example: If a detector signals danger level 3, the zone reaches the pre-stage and a first alarm is triggered. Danger level 3 of the detector is stored as the criterion for the main stage. As soon as further detectors signal danger level 3, the zone reaches the main stage and a second alarm is triggered.
Multi-detector dependency can be used for a moving fire, for example for detecting a fire on a conveyor belt.

Element	Default settings
'Multi, 2 det. dependency'	Freely selectable
'Multi, 2 det. dependency II' [AT]	1 detectors with danger level 3: ● Automatic first alarm ● Local alarming only (no delay times, internal sounder only) 2 detectors with danger level 3: ● Automatic fire alarm ● 'Manned operation': Delayed alarming ● 'Unmanned operation': Global alarming only
'Multi, 2 det. dependency III' [CH]	1 detectors with danger level 3: ● Automatic first alarm ● 'Manned operation': Delayed alarming ● 'Unmanned operation': Global alarming only 2 detectors with danger level 3: ● Automatic fire alarm ● 'Manned operation' and 'Unmanned operation': Global alarming only

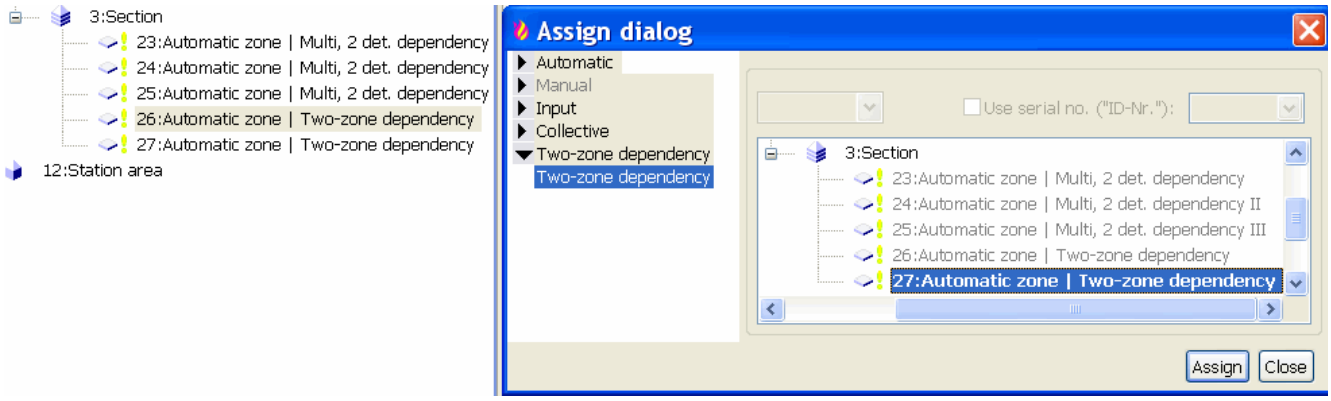
Default settings of the possible elements

8.2.4.2 2-zone dependency

If the multi-detector dependency extends over two zones, these zones can be linked together. To do this, two automatic zones are required with the 'Two-zone dependency' template that can be linked together. When the first of the two zones reaches the pre-stage this causes a message to be sent. When the second zone also reaches the pre-stage then both zones change to the main stage and send a corresponding message. One zone alone cannot reach the main stage.

Creating 2-zone dependency

1. In the 'Detection' task card, create two 'Automatic zone' elements using the 'Two-zone dependency' template.
2. Link both zones with the corresponding hardware.



'Assign dialog' window for linking the two zones

To link the two zones together, proceed as follows:

1. Select the 'Detection' task card.
2. Open 'Detection area' > 'Section' in the tree view.
3. Highlight 'Automatic zone'/'Two-zone dependency'.
4. Open the 'Assign dialog' window and highlight 'Two-zone dependency' in the list.

   ⇨ The Detection tree is displayed in the 'Assign dialog' window. The elements that can be linked are highlighted.
5. Highlight the 'Two-zone dependency' to be linked and click on the 'Assign' button.

⇨ The two zones are linked together.

Properties of the 'Two-zone dependency' automatic zone

The following default settings are made in the detail editor of the 'Two-zone dependency' automatic zone:

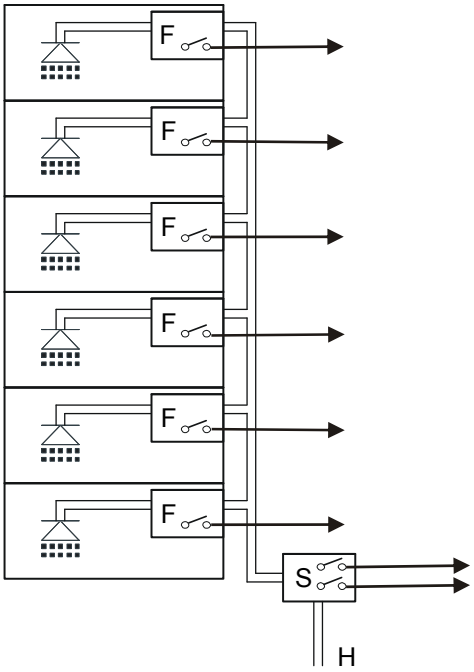
- Automatic first alarm
- Local alarming only (no delay times, internal sounder only)

8.2.5 Extinguishing zone

There are the following zone types:

- Sprinkler zone
- XC10 zone

8.2.5.1 Sprinkler zone



General setup of the sprinkler system

F Flow rate indicator: special detector zone

S Sprinkler station with one or two contacts

H Hydrant network

A sprinkler system is a piping system that is terminated at several locations with sprinkler heads. it is normally fed by the public network of hydrants. The sprinkler station is installed directly after the house feed. It separates the sprinkler network from the hydrant network due to overpressure in the sprinkler network. The sprinkler station signalizes when the sprinkler network is opened somewhere and water begins to flow. This condition is reported to the fire control panel via a contact (optionally also two). This then triggers an alarm with immediate response from the fire department.

In larger sprinkler systems, the piping system is distributed over several floors and the line network has an outlet in every floor. Flow rate indicators are built into these outlets. These signal where exactly the water runs to and generate an additional report for reporting to the sprinkler station.

Creating 'Sprinkler zone' element

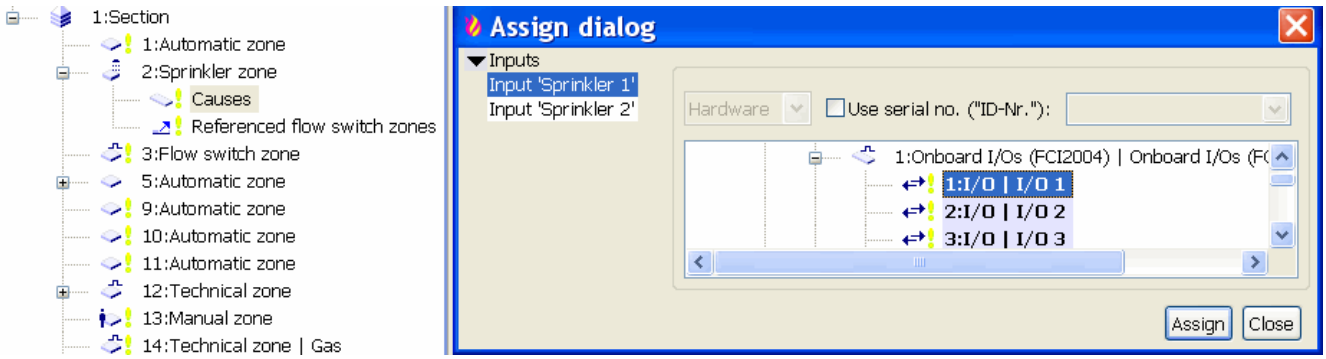
Create the 'Sprinkler zone' element in the 'Detection' task card.

Creating 'Flow switch zone' element

Create the 'Flow switch zone' element in the 'Detection' task card.

Linking 'Sprinkler zone' element

The 'Sprinkler zone' element has the 'Causes' channel for connecting the 'Input 'Sprinkler 1" and 'Input 'Sprinkler 2" contacts of the sprinkler station and the 'Referenced flow switch zones' channel, which is linked to the flow rate indicator zone.



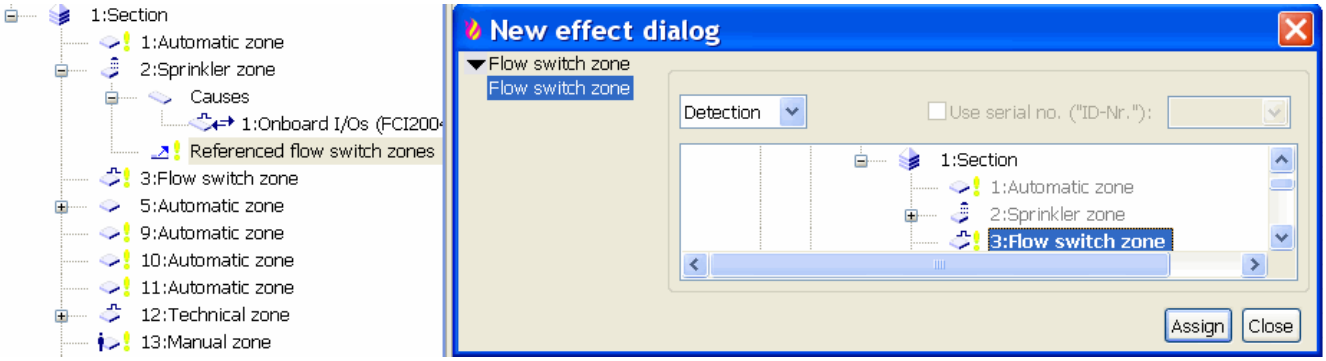
'Assign dialog' window for linking 'Causes' with 'Input 'Sprinkler 1" and 'Input 'Sprinkler 2"

To link 'Input 'Sprinkler 1", proceed as follows:

1. Select the 'Detection' task card.
2. Open 'Sprinkler zone' in the tree view.
3. Highlight 'Causes '.
4. Open the 'Assign dialog' window.
5. Select the corresponding input and click on the 'Assign' button.

⇨ 'Input 'Sprinkler 1" is linked to the input.

To link 'Input 'Sprinkler 2", proceed in the same way.



'Assign dialog' window for linking 'Referenced flow switch zone'

To link 'Referenced flow switch zones', proceed as follows:

1. Highlight 'Referenced flow switch zones '.
2. In the 'Assign dialog' window, select a 'Flow switch zone' and click on the 'Assign' button.

⇨ 'Referenced flow switch zones' is linked to 'Flow switch zone'.

See also

Flow rate indicator zone [→ 86]

8.2.5.2 Extinguishing system zone

Extinguishing systems are actuated and monitored by the autonomous extinguishing control panel. In the fire detection installation, there is an interface to the extinguishing control panel which makes it possible to send extinguishing control panel events to the fire control panel, and to transmit commands from the fire control panel to the extinguishing control panel. Input/output module FDCIO222 is used as an interface.

The inputs and outputs of the FDCIO222 are linked with the corresponding sub-elements of the element 'XC10 zone'.

Creating 'XC10 zone' element

Create the 'XC10 zone' element in the 'Detection' task card.

Linking the display signals

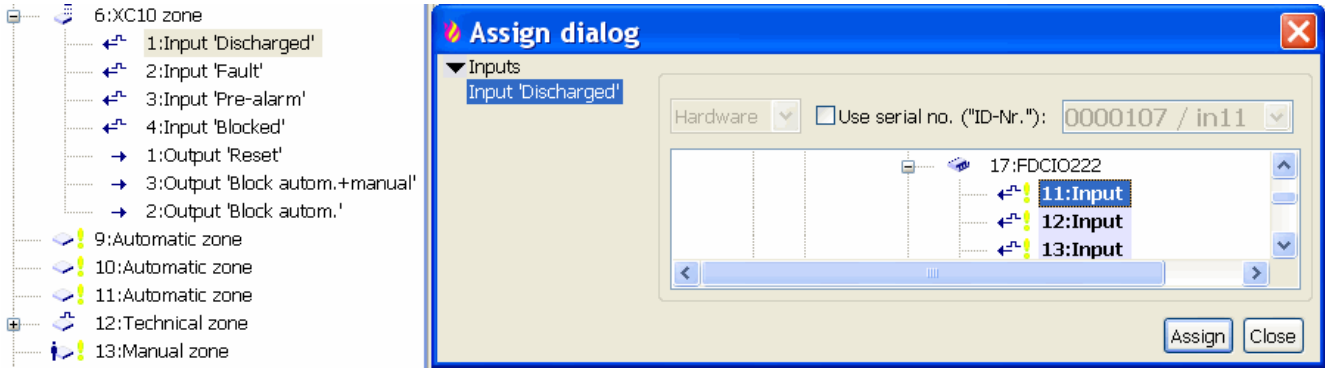
Sub-element of 'XC10 zone'	'Input' at FDCIO222	Description
Input 'Discharged'	IN1	The extinguishing control panel detects the activation or resetting of the extinguishing by activating or deactivating 'IN1'. The activation is indicated on the FC720 Person Machine Interface as an alarm and AVC started (processing as for manual fire alarm). The display 'Exting. discharged' appears on the Person Machine Interface when 'IN1' is activated. The display does not disappear automatically when 'IN1' is deactivated, i.e. when a reset is made on the extinguishing control panel. The display has to be acknowledged and reset on the FC720 Person Machine Interface.
Input 'Fault'	IN2	The extinguishing control panel detects the occurrence or disappearance of the fault condition by activating or deactivating 'IN2'. The occurrence of the fault condition is indicated on the FC720 Person Machine Interface as 'Fault'. Troubleshooting is just the same as for automatic fire detector faults. The fault display appears on the FC720' Person Machine Interface when 'IN2' is activated. It does not disappear automatically when 'IN2' is deactivated, i.e. when the indication at the extinguishing control panel disappears. The display has to be acknowledged on the Person Machine Interface.
Input 'Pre-alarm'	IN3	The extinguishing control panel detects the activation or resetting of the extinguishing pre-alarm by activating or deactivating 'IN3'. The activation is indicated on the FC720' Person Machine Interface as an alarm and AVC started (processing as for automatic fire alarm). The display 'Exting. pre-alarm' appears on the Person Machine Interface when 'IN3' is activated. It does not disappear automatically when 'IN3' is deactivated, i.e. when a reset is made on the extinguishing control panel. The display has to be acknowledged and reset on the FC720 Person Machine Interface.
Input 'Blocked'	IN4	The extinguishing control panel detects the simultaneous blocking or releasing of automatic and manual extinguishing by activating or deactivating 'IN4'. The blocking is indicated as isolation on the FC720 Person Machine Interface. The display 'Aut. ext.OFF XC' appears on the PMI when 'IN4' is interrupted while 'OUT B' is inactive. The display 'Aut. ext.OFF FC' appears on the PMI when 'IN4' is interrupted while 'OUT B' is active. This only applies when the 'Autom. exting. release blockable from FS720' function is configured. The display 'Aut+man ext.OFF XC' appears on the PMI when 'IN4' is activated while 'OUT C' is inactive. The display 'Aut+man ext.OFF FC' appears on the PMI when 'IN4' is activated while 'OUT C' is active. This only applies when the 'Autom.+manual exting. release blockable from FS720' function is configured.

Linking the control signals

Sub-element of 'XC10 zone'	'Output' at FDCIO222	Description
Output 'Reset'	OUT A	FC720 resets the extinguishing detected by 'IN1' and/or 'IN3' by pressing the 'Reset' button. This command activates 'OUT A' for 3 seconds (default). The extinguishing control panel reports the successful reset by deactivating 'IN1' and/or 'IN3'. If these inputs are not deactivated within 10 seconds, FC720 displays the text 'XC10 n. resettable' for 60 seconds. The reset function is only possible when the 'Resettable from FS720' property is activated.
Output 'Block autom.'	OUT B	FC720 blocks automatic extinguishing when the user selects one or more extinguishing sectors in the Person Machine Interface display and presses the softkey 'Autom. exting. OFF'. This command activates 'OUT B' for all selected extinguishing sectors. If 'IN4' is not interrupted by the extinguishing control panel within 10 seconds, 'OUT B' is deactivated again and FC720 displays the text 'XC10 not blockable'. If 'IN 4' is interrupted by the extinguishing control panel within 10 seconds, 'OUT B' remains active until the blocking on the FC720 Person Machine Interface is released again.
Output 'Block autom.+manual'	OUT C	FC720 blocks automatic and manual extinguishing when the user selects one or more extinguishing sectors in the Person Machine Interface display and presses the softkey 'Autom. exting. OFF'. This command activates 'OUT C' for all selected extinguishing sectors. If 'IN4' is not activated by the extinguishing control panel within 10 seconds, 'OUT C' is deactivated again and FC720 displays the text 'XC10 not blockable'. If 'IN 4' is activated by the extinguishing control panel within 10 seconds, 'OUT C' remains active until the blocking on the FC720 Person Machine Interface is released again.

In accordance with standards, the outputs are not permitted or only permitted in exceptional situations. These functions are therefore deactivated by default in the detail editor.

Linking input or output

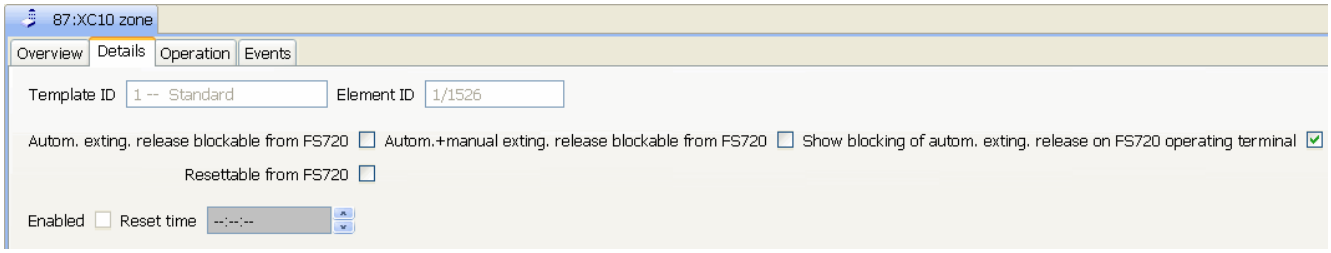


'Assign dialog' window for linking an input or output to a sub-element of the 'Extinguishing system zone'

1. Select the 'Detection' task card.
2. Open 'XC10 zone' in the tree view.
3. In 'XC10 zone', highlight an element, e.g., 'Input 'Discharged"'.
4. Open the 'Assign dialog' window.
5. Select the corresponding input and click on the 'Assign' button.

⇨ 'Input 'Discharged" is linked to the input.

Properties of the 'XC10 zone' element



Detail editor of 'Extinguishing system zone' element, 'Details'

In the detail editor of the 'XC10 zone' element, the following properties can be selected:

- 'Autom. exting. release blockable from FS720'

  Defines whether the automatic extinguishing release of the extinguishing control can be blocked from the FS720 operating terminal.

- 'Autom.+manual exting. release blockable from FS720'

  Defines whether the automatic and manual extinguishing release of the extinguishing control can be blocked from the FS720 operating terminal.

- 'Show blocking of autom. exting. release on FS720 operating terminal'

  Defines whether blocking of the automatic extinguishing release of the extinguishing control panel is displayed on the FS720 operating terminal.

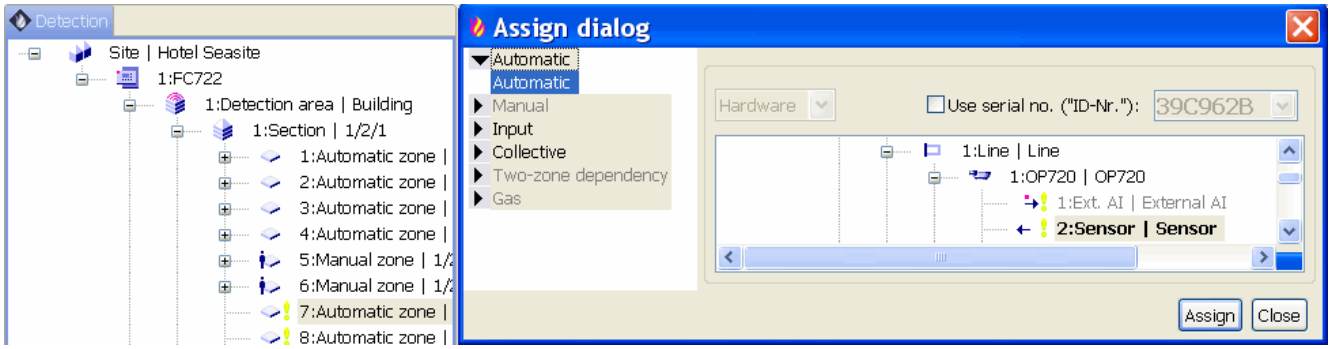
- 'Resettable from FS720'

  Defines whether the extinguishing control can be reset from the FS720 operating terminal.

- 'Reset time'

  'Resettable from FS720' must be activated in order to allow the reset time to be set.
  Defines the period for which the system attempts to reset the element before the attempt is considered a failure. Normally, the suitable reset time is set by the control panel. But this is not always possible if sub-systems are activated. In this case, the user can determine the appropriate reset time of between 1 second and 5 minutes.

8.2.6 Linking detection tree with hardware tree



Assigning sensor to a zone

To link the Detection tree to the Hardware tree, proceed as follows:

1. Select the 'Detection' task card.
2. Open 'Detection area' > 'Section' in the tree view.
3. Highlight 'Zone' or 'Physical channel', if pre-configuration has been carried out up to this level.
4. Open the 'Assign dialog' window.

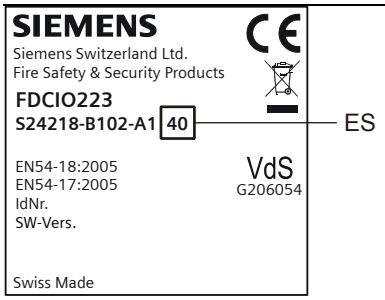
   ⇨ The hardware tree is depicted in the 'Assign dialog' window. The elements that can be linked are highlighted.
5. Mark the corresponding sensor.
6. Click on the 'Assign' button.

⇨ 'Zone' is linked to the sensor.

8.2.7 Collective line via input/output module FDCIO223

The input/output module FDCIO223 is operated on the C-NET and features two inputs/outputs. 1 to 2 collective lines can be connected to this.

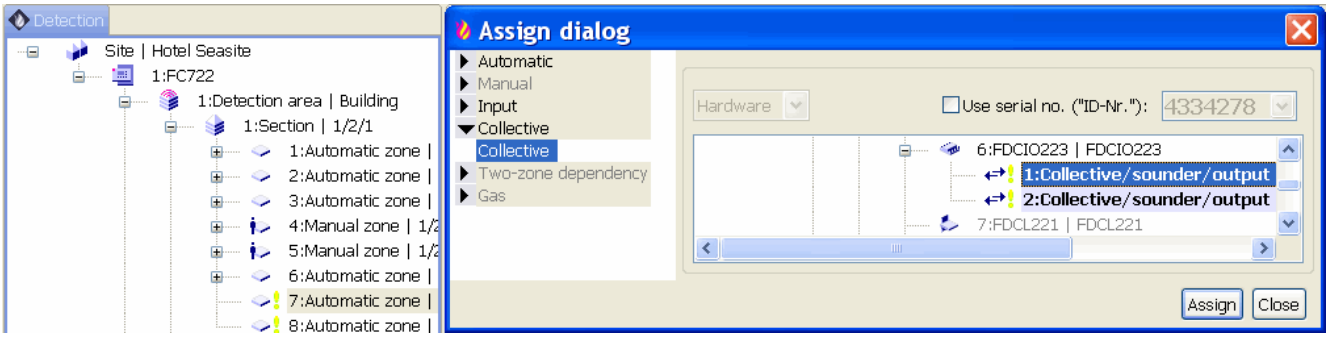
Mixed operation with a sounder line or a control line without confirmation is permitted if the product version of the input/output module FDCIO223 is 40 or higher.



Type plate of input/output module

Linking the collective line

The collective line of the input/output module FDCIO223 is linked to the logical channel of the selected detector zone via the Assign function.



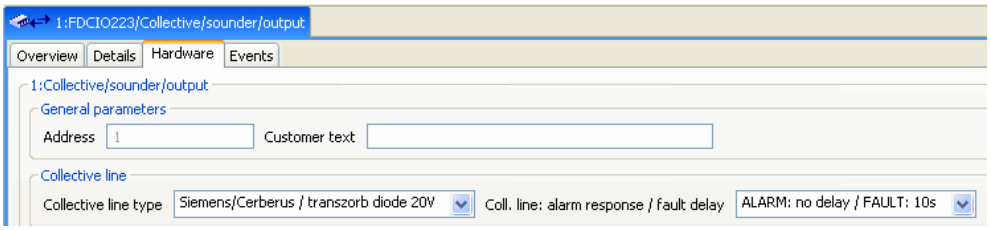
Task card 'Detection' with window 'Assign dialog'

To link the collective line with the detector zone, proceed as follows:

1. Select the 'Detection' task card.
2. Open the 'Station' in the tree view.
3. Highlight 'Section' (if available) or 'Detection area'.
4. Highlight the detector zone in the tree view.
5. Open the 'Assign dialog' window.
6. Highlight 'Assign dialog' 'Collective' at the left of the window.
   ⇨ The input/output module FDCIO223 opens in the Hardware tree.
7. Highlight 'Collective/sounder/output' and click on the 'Assign' button.

⇨ 'Automatic zone' is linked to the 'Collective/sounder/output' input.

Configuring the collective line



Detail editor 'Collective/sounder/output', 'Hardware'

The following properties can be set:

- 'Collective line type':

  Choice of type of connected collective line (type of evaluation, end-of-line unit).

- 'Coll. line: alarm response / fault delay':

  Choice of alarm response time (settings of alarm verification inside the device) and the fault delay time of the collective line.

The settings for the collective line are also visible in the detail editor of the 'Hardware' task card, under the 'Overview' button.

For details about the input/output module see 'document 009122, Technical manual.

8.2.8 Redux module [DE]

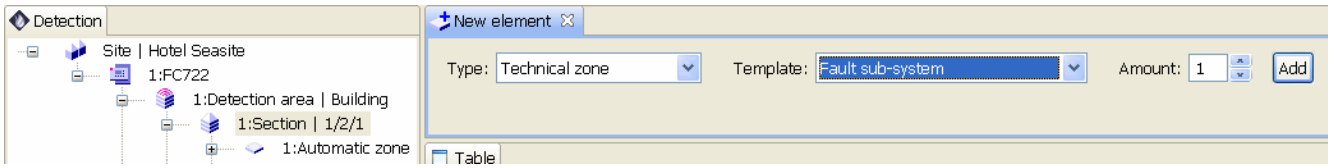
The Redux module serves for data transmission and power supply redundancy of a fire department indication panel (FAT).

The data cable is connected to the control panel's RS485 interface.

In the event of a failure of one of the connection lines to the FAT due to a short-circuit or open line, the complete functionality is ensured. The line fault is signaled by the fault relay of the Redux module which drops in case of a fault.

The fault output of the Redux module is wired to an input of the periphery board and linked to a technical zone of type 'Fault sub-system'.

Creating technical zone

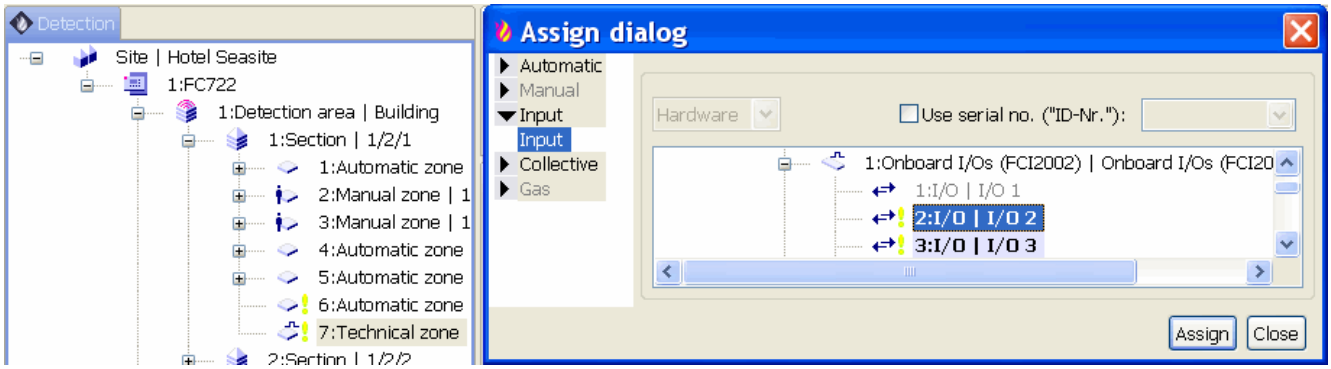


Creating technical zone 'Fault sub-system'

1. Select the 'Detection' task card.
2. Open the 'Station' in the tree view.
3. Highlight 'Section' (if available) or 'Detection area'.
4. In the 'New element' window, select 'Technical zone' in the 'Type:' field and 'Fault sub-system' in the 'Template:' field.
5. Enter the number of zones required in the 'Amount:' field.
6. Click on the 'Add' button.

   ⇨ The 'Fault sub-system' technical zone is created.
7. Enter the customer text(s).

Linking technical zone



Linking technical zone 'Fault sub-system'

1. Highlight the 'Technical zone' zone.
2. Open the 'Assign dialog' window.
   ⇨ 'Input' is highlighted and the Hardware tree opens. The elements that can be linked are highlighted.
3. Highlight the relevant 'Onboard I/Os' and click on the 'Assign' button.

⇨ 'Technical zone' is linked to the 'I/O'.

8.3 'Controls' task card

The following logical elements of the control tree are shown in the 'Control' task card:

- Alarming control group

  Controls for internal and external sounders and remote transmission outputs for Fire and Fault.

- Evacuation control group

  Controls for alarm and announcement devices.

- Fire control group

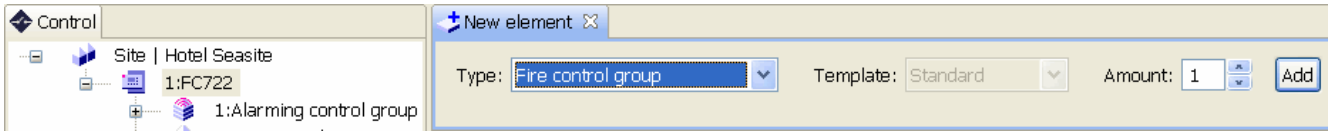
  Controls for building equipment.

- Counter control group

  Registration of fire alarms and test activities.

Each zone has one or more control elements including one or more inputs (Cause) and one or more outputs (Effect).

8.3.1 Control tree



Task card 'Control' with the tree view and window 'New element'

To create the Control tree, proceed as follows:

1. Select the 'Control' task card.
2. Highlight the 'Station' in the tree view.
3. Open the 'New element' window.
4. In the 'Type:' field, select a 'Control group'.
5. Enter the number of elements required in the 'Amount:' field.
6. Click on the 'Add' button.

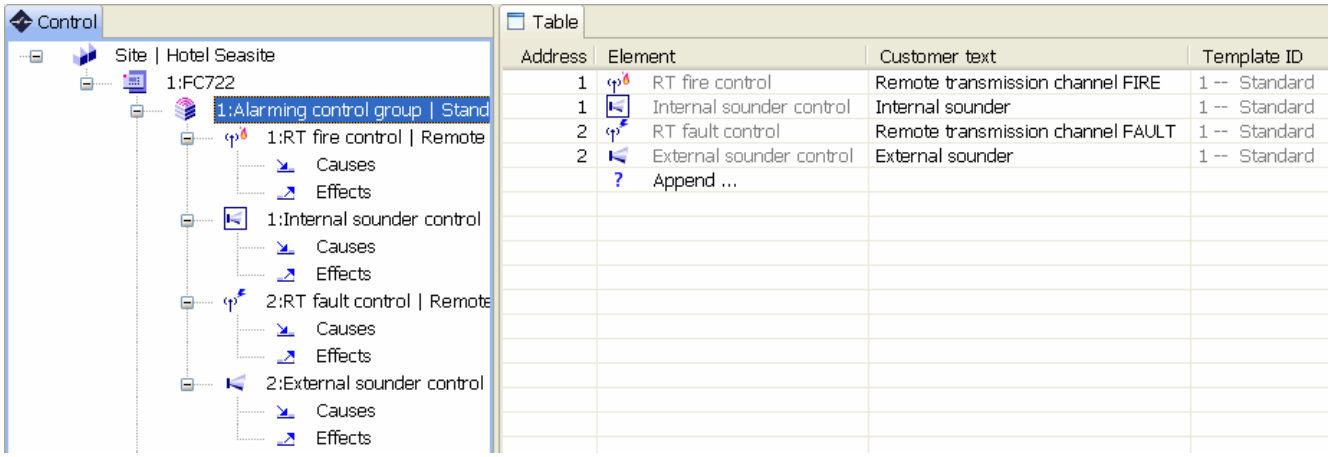
   ⇨ The elements are created.
7. Enter the customer texts.
8. Highlight 'Control group' in the tree view.
9. Select an element in the 'Type:' field of the 'New element' window.
10. Enter the number of elements required in the 'Amount:' field.
11. Click on the 'Add' button.

    ⇨ The elements are created.
12. Enter the customer text(s).

8.3.2 Alarming control group

The alarming control group includes the following control elements:

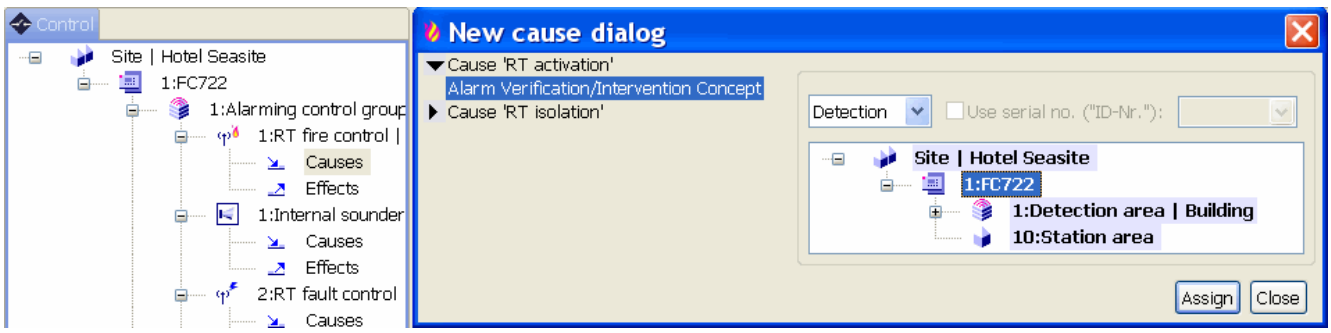
- 'Internal sounder control'
- 'External sounder control'
- 'RT fire control'
- 'RT fault control'
- 'RT 1 control' to 'RT 8 control'
- 'RT device control'



Alarming control group

- The causes of the elements are linked to the event verification of the station.
- The effects of the different 'RT' elements are linked to the corresponding on-board I/Os, the fire department periphery module or the I/O card (programmable). A confirmation input can be assigned to the effects.
- The effects of the 'Sounder' elements can be linked to the base sounder or loop sounder on the C-NET line or to the corresponding on-board I/Os, the fire department periphery module, or the I/O card (programmable).
- A fault input and a confirmation input can be assigned to the 'RT device control'.

Linking cause

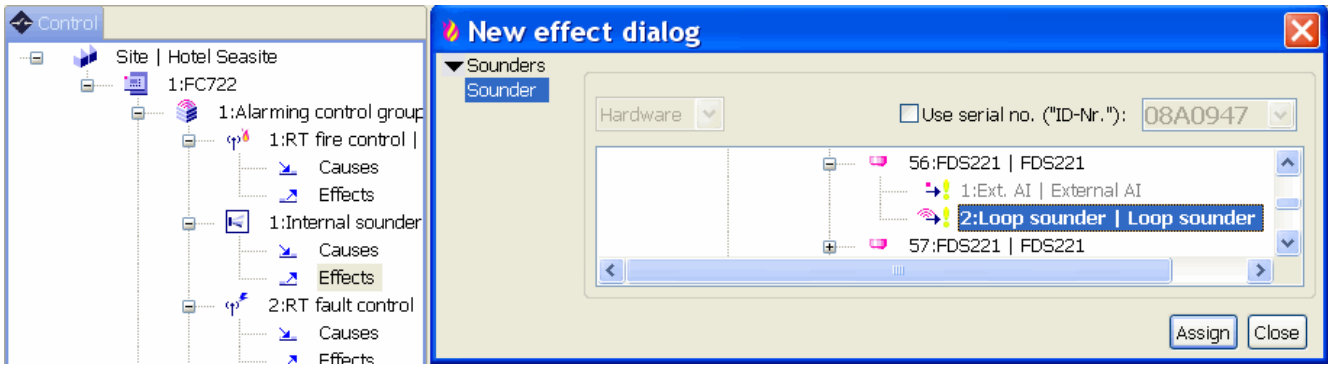


Task card 'Control' with the tree view and window 'Assign dialog'

1. Select the 'Control' task card.
2. Open the 'Station' in the tree view.
3. Highlight 'Causes' in a control element of the 'Alarming control group'.
4. Open the 'Assign dialog' window.
5. In the window click an event category and select the cause from the list.
   ⇨ The appropriate tree is shown in the right side of the window. The elements that can be linked are highlighted.
6. Select the appropriate ID No. or open the tree and select the corresponding element.
7. Click on the 'Assign' button.

⇨ 'Causes' is linked to the element.

Linking effect



Task card 'Control' with the tree view and window 'Assign dialog'

1. Select the 'Control' task card.
2. Open the 'Station' in the tree view.
3. Highlight the 'Effects' element in a control element of the 'Alarming control group'.
4. Open the 'Assign dialog' window.
5. Click an output with or without confirmation on the left in the window.
   ⇨ The hardware tree is depicted on the right in the window. The elements that can be linked are highlighted.
   ⇨ In the case of an output with confirmation, a second Hardware tree opens for linking the confirmation input.
6. Select the appropriate ID No. (outputs only) or open the tree and select the corresponding element.
7. Click on the 'Assign' button.

⇨ 'Effects' is linked to the element.

8.3.2.1 Automatically isolating remote transmission

If remote transmission is active, under certain circumstances this can be isolated automatically.

There are two ways of doing this:

- 'Access level <> default level': Remote transmission is automatically deactivated when the current access level of an assigned Person Machine Interface (PMI) corresponds to at least the configured level.
- 'All activations': The activated remote transmission function is automatically deactivated when an input for any control (e.g., a door contact) changes status.

'Access level <> default level'

Window 'Assign dialog' with the event category 'RT isolation, Access level > 1'

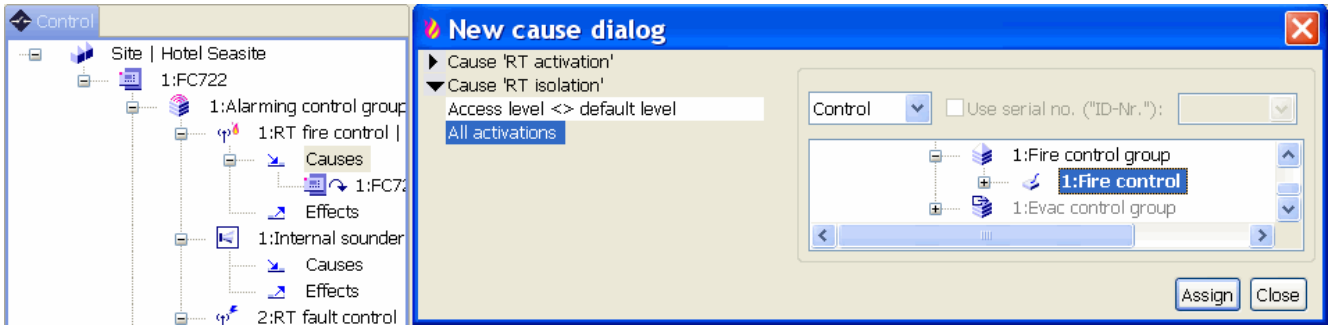
To assign a Person Machine Interface (PMI) to the cause, proceed as follows:

1. Select the 'Control' task card.
2. Open the 'Station' in the tree view.
3. Highlight the 'Causes' element in an 'RT' element of the 'Alarming control group'.
4. Open the 'Assign dialog' window.
5. In the window, click on the 'Cause 'RT isolation" > 'Access level <> default level' event category and select the 'Operation' task card from the dropdown list field.

   ⇨ The corresponding PMI is highlighted in the window on the right.
6. Click on the 'Assign' button.

   ⇨ PMI is linked to 'Causes'.
7. Highlight the linked PMI element in the tree view.
8. In the 'Required access level' field of the detail editor, determine the minimum access level that must be reached for remote transmission to be deactivated.

'All activations'



'Assign dialog' window with the 'RT isolation, all activations' event category

To attain automatic isolation by any control, proceed as follows:

1. Select the 'Control' task card.
2. Open the 'Station' in the tree view.
3. Highlight the 'Causes' element in an 'RT' element of the 'Alarming control group'.
4. Open the 'Assign dialog' window.
5. In the window, click on 'Cause 'RT isolation" > 'All activations' and select the 'Control' task card from the dropdown list field.

   ⇨ The corresponding 'Fire control' elements are displayed at the right of the window.
6. Select the corresponding element and click on the 'Assign' button.

   ⇨ 'Fire control' is linked to 'Causes'.
7. In the tree view, highlight the 'Fire control' link and use the hyperlink in the detail editor to navigate to the original 'Fire control' element.
8. Link its cause with the corresponding input.

8.3.3 Evacuation control group

The evacuation control group makes it possible to program a complete evacuation function for each alarm device group, e.g. on one floor. Two function blocks are available for each control:

- Alert

  The linking of all conditions, so that the corresponding alarm devices transmit a warning signal.

- Evac

  The linking of all conditions, so that the corresponding alarm devices transmit an evacuation signal.

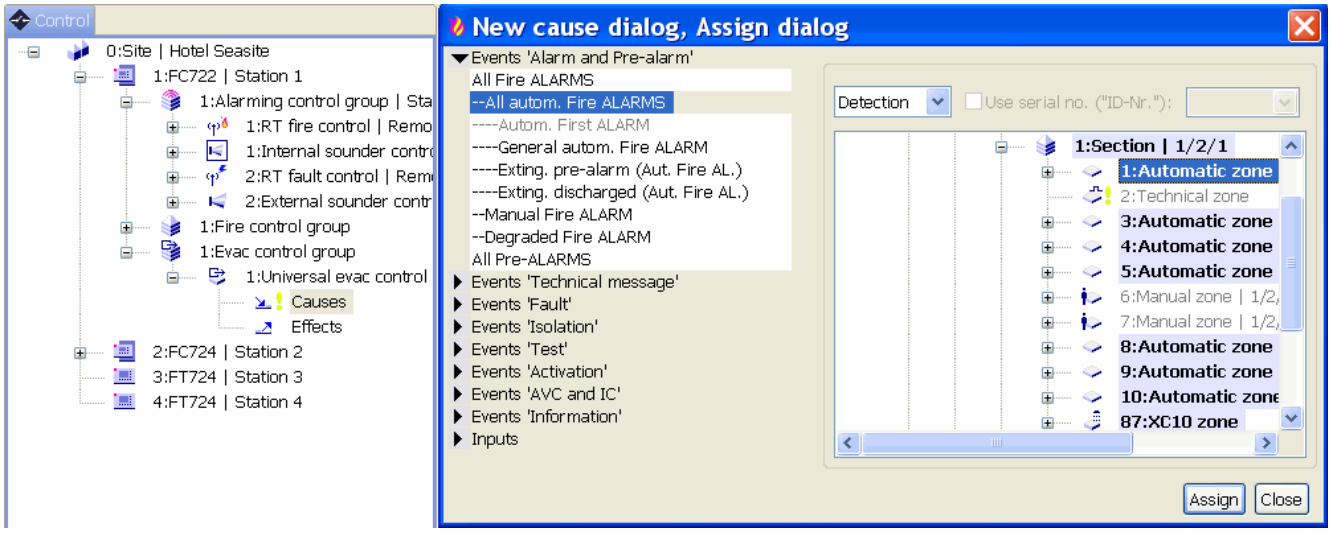
Events in the Station, the Detector lines, the Section, or the Zone (cause) initiate evacuation control.

The evacuation control group unites the following evacuation control elements:

- 'Universal evac control'
- 'Phased evac control'

8.3.3.1 Cause of element 'Universal evac control'

The graphic below shows the event categories that can be linked with an element of the hardware tree, detection tree or control tree.



Window 'Assign dialog' with the event category 'All autom. Fire ALARMS'

To link the cause, proceed as follows:

1. Select the 'Control' task card.
2. Open 'Station' > 'Evac control group' in the tree view.
3. In 'Universal evac control', highlight the 'Causes' element.
4. Open the 'Assign dialog' window.

5. Click on an event category in the left of the window and select an event from the list.
6. In the right of the window, select the tree and mark the corresponding highlighted element in it.
7. Click on the 'Assign' button.

⇨ 'Causes' is linked to the element.

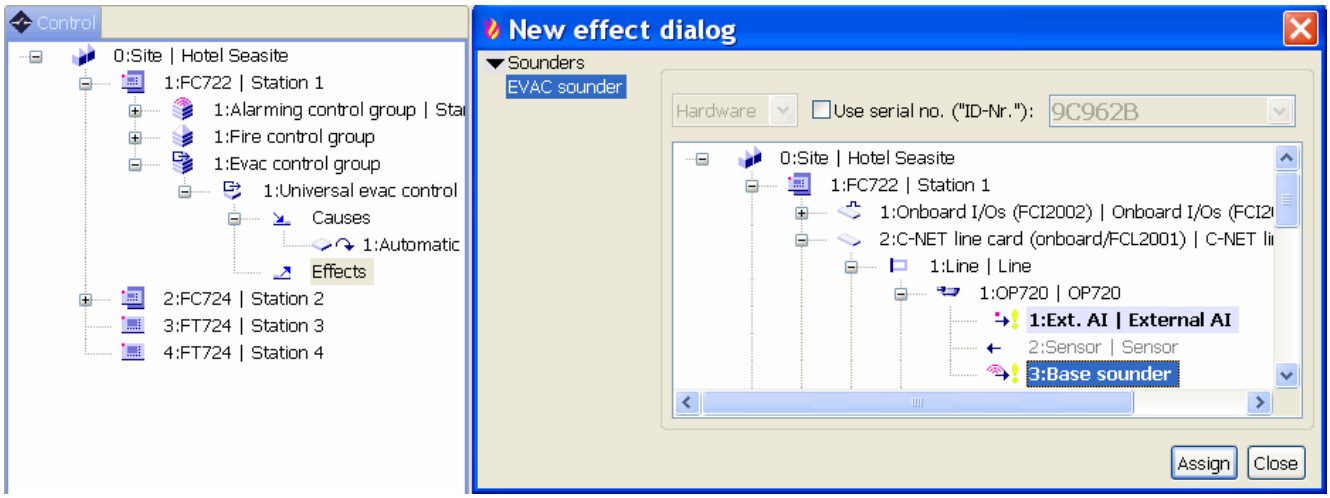
Event category	Cause	Link with
Outputs with confirmation	All Fire ALARMS '--All autom. Fire ALARMS '----Autom. First ALARM '----General autom. Fire ALARM '----Exting. pre-alarm (Aut. Fire AL.) '----Exting. discharged (Aut. Fire AL.) '--Manual Fire ALARM All Pre-ALARMS	Hardware tree Detection tree
	'--Degraded Fire ALARM	Hardware tree
Events 'Technical message'	All technical messages	Detection tree Operation tree
Events 'Fault'	All faults '--Other fault '--All system faults '----System fault: general connection fault '----System fault: module '----Other system fault '--Mains failure '--Battery failure '--Emergency power operation	Hardware tree Detection tree Control tree Operation tree Network tree
Events 'Isolation'	All isolations '--Other isolation '--Temporary isolation '--Alarm evaluation OFF '--Sub-system isolation '--Automatic extinguishing release OFF '--Autom.+man. extinguishing release OFF '--Renovation mode ''--Not ready '--Fire related controls OFF '--RT FIRE channels OFF '--Sounders OFF	Detection tree

Event category	Cause	Link with
Events 'Test'	All test modes '--Detector test mode '--Installation test mode '--Control test mode All test activations '--Test activation ALERT '--Test activation EVAC '--Other test activation	Detection tree Control tree
Events 'Activation'	All activations '--Activation/ALERT '--Activation/EVAC '--Other activation '--Activation/confirmed '--Activation/NOT active '--Activation/unexpected	Detection tree Control tree Operation tree
Events 'AVC and IC'	AVC, Fire ALARM AVC, Pre-ALARM	Detection tree
	IC, Technical IC, Fault IC, Isolation IC, Test IC, Activation IC, Information	Station
Events 'Information'	Manned operation Unmanned operation Service information: Service required Access level <> default level '--Access level 1 '--Access level 2.1 '--Access level 2.2 '--Access level 3 Expiry reminder of time lim. isol. Other information Visibility	Hardware tree Detection tree
Inputs	• Input	• Hardware tree

Events which can be assigned

8.3.3.2 Effect of element 'Universal evac control'

The effect is linked with the corresponding hardware (outputs, alarm devices). The alarm devices know only one operating mode, EVAC.



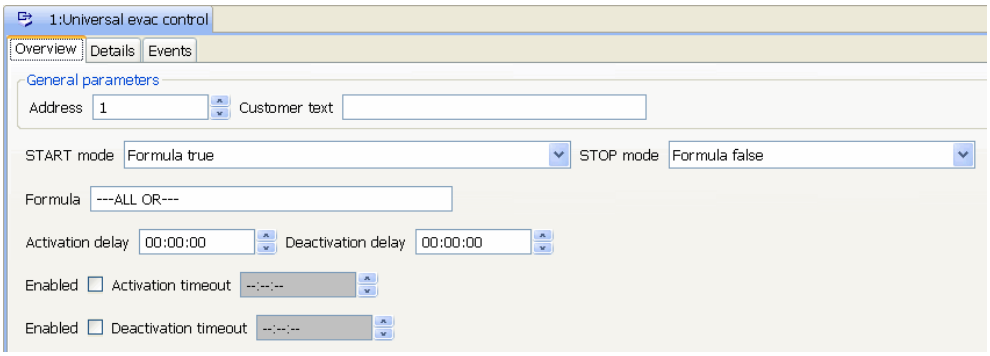
Window 'Assign dialog' for linking a sounder

To link the effect, proceed as follows:

1. Select the 'Control' task card.
2. Open 'Station' > 'Evac control group' in the tree view.
3. In 'Universal evac control', highlight the 'Effects' element.
4. Open the 'Assign dialog' window.
   ⇨ The 'EVAC sounder' command is highlighted, and the hardware tree is displayed at the right of the window.
5. Mark the corresponding highlighted element in the tree.
6. Click on the 'Assign' button.

⇨ 'Effects' is linked to the element.

8.3.3.3 Properties of element 'Universal evac control'



Detail editor 'Universal-evac control', 'Overview'

The properties shown in the following tables can be set in the detail editor of the 'Universal evac control' element.

Formula

Cause	Formula
Inputs and events	● Operators for the link: – OR = '+' – AND = '*' – NOT = '–'. ● Mixed application is possible when brackets are used

Formula for linking causes

Several causes can be linked with a formula:

'1 * (2 + 3)' means '1 AND (2 OR 3)'.

If no formula has been defined, all causes are linked with the OR function.

START mode

Start mode
Undefined (no autom. activation)
Formula true
Value rising and >= threshold (all causes OR-combined)

Start conditions for the activation of an effect

- The START mode indicates how the control shall be activated.

STOP mode

Stop mode
Undefined (no autom. deactivation)
Formula false
All causes inactive

Stop conditions for the deactivation of an effect

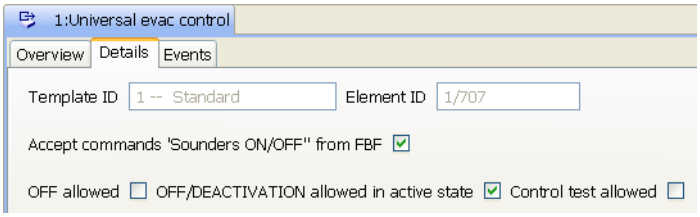
- The STOP mode indicates how the control shall be deactivated.

Additional functions

Function	Settings
Activation delay	0 to 30 minutes
Deactivation delay	0 to 30 minutes
Activation timeout	1 second to 30 minutes (default 5 minutes)
Deactivation timeout	1 second to 30 minutes (default 5 minutes)

Delays and timeout

- 'Activation delay': Activation of the control is delayed by the set time when the start conditions are met.
- 'Deactivation delay': Deactivation of the control is delayed by the set time when the stop conditions are met.
- 'Activation timeout': This is started when the control is activated. After the expiry of the set time the control is deactivated again automatically.
- 'Deactivation timeout': This is started when the control is deactivated. After the expiry of the set time the control is activated again automatically.



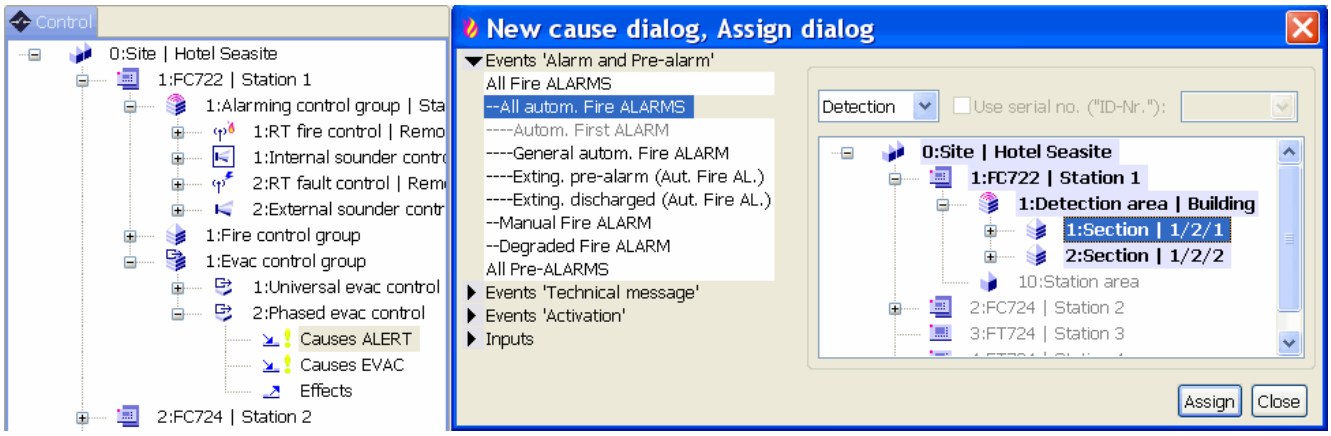
Detail editor 'Universal evac control', 'Details'

The following properties can be selected:

- Accept commands 'Sounders ON/OFF" from FBF: If the checkmark is placed, the effects of the sounder control relating to the corresponding area are switched off or on by the FBF function.
- OFF allowed: If the checkmark is placed, the control can be switched off by an operating command.
- OFF/DEACTIVATION allowed in active state: If the checkmark is placed, the control can be switched off or deactivated when the control is in active status.
- Control test allowed: If the checkmark is placed, the control can be switched to 'Control test' by an operating command.

8.3.3.4 Cause of element 'Phased evac control'

The 2-stage evacuation has separate causes for ALERT and EVAC. The graphic below shows the event categories that can be linked to an element of the hardware tree, detection tree, or control tree.



Window 'Assign dialog' with the event category 'All autom. Fire ALARMS'

To link 'Causes ALERT' or 'Causes EVAC', proceed as follows:

1. Select the 'Control' task card.
2. Open 'Station' > 'Evac control group' in the tree view.
3. In 'Phased evac control', highlight the 'Causes ALERT' or 'Causes EVAC' element.
4. Open the 'Assign dialog' window.
5. Click on an event category in the left of the window and select an event from the list.
6. In the right of the window, select the tree and mark the corresponding highlighted element in it.
7. Click on the 'Assign' button.

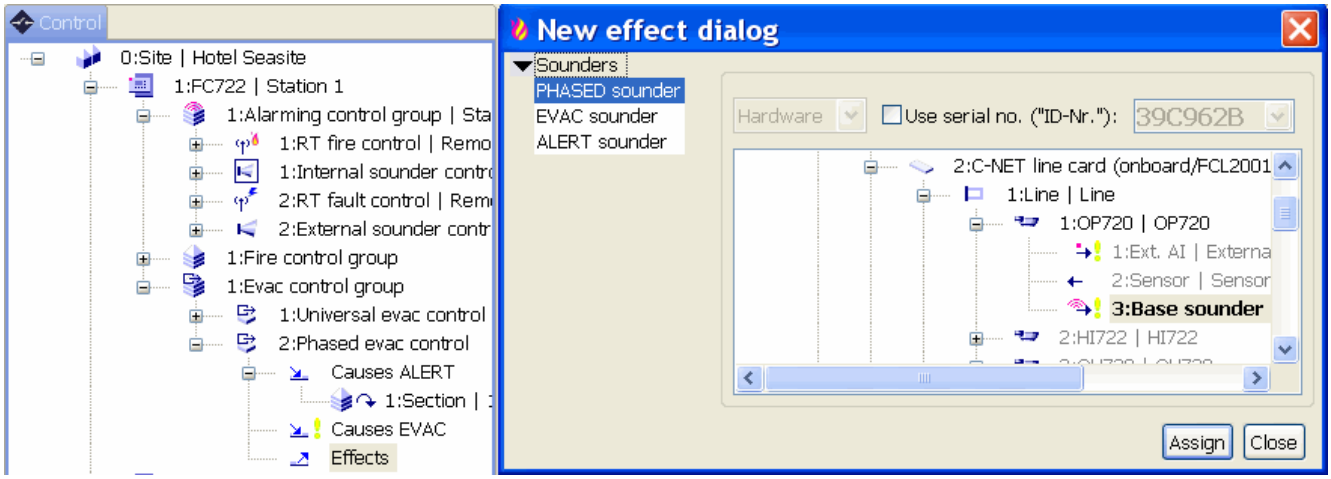
⇨ 'Causes' is linked to the element.

Event category	Cause	Link with
Events 'Alarm and Pre-alarm'	• 'All Fire ALARMS' • "--All autom. Fire ALARMS' • '----General autom. Fire ALARM • '----Exting. discharged (Aut. Fire AL.) • '----Exting. pre-alarm (Aut. Fire AL.) • '--Manual Fire ALARM • '--Degraded Fire ALARM • All Pre-ALARMS	• Detection tree • Hardware tree • Control tree
Events 'Technical message'	• All technical messages	• Detection tree • Hardware tree
Events 'Activation'	• All activations	• Detection tree • Control tree
Inputs	• Input	• Hardware tree

Overview of events

8.3.3.5 Effect of element 'Phased evac control'

The effect is linked with the corresponding hardware (sounders). Different tonalities can be selected for the warning (ALERT) and evacuation (EVAC) for the sounder.



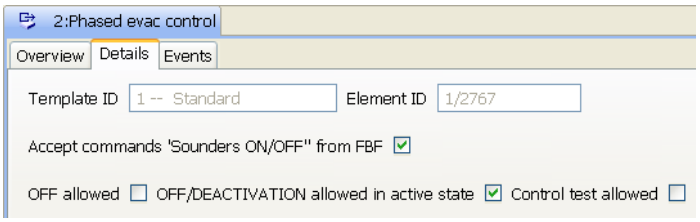
Window 'Assign dialog' for linking a sounder

To link the effect, proceed as follows:

1. Select the 'Control' task card.
2. Open 'Station' > 'Evac control group' in the tree view.
3. In 'Phased evac control', highlight the 'Effects' element.
4. Open the 'Assign dialog' window.
   ⇨ The 'EVAC sounder' command is highlighted, and the hardware tree is displayed at the right of the window.
5. Mark the corresponding highlighted element in the tree.
6. Click on the 'Assign' button.

⇨ 'Effects' is linked to the element.

8.3.3.6 Properties of element 'Phased evac control'



Detail editor 'Phased evac control', 'Details'

The following properties can be selected:

- Accept commands 'Sounders ON/OFF" from FBF: If the checkmark is placed, the effects of the sounder control relating to the corresponding area are switched off or on by the FBF function.
- OFF allowed: If the checkmark is placed, the control can be switched off by an operating command.
- OFF/DEACTIVATION allowed in active state: If the checkmark is placed, the control can be switched off or deactivated when the control is in active status.
- Control test allowed: If the checkmark is placed, the control can be switched to 'Control test' by an operating command.

8.3.3.7 2-stage evacuation, special case [GB]

Evacuation is undertaken in two stages. First, all floors are warned (ALERT). After that, the evacuation (EVAC) of individual floors is performed at particular intervals (phases), starting with the floor on which the seat of fire is located, in order to prevent a blocking of the escape routes.

- In the first phase the floor on which the fire is located as well as the one above and the two top floors, all basement floors and possibly the ground floor are evacuated.
- In additional phases, one upper and one lower floor are also evacuated at predefined intervals. If need be, additional floors can be evacuated during the same phase.

Floor	Stages of evacuation											
	UG	EG	1. Floor	2. Floor	3. Floor	4. Floor	5. Floor	6. Floor	7. Floor	8. Floor	9. Floor	10. Floor
UG	1	1	2	2	3	3	4	4	5	5	1	1
EG	1	1	1	2	2	3	3	4	4	5	1	1
1. Floor	1	2	1	1	2	3	3	4	4	5	1	1
2. Floor	1	3	2	1	1	2	3	4	4	5	1	1
3. Floor	1	4	3	2	1	1	2	3	4	5	1	1
4th floor	*1*	*5*	*4*	*3*	*2*	*1*	*1*	*2*	*3*	*4*	*1*	*1*
5. Floor	1	5	4	4	3	2	1	1	2	3	1	1
6. Floor	1	5	4	4	3	3	2	1	1	2	1	1
7. Floor	1	5	4	4	3	3	2	2	1	1	1	1
8. Floor	1	5	5	4	4	3	3	2	2	1	1	1
9. Floor	1	5	5	5	4	4	3	3	2	2	1	1
10. Floor	1	1	2	2	3	3	4	4	5	5	1	1

Sequence of the 2-phased evacuation

UG	Basement
EG	Ground floor
Floor	Floor
1 - 5	Phases of evacuation

Evacuation if fire breaks out on the 4th floor:

- Phase *1*: 4th floor, 5th floor, 9th floor, 10th floor, and basement
- Phase *2*: 3rd floor, 6th floor
- Phase *3*: 2nd floor, 7th floor
- Phase *4*: 1st floor, 8th floor
- Phase *5*: EG

Configuration example for the 2-phase evacuation control element

▷ Each floor is represented by one section.

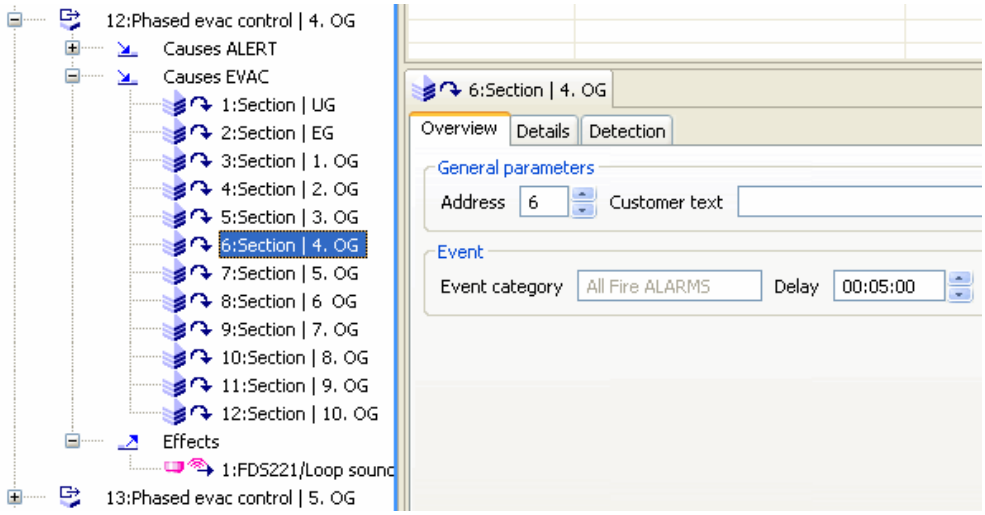
▷ Each floor is equipped with a combined 'ALERT sounder'/'EVAC sounder'.

1. Create the 'Phased evac control' element for each floor.
2. In the first 'Phased evac control', highlight the 'Causes ALERT' element.
3. Link 'Causes ALERT' with all sections. Leave the delay times of the sections at '00:00:00' as immediate warning is required on each floor.
4. Use multiselection to select all sections and use the 'Copy' function to copy them.
5. Highlight 'Causes EVAC' and insert the sections using the 'Paste' function.

6. Repeat the 'Paste' function for each 'Causes ALERT' and 'Causes EVAC' element in each 'Phased evac control' element.

7. Configure the delay times for evacuation:
   For the example above, open 'Phased evac control/4th floor' > 'Causes EVAC'.
   For phase 1, highlight 'Section/4th floor', 'Section/5th floor', 'Section/9th floor', 'Section/10th floor', and 'Section/basement' one after the other, and set the delay time to 5 minutes in each case.
   For phase 2, highlight 'Section/3rd floor' and 'Section/6th floor' one after the other and set the delay time to 10 minutes in each case.
   Continue this process up to phase 5.

8. Using this method and referring to the table above, configure the delay times for evacuation for each 'Phased evac control' element.



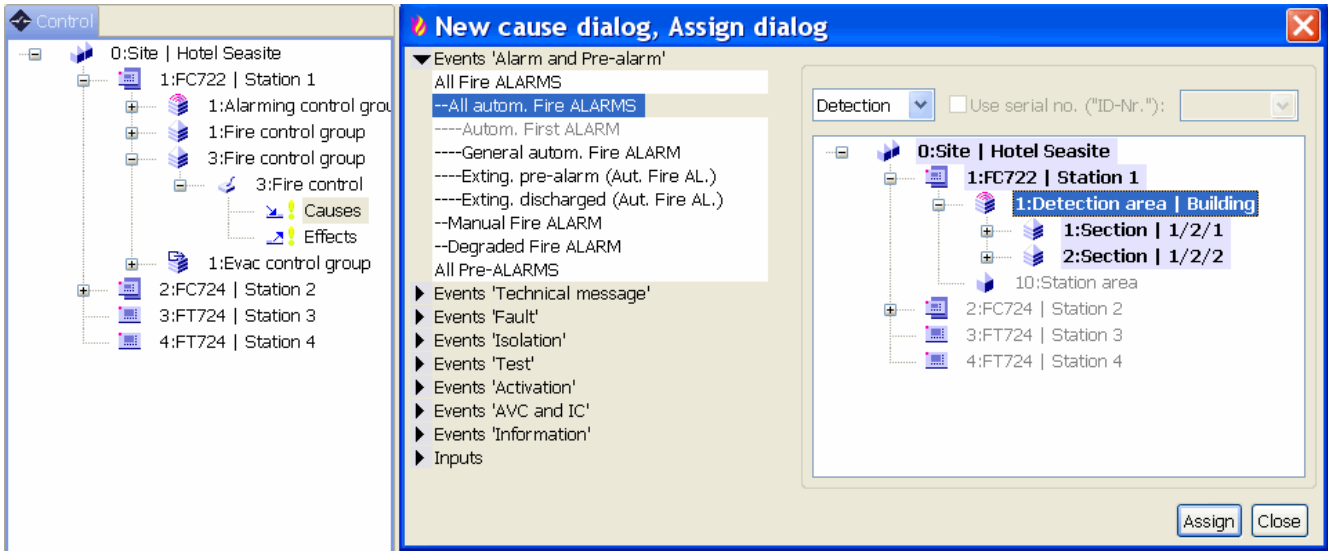
Task card 'Control', 'Phased evac control' with detail editor 'Section', 'Overview'

8.3.4 Fire control group

The fire control group unites several fire control elements. In the fire control, one or more 'Input' elements are created in the cause. An event can be assigned to this. The executing element is assigned to the effect of the 'Fire control' element.

8.3.4.1 Cause of element 'Fire control'

The graphic below shows the event categories that can be linked to an element of the hardware tree, detection tree, or control tree.



Window 'Assign dialog' with the event category 'All autom. Fire ALARMS'

To link a cause, proceed as follows:

1. Select the 'Control' task card.
2. Open the 'Station' in the tree view.
3. In 'Fire control', highlight the 'Causes' element.
4. Open the 'Assign dialog' window.
5. In the window click event category on the left and select the cause from the list.

   ⇨ The appropriate tree is now shown in the right side of the window. The elements that can be linked are highlighted.
6. Open the tree and select the corresponding element.
7. Click on the 'Assign' button.

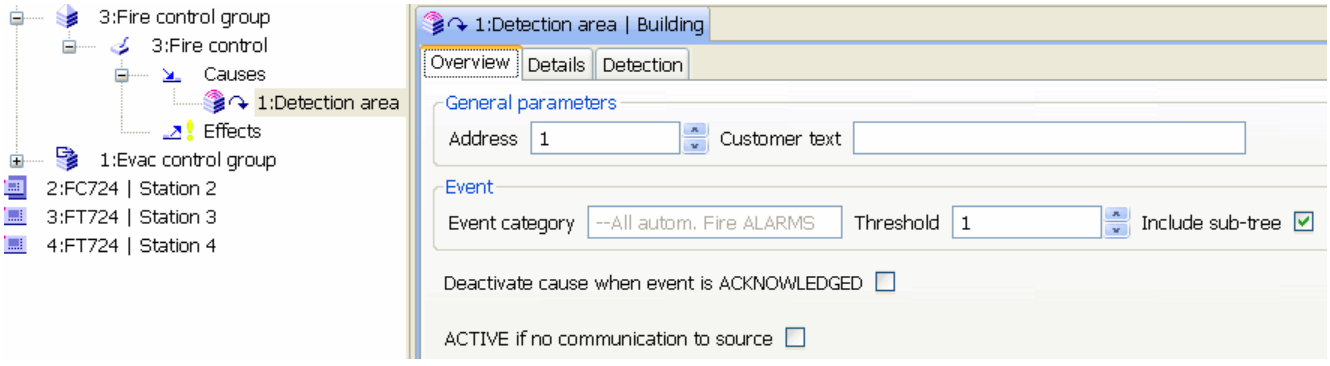
⇨ 'Causes' is linked to the element.

Event category	Cause	Link with
Outputs with confirmation	All Fire ALARMS '--All autom. Fire ALARMS '----Autom. First ALARM '----General autom. Fire ALARM '----Exting. pre-alarm (Aut. Fire AL.) '----Exting. discharged (Aut. Fire AL.) '--Manual Fire ALARM All Pre-ALARMS	Hardware tree Detection tree
	'--Degraded Fire ALARM	Hardware tree
Events 'Technical message'	All technical messages	Detection tree Operation tree
Events 'Fault'	All faults '--Other fault '--All system faults '----System fault: general connection fault '----System fault: module '----Other system fault '--Mains failure '--Battery failure '--Emergency power operation	Hardware tree Detection tree Control tree Operation tree Network tree
Events 'Isolation'	All isolations '--Other isolation '--Temporary isolation '--Alarm evaluation OFF '--Sub-system isolation '--Automatic extinguishing release OFF '--Autom.+man. extinguishing release OFF '--Renovation mode "--Not ready '--Fire related controls OFF '--RT FIRE channels OFF '--Sounders OFF	Detection tree
Events 'Test'	All test modes '--Detector test mode '--Installation test mode '--Control test mode All test activations '--Test activation ALERT '--Test activation EVAC '--Other test activation	Detection tree Control tree

Event category	Cause	Link with
Events 'Activation'	All activations '--Activation/ALERT '--Activation/EVAC '--Other activation '--Activation/confirmed '--Activation/NOT active '--Activation/unexpected	Detection tree Control tree Operation tree
Events 'AVC and IC'	AVC, Fire ALARM AVC, Pre-ALARM	Detection tree
	IC, Technical IC, Fault IC, Isolation IC, Test IC, Activation IC, Information	Station
Events 'Information'	Manned operation Unmanned operation Service information: Service required Access level <> default level '--Access level 1 '--Access level 2.1 '--Access level 2.2 '--Access level 3 Expiry reminder of time lim. isol. Other information Visibility	Hardware tree Detection tree
Inputs	• Input	• Hardware tree

Events which can be assigned

Properties of the element linked to the cause



Detail editor of the element linked to the cause, overview

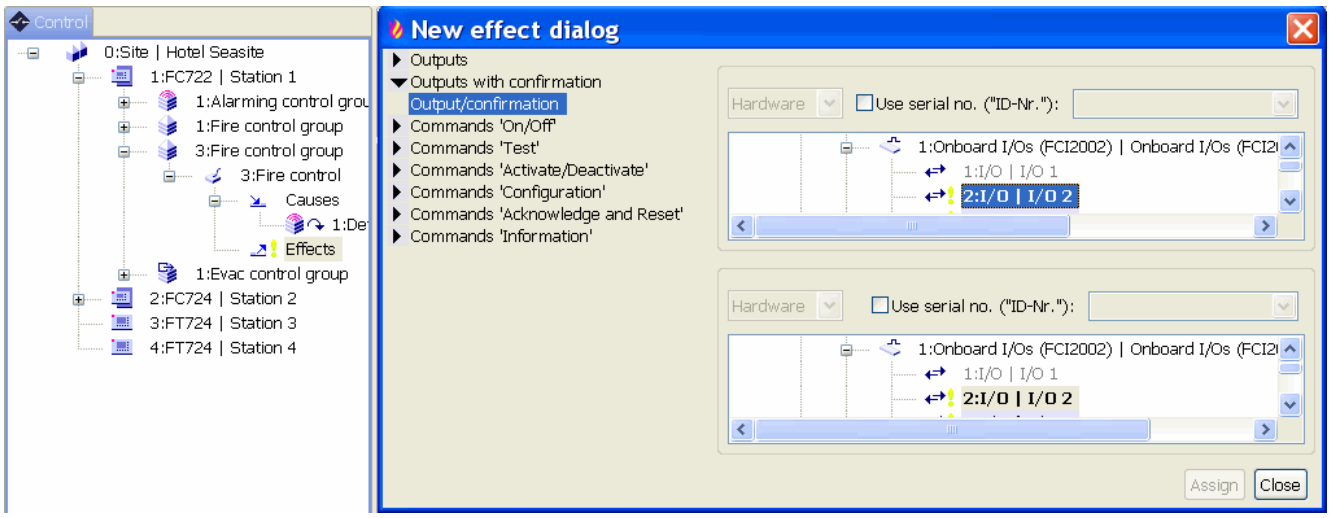
The following properties can be set in the detail editor of the element linked to the cause, in the 'Detection area' example:

- 'Include sub-tree': If the box contains a checkmark, not only the events from this level but also the events from all lower levels are considered.

- 'Deactivate cause when event is ACKNOWLEDGED': If the box contains a checkmark, the cause is deactivated as soon as the linked event is acknowledged. If the checkmark is not set then the cause is deactivated as soon as the linked event disappears.
- 'ACTIVE if no communication to source': If the box contains a checkmark, the status of the cause is active in the event of a communication failure on the station that contains the linked element. If the checkmark is not set then the status of the cause remains silent.

8.3.4.2 Effect of element 'Fire control'

The graphic below shows the 'Assign dialog' window. This shows possible outputs and commands that can be linked with an output element of the hardware tree, detection tree or control tree.



Window 'Assign dialog' with effect example 'Output with confirmation'

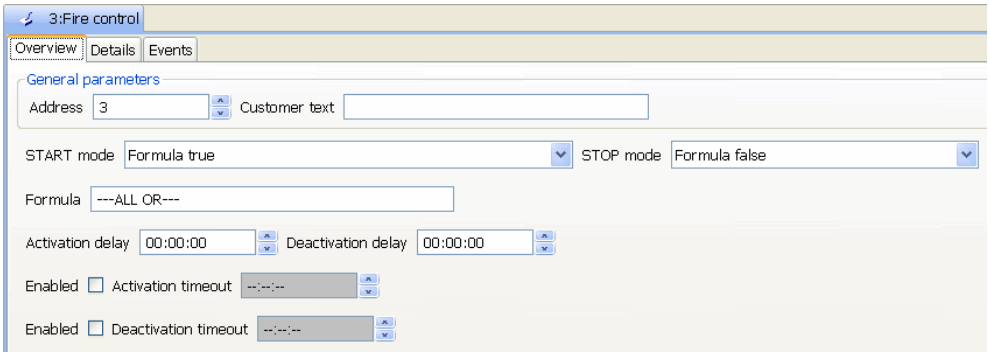
In the example, two trees are shown one below the other. The lower tree view appears only when a confirmation input can be linked.

To link the effect, proceed as follows:

1. Select the 'Control' task card.
2. Open the 'Station' in the tree view.
3. In 'Fire control', highlight the 'Effects' element.
4. Open the 'Assign dialog' window.
5. Click on an output or command on the left in the window.
   ⇨ The appropriate tree is now shown in the right side of the window. The elements that can be linked are highlighted.
6. Select the appropriate ID No. (outputs only) or open the tree and select the corresponding element.
7. Click on the 'Assign' button.

⇨ 'Effects' is linked to the element.

8.3.4.3 Properties of element 'Fire control'



Detail editor of element 'Fire control', 'Overview'

The properties shown in the following tables can be set in the detail editor of the 'Fire control' element.

Formula

Cause	Formula
Inputs and events	• Operators for the link: – OR = '+' – AND = '*' – NOT = '–'. • Mixed application is possible when brackets are used

Formula for linking causes

Several causes can be linked with a formula:

'1 * (2 + 3)' means '1 AND (2 OR 3)'.

If no formula has been defined, all causes are linked with the OR function.

START mode

Start mode
Undefined (no autom. activation)
Formula true
Value rising and >= threshold (all causes OR-combined)

Start conditions for the activation of an effect

- The START mode indicates how the control shall be activated.

STOP mode

Stop mode
Undefined (no autom. deactivation)
Formula false
All causes inactive

Stop conditions for the deactivation of an effect

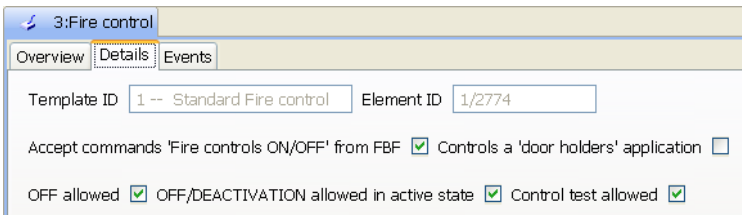
- The STOP mode indicates how the control shall be deactivated.

Additional functions

Function	Settings
Activation delay	0 to 30 minutes
Deactivation delay	0 to 30 minutes
Activation timeout	1 second to 30 minutes (default 5 minutes)
Deactivation timeout	1 second to 30 minutes (default 5 minutes)

Delays and timeout

- 'Activation delay': Activation of the control is delayed by the set time when the start conditions are met.
- 'Deactivation delay': Deactivation of the control is delayed by the set time when the stop conditions are met.
- 'Activation timeout': This is started when the control is activated. After the expiry of the set time the control is deactivated again automatically.
- 'Deactivation timeout': This is started when the control is deactivated. After the expiry of the set time the control is activated again automatically.



Detail editor of element 'Fire control', 'Details'

The following properties can be selected:

- Accept commands 'Fire controls ON/OFF' from FBF: If the box contains a checkmark, the effects of the control relating to the corresponding area switched off or on by the FBF function.
- OFF allowed: If the checkmark is placed, the control can be switched off by an operating command.

- OFF/DEACTIVATION allowed in active state: If the checkmark is placed, the control can be switched off or deactivated when the control is in active status.
- Control test allowed: If the checkmark is placed, the control can be switched to 'Control test' by an operating command.

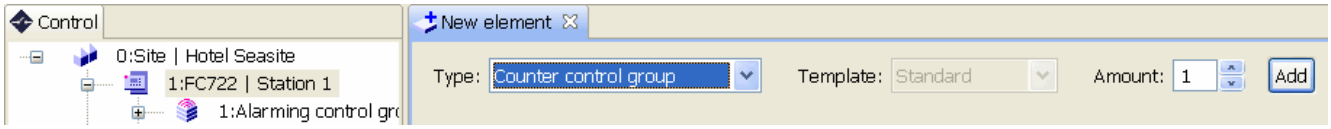
8.3.5 Counter control group

The counter control group groups the 'Alarm counter control' control elements. These register the following station events:

- 'All Fire ALARMS'
- 'All test activations'

Both the counter control group and the 'Alarm counter control' element can be switched off (via the Person Machine Interface, for example).

Creating counter control group



Task card 'Control' with the tree view and window 'New element'

1. Select the 'Control' task card.
2. Highlight the 'Station' in the tree view.
3. Open the 'New element' window.
4. In the 'Type:' field, select the 'Counter control group' element and click on the 'Add' button.

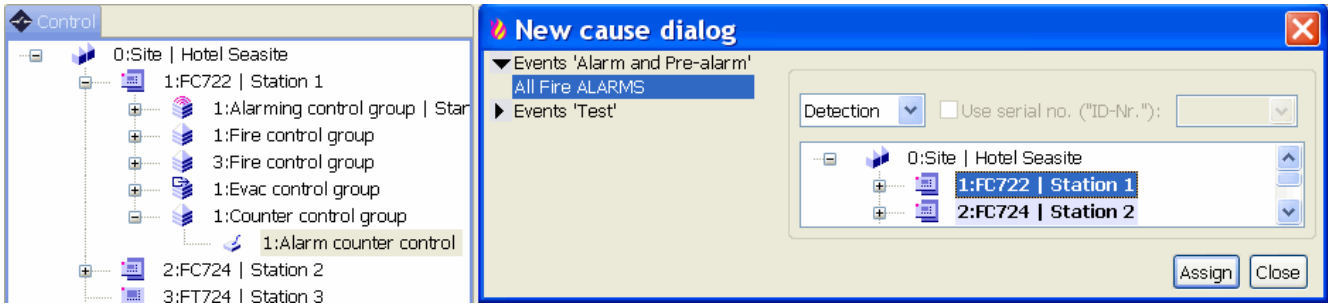
   ⇨ The element is created.
5. Highlight 'Counter control group' in the tree view.

   ⇨ The 'Alarm counter control' element is displayed in the 'Type:' field.
6. Enter the number of elements required in the 'Amount:' field and click on the 'Add' button.

   ⇨ The elements are created.
7. Enter the customer texts.

Linking alarm counter control

The 'Alarm counter control' element can be linked to one or more stations. One or both of the events can be assigned to the station or stations.



Task card 'Control' with the tree view and window 'Assign dialog'

1. Highlight the 'Alarm counter control' element in the tree view.
2. Open the 'Assign dialog' window.
3. Click the event category in the window.
   ⇨ The Hardware tree is depicted at the right of the window. The stations that can be linked are highlighted.
4. Select the relevant station and click on the 'Assign' button.
   ⇨ 'Alarm counter control' is linked to the station.

Deactivating/activating counter control group

The 'OFF' and 'ON' functions can, for example, be assigned to a standard key by linking the 'Standard key'/'Function key' element to 'Counter control group'.

8.3.6 Extinguishing standard interface SST [DE]

The extinguishing standard interface SST is used for the control and indication of the extinguishing activation of a third party extinguishing control installation. The input/output module FDCIO224, which is integrated in the fire control panel, is used as an interface between the fire control panel and the extinguishing control installation. The inputs of the fire control panel for the extinguishing control equipment are monitored for short-circuit and open line.

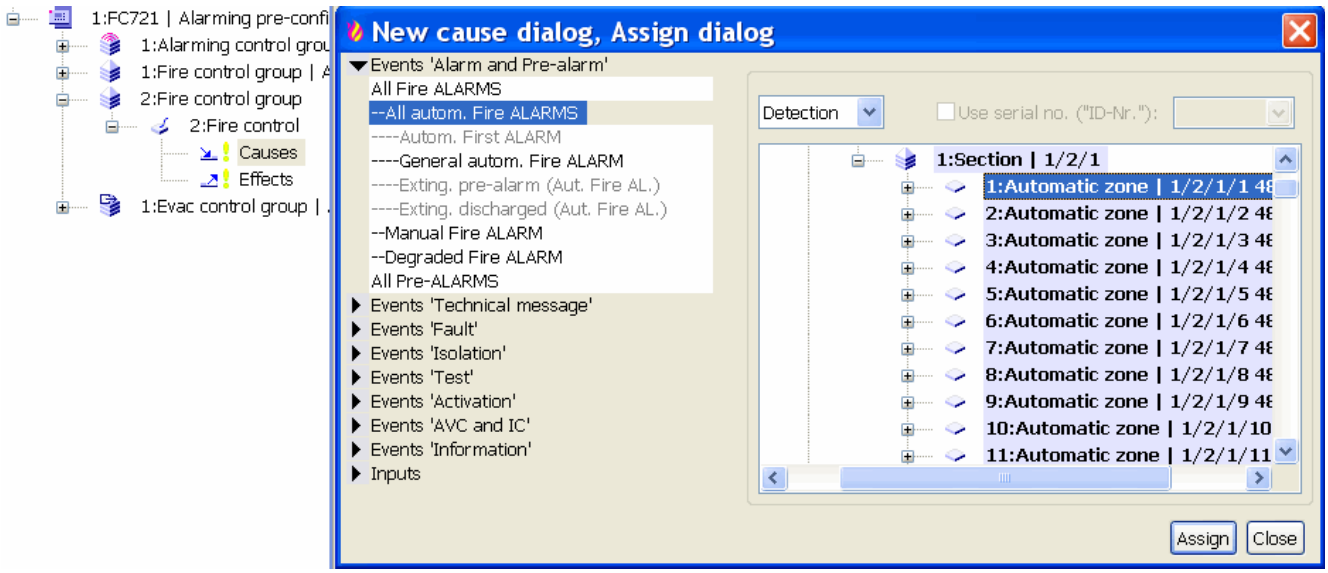
The following events are evaluated by the extinguishing control system via the inputs of the input/output module:

- 'Input 'Discharged"
- 'Fault extinguish.'

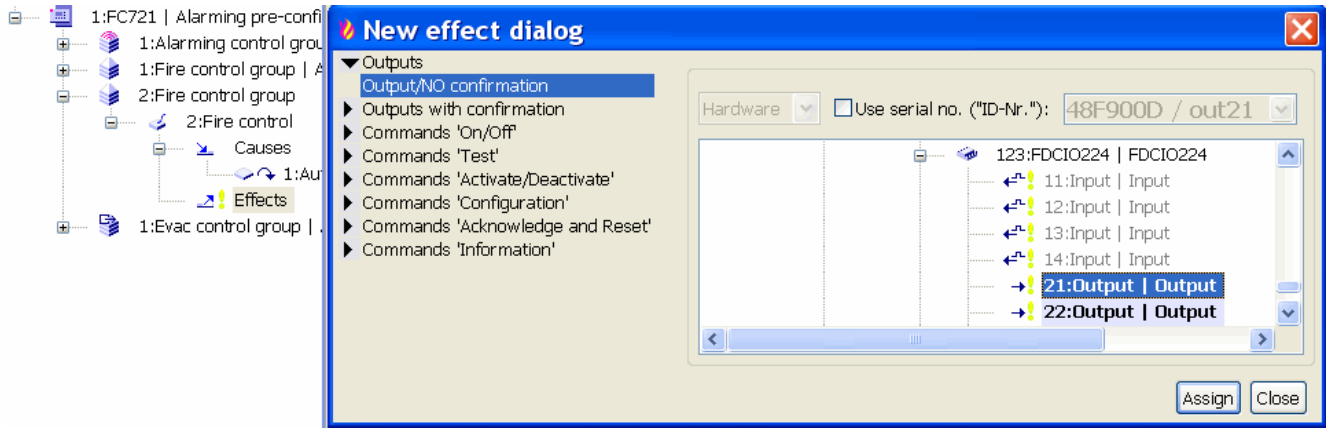
Extinguishing is activated via an output of the input/output module.

Creating an output for extinguishing actuation

An output of the input/output module is used to actuate the extinguishing process via the extinguishing control system. The command for the extinguishing actuation is give by detector zone(s) of the fire control panel.



'Assign dialog' window for linking the cause for the extinguishing actuation



'Assign dialog' window for linking the effect for the extinguishing actuation

To link the cause and effect of extinguishing release, proceed as follows:

1. Select the 'Control' task card.
2. Highlight the 'Station' in the tree view and create a 'Fire control group' element and a 'Fire control' element below this.
3. Open the 'Assign dialog' window.
4. Highlight 'Causes' and, in the 'New cause dialog' window, highlight "--All autom. Fire ALARMS' in the 'Event' list.
5. Select the relevant automatic zone(s) and click on the 'Assign' button.

   ⇨ 'Causes' is linked to the zone(s).
6. Highlight 'Fire control' and set the conditions for extinguishing activation in the detail editor, 'Overview' button.
7. Highlight 'Effects' and, in the 'New effect dialog' window, highlight 'Output/NO confirmation'.
8. Select the relevant 'Output' of input/output module FDCIO224 and click on the 'Assign' button.

⇨ 'Effects' is linked to the 'Output'.

'Input 'Discharged": Linking

An input of the input/output module serves is used to confirm extinguishing activated.

'Assign dialog' window for linking the 'Input discharged' element

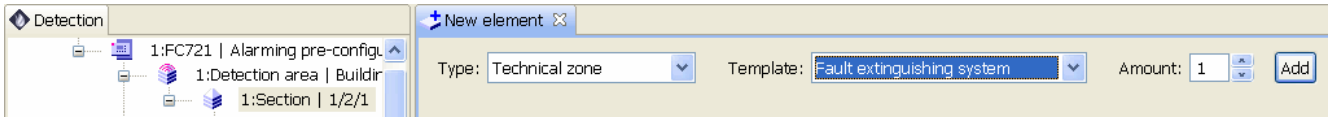
To link 'Input 'Discharged'', proceed as follows:

1. Select the 'Detection' task card.
2. Open the 'Station' in the tree view.
3. Highlight 'Section' (if available) or 'Detection area' and create an 'XC10 zone' element.
4. Open 'XC10 zone' and highlight 'Input 'Discharged''.
5. Open the 'Assign dialog' window.

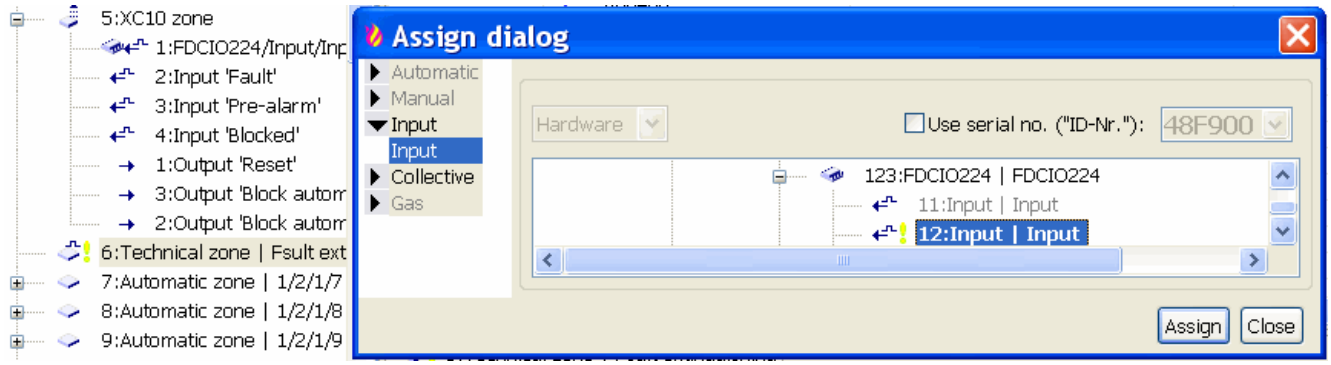
   ⇨ 'Input 'Discharged'' is highlighted and the Hardware tree appears. The elements that can be linked are highlighted.
6. In the 'Assign dialog' window, select the relevant 'Input' of input/output module FDCIO224 and click on the 'Assign' button.

⇨ 'Input 'Discharged'' is linked to the 'Input'.

Creating a 'Fault extinguish.' input



'New element' window for creating the technical zone for 'Fault extinguish.'



'Assign dialog' window for linking the 'Fault extinguish.' input

To create and link the 'Fault extinguish.' input, proceed as follows:

1. Highlight 'Section' (if available) or 'Detection area'.
2. In the 'New element' window, select the 'Technical zone' zone in the 'Type:' field and 'Fault extinguishing system' in the 'Template:' field, and click on the 'Add' button.
3. Highlight the 'Technical zone' zone.
4. Open the 'Assign dialog' window and highlight 'Input'.

   ⇨ The Hardware tree is shown. The elements that can be linked are highlighted.
5. Select the relevant 'Input' of input/output module FDCIO224 and click on the 'Assign' button.

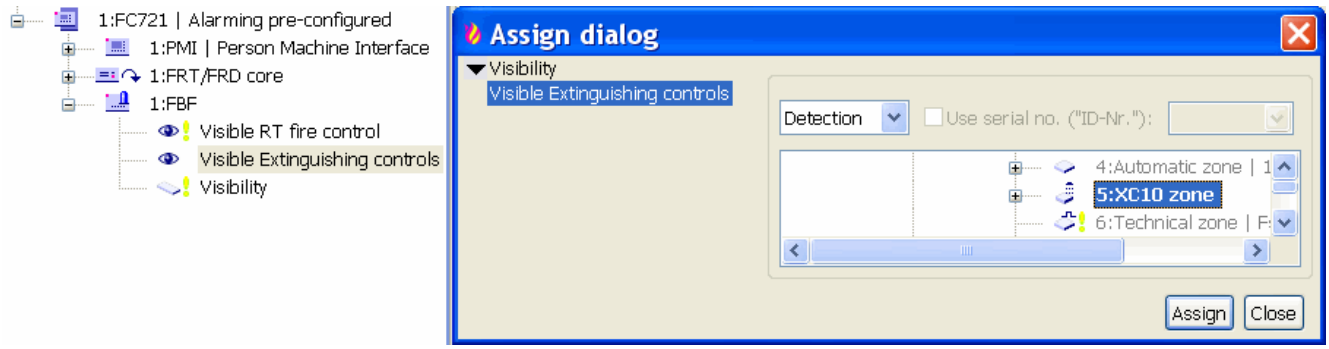
⇨ 'Technical zone' is linked to the 'Input'.

Creating fire department control panel (FBF)

See [→ 176]

Configuring the visibility on the fire department operating panel (FBF)

To ensure that the extinguishing system activation is correctly signaled by the LED on the fire department operating panel, the 'XC10 zone' element must be assigned to the fire department operating panel.



'Assign dialog' window for linking the visibility on the fire department operating panel (FBF)

To link the visibility on the fire department operating panel (FBF), proceed as follows:

1. Select the 'Operation' task card.
2. Open 'FBF' in the tree view.
3. Highlight 'Visible Extinguishing controls '.
4. Open the 'Assign dialog' window.
   ⇨ 'Visible Extinguishing controls' is highlighted and the Detection tree is shown. The 'XC10 zone' element that can be linked is highlighted.
5. Select 'XC10 zone' and click on the 'Assign' button.

⇨ 'Visible Extinguishing controls' is linked to 'XC10 zone'.

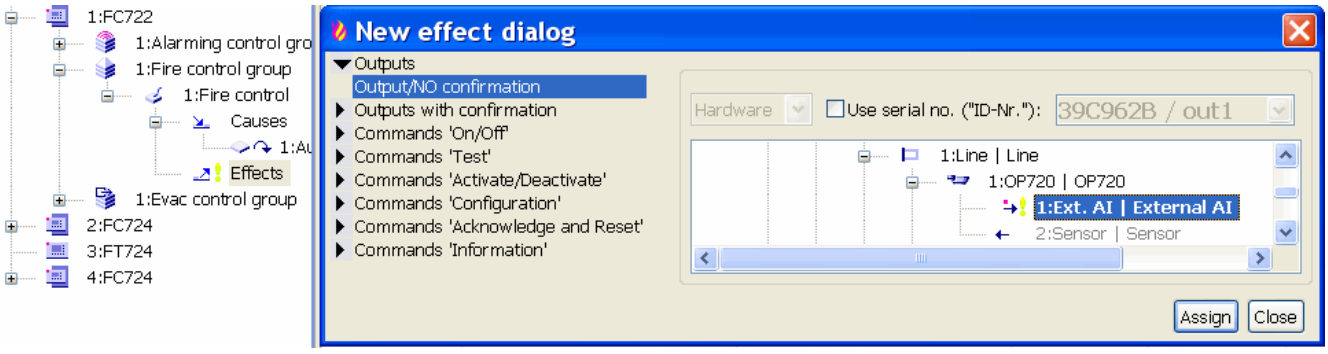
8.3.7 External alarm indicator

The external alarm indicator output of an C-NET device can be used for any evacuation control or fire control.

Prerequisite

'Activated by a control (independent output)' activation mode for the external alarm indicator output is selected.

Linking external alarm indicator output



Window 'Assign Dialog' with 'Output/no confirmation'

1. Select the 'Control' task card.
2. In the tree view, open
   'Fire control group' > 'Fire control'
   - OR -
   'Evac control group' > 'Universal evac control' or 'Phased evac control'.
3. Highlight 'Effects '.
4. Open the 'Assign dialog' window.
5. Highlight 'Output/NO confirmation' at the left of the window.
6. Open the corresponding C-NET device in the hardware tree.
7. Highlight 'Ext. AI' and click on the 'Assign' button.

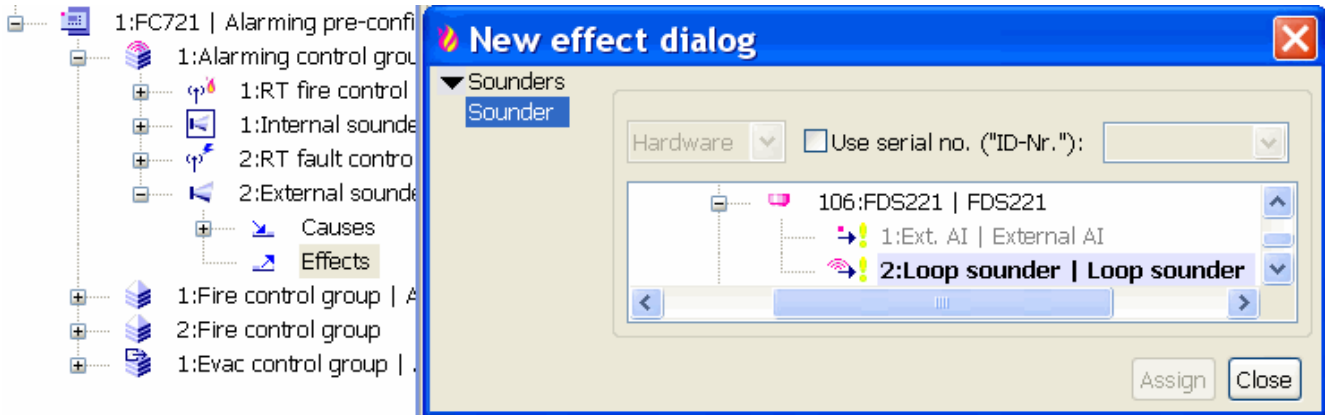
⇨ The effect of the control is linked with the external alarm indicator output.

8.3.8 Loop sounder, loop sounder/beacon, and base sounder

Loop sounder, Loop sounder beacon, and Base sounder can be assigned to the following controls:

- In the alarming control group as
  - internal Sounder
  - or external Sounder
- In the evac control group for
  - universal evacuation
  - or 2-stage evacuation

Linking a Sounder



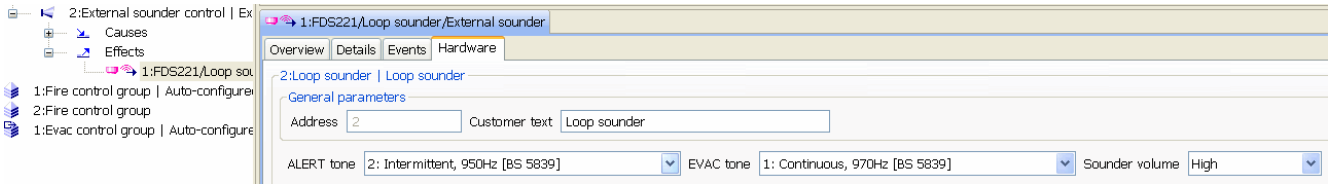
Task card 'Control', alarming and evac control groups, with window 'Assign dialog' for linking a sounder

1. Select the 'Control' task card.
2. Depending on the application in question, open the following in the tree view:
   'Alarming control group' > 'Internal sounder control' or 'External sounder control'
   - OR -
   'Evac control group' > 'Universal evac control' or 'Phased evac control'
3. Highlight 'Effects '.
4. Open the 'Assign dialog' window.

   ⇨ 'Assign dialog' is highlighted at the left of the 'Sounder' window.
5. In Hardware tree, select the 'Sounder' channel.
6. Click on the 'Assign' button.

⇨ 'Effects' is linked to 'Sounder'.

Configuring the Sounder



Task card 'Control' with detail editor 'Sounder', 'Hardware'

The 'Sounder' configuration is displayed in the detail editor of the 'Control' task card, provided that the following conditions are met:

- Sounder is linked to the control effect.
- Sounder is highlighted in the tree view.

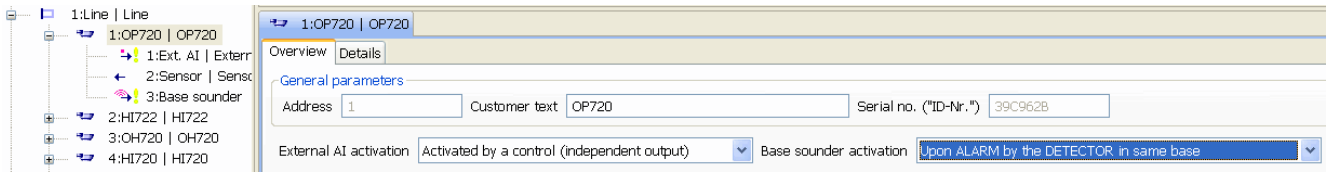
In the detail editor the following configurations are possible:

- 'ALERT tone', 'EVAC tone', and 'Sounder volume' can be set using the 'Hardware' button.
- For the Loop sounder beacon, 'Strobe activation' can also be configured using the 'Hardware' button.
- The 'Overview' button can also be used to set a time limit for 'Manned operation' and 'Unmanned operation' separately.

The settings for 'Sounder' can also be viewed in the detail editor of the 'Hardware' task card, using the 'Overview' and 'Control' buttons.

8.3.9 Base sounder with direct activation

The Base sounder can be activated directly in the event of a detector alarm in the same sounder base or an alarm in the corresponding zone. The Base sounder is activated with the evac tone in such cases.



'Base sounder activation' in the detail editor 'Detector' (with sounder base), 'Overview'

To set direct activation, proceed as follows:

1. Highlight the detector with the sounder base in the tree view.
2. In the detail editor, select the following activation type in the 'Base sounder activation' field:
   'Upon ALARM by the DETECTOR in same base'
   - OR -
   'Upon ALARM in the ZONE of the detector in same base'

Parallel activation

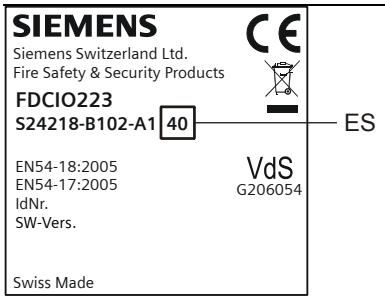
In parallel to direct activation, an evacuation control can be used to define what is to happen in other cases. To activate the Base sounder, ALERT can be used, for example.

It is always the event with the higher priority that is relevant to activation, i.e., when the evacuation control requires ALERT and the Base sounder has been activated directly, EVAC is used.

8.3.10 Sounder line via input/output module FDCIO223

The input/output module FDCIO223 is operated on the C-NET and features inputs/outputs: 1 to 2 Sounder lines can be connected to this.

Mixed operation with a collective detector line or a control line without confirmation is permitted if the input/output module FDCIO223 has a product version ≥ 40.



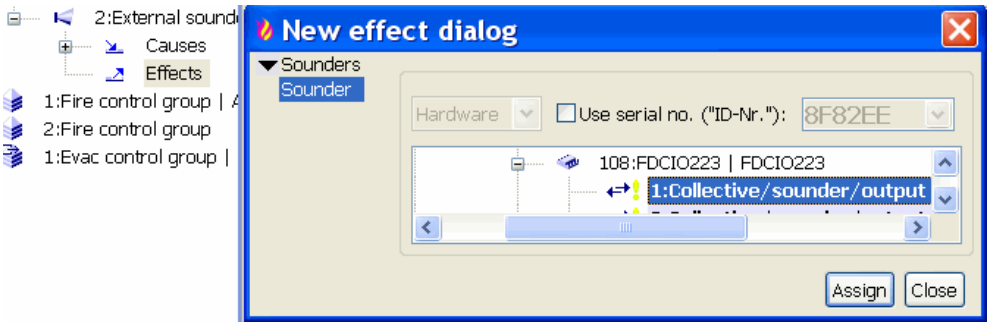
Type plate of input/output module

Linking the Sounder line

The Sounder line of the input/output module FDCIO223 is linked to the effect of the selected control element via the Assign function.

The Sounder line can be assigned to the following controls:

- In the alarming control group as
  - internal Sounder
  - or external Sounder
- In the evacuation control group for
  - universal evacuation
  - or 2-stage evacuation



Task card 'Control', alarming control groups, with window 'Assign dialog' for linking the sounder line

To link the Sounder line, proceed as follows:

1. Select the 'Control' task card.
2. Depending on the application in question, open the following in the tree view:
   'Alarming control group' > 'Internal sounder control' or 'External sounder control'
   - OR -
   'Evac control group' > 'Universal evac control' or 'Phased evac control'
3. Highlight 'Effects '.
4. Open the 'Assign dialog' window.

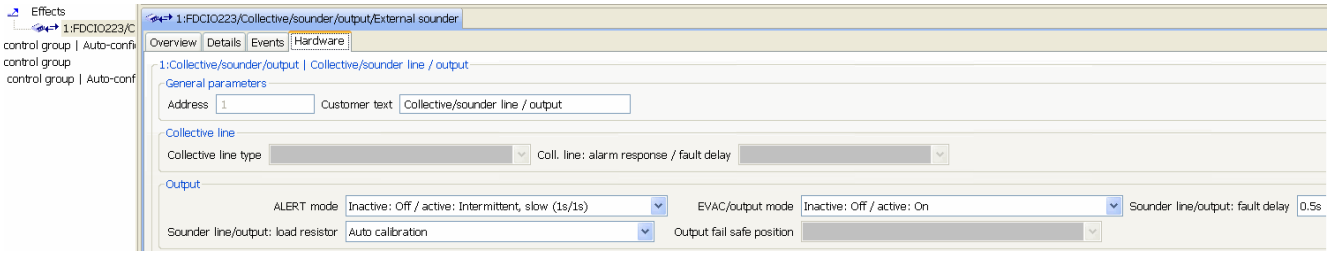
   ⇨ 'Assign dialog' is highlighted at the left of the 'Sounder' window.
5. In the Hardware tree, open the input/output module FDCIO223.
6. Select 'Collective/sounder/output'.
7. Click on the 'Assign' button.

⇨ 'Effects' is linked to 'Collective/sounder/output'.

Configuring the Sounder line

The settings for the Sounder line are displayed in the detail editor of the 'Control' task card, provided that the following conditions are met:

- The Sounder line is linked to the control effect.
- The Sounder line is highlighted in the tree view.



Task card 'Control' with detail editor 'Collective/sounder/output', 'Hardware'

- The following settings can be made using the 'Hardware' button:
  - 'ALERT mode'
  - 'EVAC/output mode'
  - 'Sounder line/output: fault delay'
  - 'Sounder line/output: load resistor'
- The 'Overview' button can also be used to set a time limit for 'Manned operation' and 'Unmanned operation', separately.

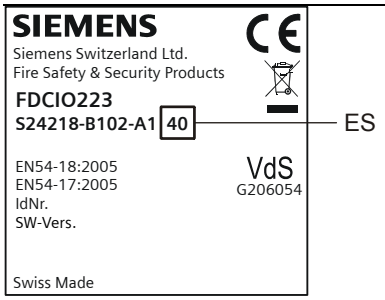
The settings for the Sounder lines are also visible in the detail editor of the 'Hardware' task card, under the 'Overview' button.

For details about the input/output module see 'document 009122, Technical manual.

8.3.11 Control line via input/output module FDCIO223

The input/output module FDCIO223 is operated on the C-NET and features two inputs/outputs. 1 to 2 control lines without confirmation can be connected to this:

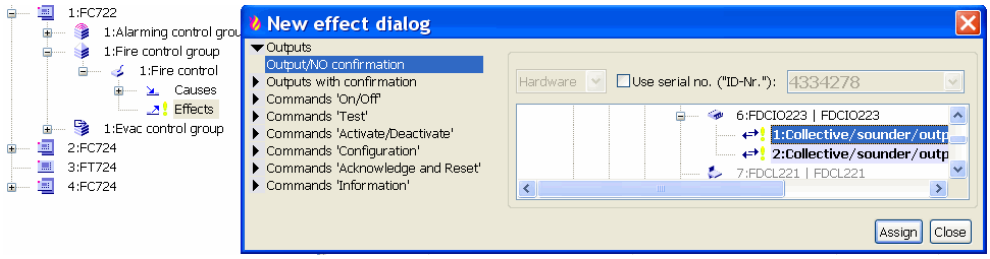
Mixed operation of a control line without confirmation using a Sounder line or collective detector line is permitted if the input/output module FDCIO223 product version is 40 or higher.



Type plate of input/output module

Linking control line without confirmation

The output for the control line on the input/output module FDCIO223 is linked to the effect of the control selected ('Fire control' or 'RT control') using the Assign function.



Task card 'Control', fire control group, with window 'Assign dialog' for linking the control line

To link the control line via the input/output module FDCIO223, proceed as follows:

1. Select the 'Control' task card.
2. Open 'Fire control group' in the tree view.
3. Highlight 'Effects' under 'Fire control'.
4. Open the 'Assign dialog' window.

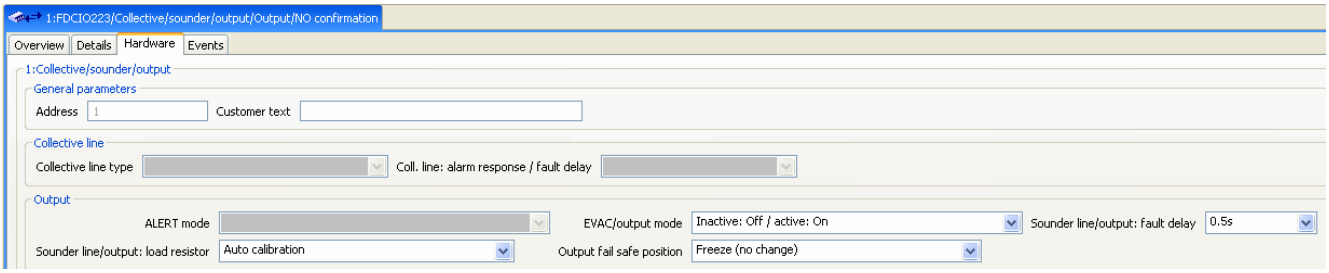
   ⇨ 'Output/NO confirmation' is highlighted at the left of the 'Assign dialog' window.
5. In the hardware tree, open the input/output module FDCIO223.
6. Select 'Collective/sounder/output'.
7. Click on the 'Assign' button.

⇨ 'Effects' is linked to 'Collective/sounder/output'.

Configuring control line

The output configuration for the control line is displayed in the detail editor of the 'Control' task card, provided that the following conditions are met:

- The output for the control line is linked to the control effect.
- The output for the control line is marked in the tree view.



Task card 'Control' with detail editor 'Collective/sounder/output', 'Hardware'

The following settings can be made using the 'Hardware' button:

- 'EVAC/output mode'
- 'Sounder line/output: fault delay'
- 'Sounder line/output: load resistor'
- 'Output fail safe position'

The output settings for the control line are also visible in the detail editor of the 'Hardware' task card, under the 'Overview' button.

For details about the input/output module see 'document 009122, Technical manual.

8.4 'Operation' task card

The 'Operation' task card contains the logical elements for the global system configuration and for configuring the operation and indication units.

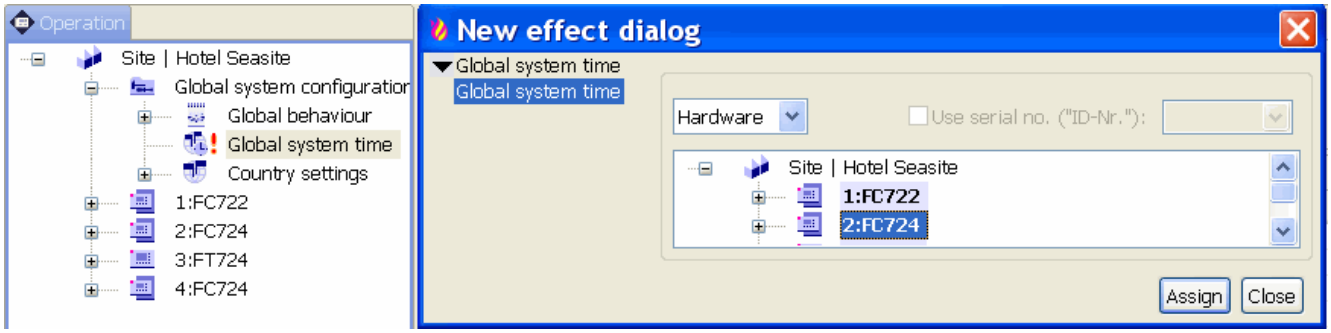
8.4.1 Global system configuration

8.4.1.1 Global behaviour

Under this element, the user can set the behaviour of all events such as type of processing and buzzer setting. The behaviour set here is always valid unless a different behaviour is set locally.

8.4.1.2 Master clock

The 'Global system time' element shows which station is the master clock. When the first station is created, Cerberus-Engineering-Tool automatically links this element to the first station (Address 1). It may be possible that the link to the station is deleted or changed. In this case, the link must be re-established with the Assign function.



Window 'Assign dialog' for linking the master clock

To link the master clock, proceed as follows:

1. Select the 'Operation' task card.
2. Open 'Global system configuration' in the tree view.
3. Highlight 'Global system time '.
4. Open the 'Assign dialog' window.

   ⇨ 'Global system time' is highlighted and the Hardware tree is shown.
5. Select the relevant station and click on the 'Assign' button.

⇨ 'Global system time' is linked to the station.

8.4.1.3 National settings

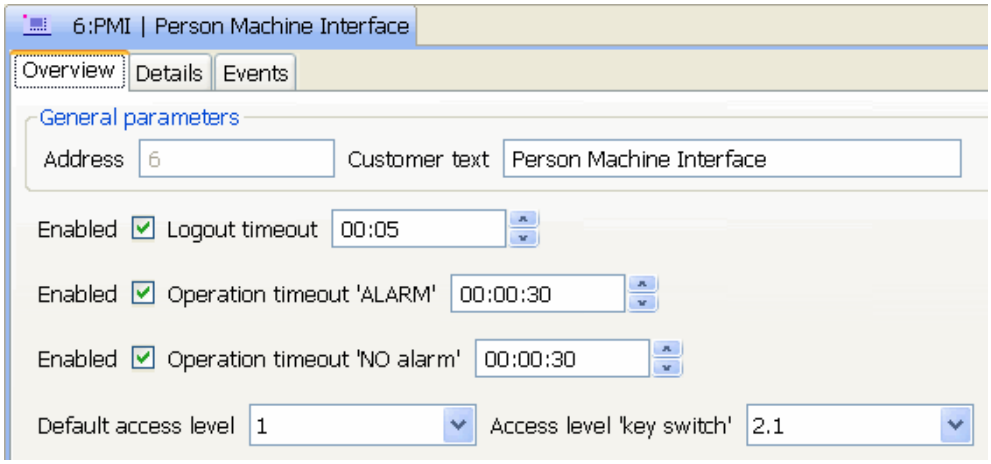
This element defines switching between summer/winter time and other time-dependent settings. You only seldom have to change these settings.

8.4.2 Person Machine Interface (PMI)

The PMI is also created when creating a Station. The following can be configured:

- Basic settings
- View of all Stations and Areas events
- LEDs can be programmed 1 to 6
- Standard keys can be programmed 1 to 2
- Favourites buttons can be programmed 1 to 8

8.4.2.1 Basic settings



Detail editor 'PMI', 'Overview'

The following basic settings can be made in the detail editor of the 'PMI' element:

- 'Logout timeout': The time after which the operating terminal automatically switches back to the default access level if no keys are pressed.
- 'Operation timeout 'ALARM'': The time after which the operating terminal automatically exits the operating menu and returns to the message display if no keys are pressed. This timeout is used if ALARM events are present.
- 'Operation timeout 'NO alarm'': The time after which the operating terminal automatically exits the operating menu and returns to the message display if no keys are pressed. This timeout is used if NO alarm events are present.
- 'Default access level': The default access level on the operating terminal (key switch in 'off' position).
- 'Access level 'key switch'': The default access level on the operating terminal (key switch in 'on' position)

8.4.2.2 Visibility

The visibility defines which parts of a fire detection installation is visible and can be operated on a station, a printer, an FAT [DE] or an FBF [DE]. The configuration of the visibility is possible in the following granularity:

- 'Site': Visibility across the entire site
- 'Site without areas': Visibility for all events from the Hardware tree for the site.
- 'Station': Visibility for a station within the site with all areas in this station
- 'Station without areas': Visibility for all events from the Hardware tree for the station.
- 'Area': Visibility for an area within a control panel

This can be restricted further, so that for example only the alarm and fault event categories are displayed instead of all events of an area.

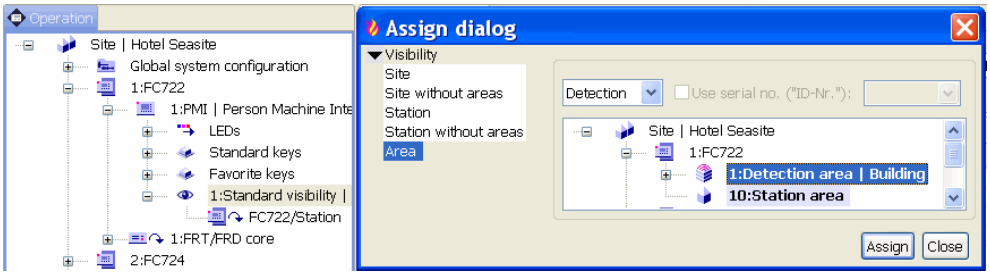
Three different visibility modes mean that additional visibilities can be added depending on the situation.

- 'Standard visibility': Standard visibility if no additional conditions are fulfilled.
- 'Standby visibility for Operating terminal': This type of visibility is also activated in the event of a configured station failing.
- 'Expanded visibility': This type visibility is activated manually, e.g., using a favorites key or a standard key.

The situation-dependent change of visibilities is only configured for stations and not for printers, for example.

Standard visibility mode

This visibility mode is created by default when a 'PMI' element is created. It defines which events of the site, stations and areas in the station to be configured can always be seen by default.



'Assign dialog' window for linking the visibility

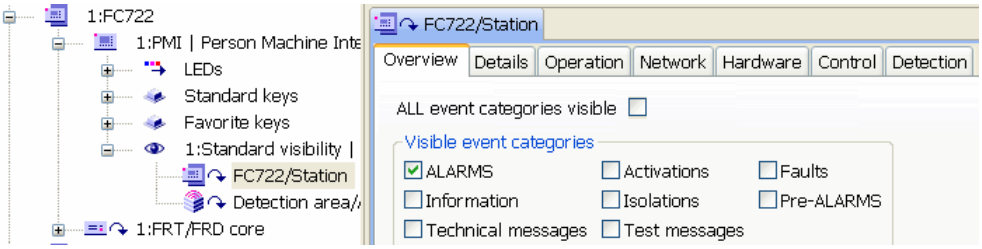
To link additional visibility, proceed as follows:

1. Select the 'Operation' task card.
2. In the tree view, open 'PMI' and highlight 'Standard visibility'.
3. Open the 'Assign dialog' window.

   ⇨ 'Visibility' list and Hardware tree or Detection tree are displayed.
4. Select the site, station, or area and click on the 'Assign' button (you can link the visibility to several elements).

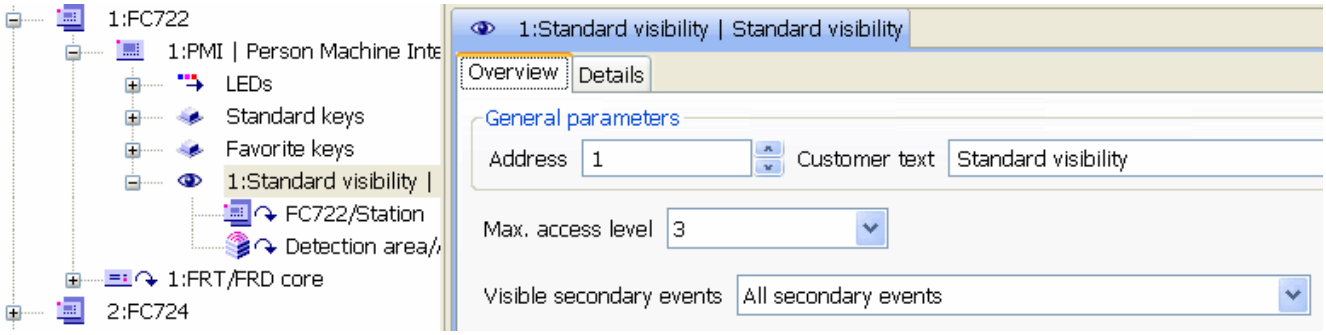
⇨ 'Visibility' is linked to the corresponding element.

One or more event categories can be selected in the detail editor of the linked elements (remove checkmark from 'ALL event categories visible').



Detail editor 'Station', 'Overview', selection of event categories

In the detail editor of the 'Standard visibility' element, it is possible to configure whether events that occur due to another visible event (e.g., confirmation messages from activated controls) should also be visible.



Detail editor 'Standard visibility', 'Overview'

- 'Visible secondary events'

  This field offers the following options:
  – 'None'
  – 'All secondary events': Activations for all controls, incl. remote transmission
  – 'Secondary events by RT ch. to Fire Brigade only'

- 'Max. access level'

  The maximum access level that can be reached in the 'Standard visibility' visibility mode is defined in this field. The 'Max. access level' value is set to 3 by default. However, in [AT] the parameter is set to 1 for sub-control panels. In this way, operation in access level 1 at most is possible in normal operation, as demanded by TRVB S 123. The value can be left at 3 for all countries except [AT].

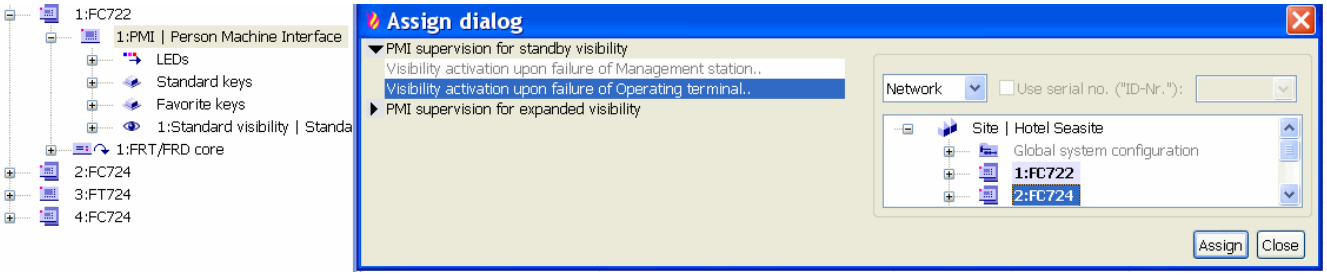
Standby visibility mode

A station with the standby visibility configured monitors one or more other stations in the configured visibility.

- When the fire detection installation is in normal operating condition, standby visibility is deactivated. The station configured and the display are then in quiescent condition.
- If a monitored station fails or if the connection to a monitored station is interrupted, the configured standby visibility becomes active and the fire detection installation can be operated in the configured visibility via this station exactly as was previously the case with the failed station.

The following standby visibilities can be defined depending on the station to be monitored:

- 'Standby visibility for Operating terminal': This must be used if the monitored station is a FC720 control panel or a FT724 terminal.
- 'Standby visibility for Management station': This must be used if the monitored station is a management station.



Window 'Assign dialog' for creating and linking standby visibility

To create and link standby visibility, proceed as follows:

1. Select the 'Operation' task card.
2. Highlight 'PMI' in the tree view.
3. Open the 'Assign dialog' window.
4. Select the relevant 'PMI supervision for standby visibility' element from the list.
5. Select the station from the tree view (multiselection is possible) and click on the 'Assign' button.

   ⇨ The corresponding 'Standby visibility' element is created for each station selected and linked to the station.
6. Highlight the 'Standby visibility' element and link the visibility (same selection options available as with standard visibility).

Elements are configured in the detail editor in the same way as with standard visibility. The maximum access level for the standby visibility is set to 2.1 by default. If several visibility modes are active, e.g. standard visibility and standby visibility, the maximum access level corresponds to the highest of the two maximum access levels. This means, amongst other things, that if a maximum access level in the standard visibility is 3 then the maximum access level under all circumstances is 3 because the standard visibility always exists.

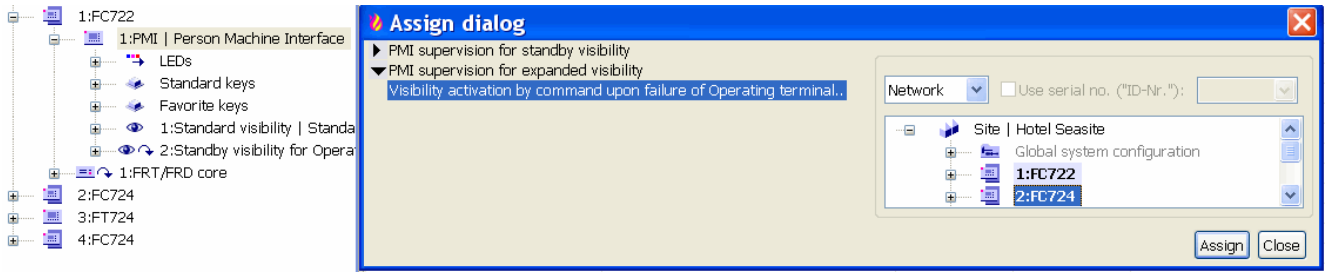
Expanded visibility mode

Expanded visibility is a visibility mode that can be activated by a manual command in addition to the normal visibility. Activation is possible e.g. by a favorite key or a standard key.

The expanded visibility is used in [AT] in order to give the sub-control panels visibility of the remainder of the system in the event of a system collapse because of several network errors, in acc. with TRVB S 123.

Furthermore, the expanded visibility is used so that commissioning or maintenance personnel can access further parts of the system temporarily.

The 'Expanded visibility' element can be created using the 'New element' or 'Assign' function to configure the expanded visibility.



Window 'Assign dialog' for creating and linking extended visibility

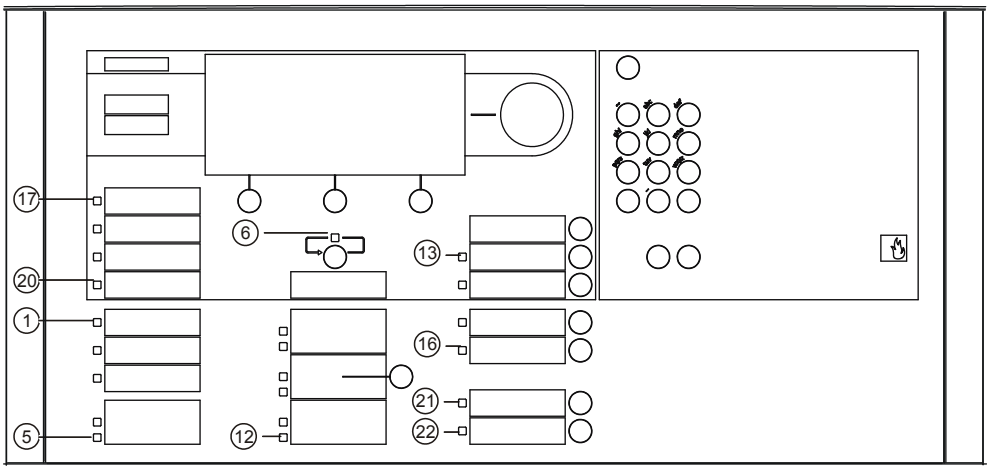
To create and link extended visibility, proceed as follows:

1. Select the 'Operation' task card.
2. Highlight 'PMI' in the tree view.
3. Open the 'Assign dialog' window.
4. Select the relevant 'Expanded visibility' element from the list.
5. Select the station from the tree view (multiselection is possible) and click on the 'Assign' button.

   ⇨ The 'Expanded visibility' element is created for each station selected and linked to the station.
6. Highlight the 'Expanded visibility' element and link the visibility (same selection options available as with standard visibility).

Elements are configured in the detail editor in the same way as with standard visibility. The maximum access level for the expanded visibility is set to 2.1 by default.

8.4.2.3 LEDs



LEDs in the Person Machine Interface

1 to 16	LEDs with permanently assigned cause
17 to 22	Programmable LEDs 1 to 6

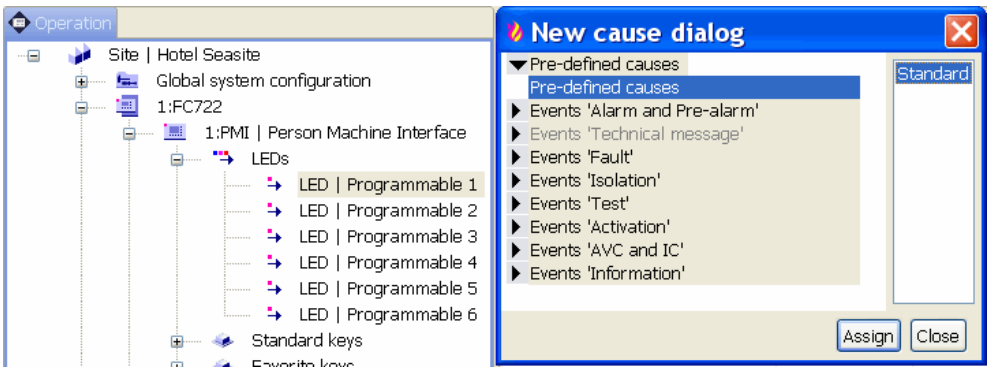
The LEDs on the Person Machine Interface signal events and conditions (causes). In addition, the LEDs support the operator's orientation.

There are two ways of assigning a cause to a LED:

- Event with defined, local visibility
- Event with optional, global visibility on particular element from the hardware tree or a logical tree.

Assigning event with defined, local visibility

The Assign function or 'New element' can be used to assign one or more predefined causes to any programmable LED. If several causes are assigned, the LED properties (priority, LED mode, colour) must be different in each case.



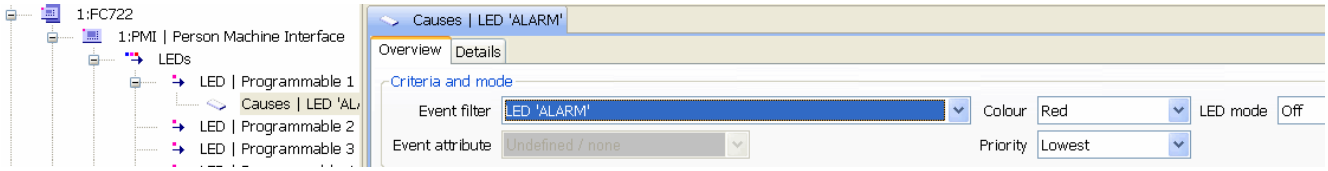
'Assign dialog' window for assigning a predefined cause to an LED

To assign the predefined cause to an LED, proceed as follows:

1. Select the 'Operation' task card.
2. In the tree view, open 'PMI' > 'LEDs' and highlight 'LED'/'Programmable 1' - 'Programmable 6'.
3. Open the 'Assign dialog' window.

   ⇨ The list of events is displayed.
4. Select 'Pre-defined causes', highlight 'Standard', and click on the 'Assign' button.

⇨ 'LED'/'Programmable 1' - 'Programmable 6' contains the 'Causes'/'Undefined' sub-element.



'Causes / ...', 'Overview' detail editor

An event filter and/or event attribute is now assigned to the sub-element and the LED properties determined.

Event filter			Event attribute
Undefined LED 'ALARM' LED 'ALARM': on (buzzer silenced) LED 'ALARM': intermittent, slow (buzzer active) LED 'PRE-ALARM' LED 'PRE-ALARM': on (buzzer silenced) LED 'PRE-ALARM': intermittent, slow (buzzer active) LED 'FAULT' LED 'ISOLATION' LED 'DETECTOR TEST' LED 'TECHNICAL' LED 'Active' LED 'INFORMATION' LED 'System On'	LED 'System Fault' LED 'More alarms' LED 'Remote alarm Active' LED 'Remote alarm not activated' LED 'Remote alarm Fault' LED 'Remote alarm Off' LED 'Alarm device/EVAC Active' LED 'Alarm device/EVAC Fault' LED 'Alarm device/EVAC Off' LED 'Control function Active (without confirmation)' LED 'Control function Active (with confirmation)' LED 'Control function Active (with or without confirmation)' LED 'Control function Fault'	LED 'Control function Off' LED 'Acknowledge' LED 'Reset' LED 'Alarm delay off' LED 'Premises manned' LED 'Premises manned' AND 'Premises unmanned' LED 'Key depot Sabotage ALARM' LED 'Key depot unlocked' LED 'Power supply fault' LED 'Extinguishing discharged' LED 'Autom. extinguishing release OFF' LED 'Autom.+man. extinguishing release OFF'	Undefined / none Intervention text available

Assignable event filter and/or event attribute

Colour	Priority	LED mode
Depends whether LED is available or not. Red Yellow Green	The priority of the cause selected compared with other causes which are defined for the same LED. High Highest Low Lowest Medium	Intermittent Intermittent, fast Intermittent, long period Intermittent, short period Off On

LED properties

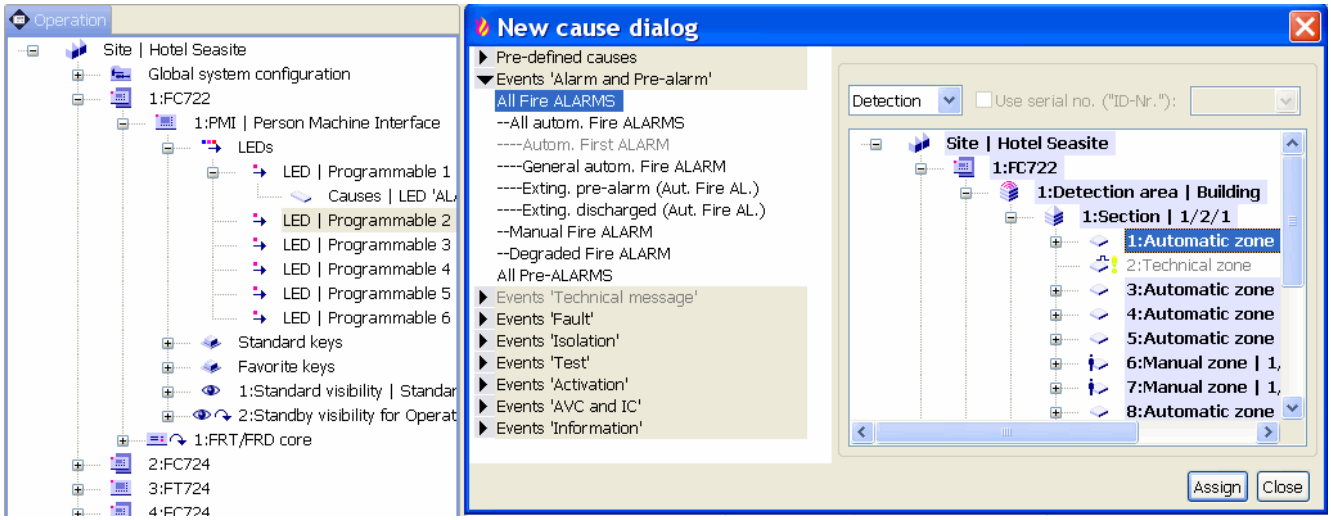
Assigning event with optional, global visibility

The table below provides an overview of the events which can be assigned to an LED. In this process an event can be assigned to any LED and the LED properties determined.

Event category	Cause	Link with
Outputs with confirmation	All Fire ALARMS '--All autom. Fire ALARMS '----Autom. First ALARM '----General autom. Fire ALARM '----Exting. pre-alarm (Aut. Fire AL.) '----Exting. discharged (Aut. Fire AL.) '--Manual Fire ALARM All Pre-ALARMS	Hardware tree Detection tree
	'--Degraded Fire ALARM	Hardware tree
Events 'Technical message'	All technical messages	Detection tree Operation tree
Events 'Fault'	All faults '--Other fault '--All system faults '----System fault: general connection fault '----System fault: module '----Other system fault '--Mains failure '--Battery failure '--Emergency power operation	Hardware tree Detection tree Control tree Operation tree Network tree

Event category	Cause	Link with
Events 'Isolation'	All isolations '--Other isolation '--Temporary isolation '--Alarm evaluation OFF '--Sub-system isolation '--Automatic extinguishing release OFF '--Autom.+man. extinguishing release OFF '--Renovation mode ''--Not ready '--Fire related controls OFF '--RT FIRE channels OFF '--Sounders OFF	Detection tree
Events 'Test'	All test modes '--Detector test mode '--Installation test mode '--Control test mode All test activations '--Test activation ALERT '--Test activation EVAC '--Other test activation	Detection tree Control tree
Events 'Activation'	All activations '--Activation/ALERT '--Activation/EVAC '--Other activation '--Activation/confirmed '--Activation/NOT active '--Activation/unexpected	Detection tree Control tree Operation tree
Events 'AVC and IC'	AVC, Fire ALARM AVC, Pre-ALARM	Detection tree
	IC, Technical IC, Fault IC, Isolation IC, Test IC, Activation IC, Information	Station
Events 'Information'	Manned operation Unmanned operation Service information: Service required Access level <> default level '--Access level 1 '--Access level 2.1 '--Access level 2.2 '--Access level 3 Expiry reminder of time lim. isol. Other information Visibility	Hardware tree Detection tree

Events which can be assigned



'Assign dialog' window for assigning the cause to an LED

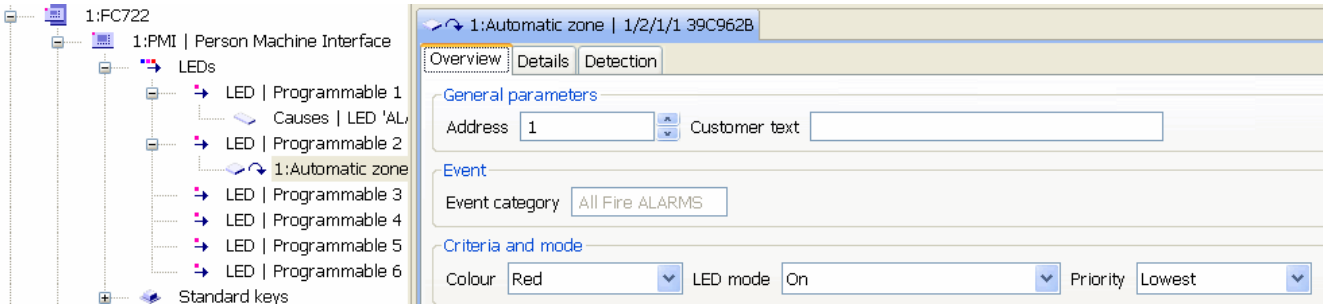
To assign the cause to an LED, proceed as follows:

1. Select the 'Operation' task card.
2. In the tree view, open 'PMI' > 'LEDs' and highlight 'LED'/'Programmable 1' - 'Programmable 6'.
3. Open the 'Assign dialog' window.

   ⇨ The list of events is displayed.
4. Select an event and element from one of the trees and click on the 'Assign' button.

⇨ 'LED'/'Programmable 1' - 'Programmable 6' is linked to the corresponding cause.

- Highlight the linked cause and determine the LED properties in the detail editor.

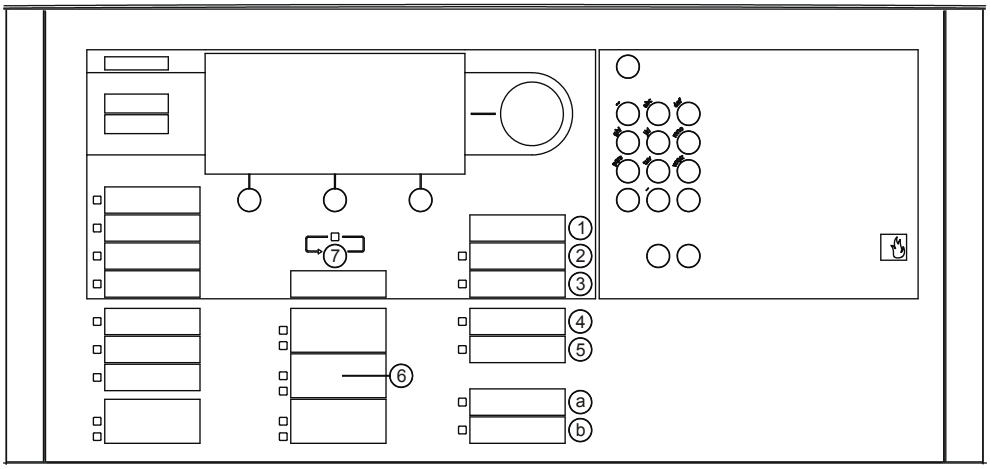


'Automatic zone', 'Overview' detail editor

Colour	Priority	LED mode
Depends whether LED is available or not. Green Red Yellow	The priority of the cause selected compared with other causes which are defined for the same LED. High Highest Low Lowest Medium	Intermittent Intermittent, fast Intermittent, long period Intermittent, short period Off On

LED properties

8.4.2.4 Standard keys



Standard keys in PMI

1 to 7	Standard keys with permanently assigned functions	a, b	Freely configurable function keys 1 and 2

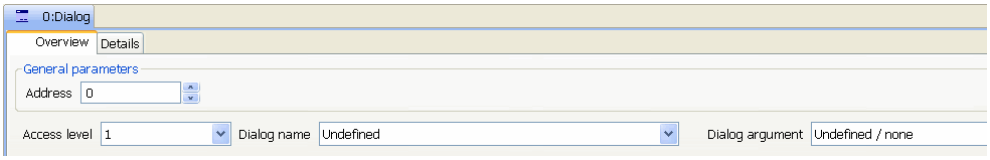
Frequently used functions can be assigned to the standard keys.

Functions are:

- Views, e.g. message indicator, customer text view, fire department view.
- Commands, e.g. activate/deactivate, test, configuration ('Set PS MANNED', 'Switch to UNMANNED', etc.).

Configuring views

- In the tree view, create the 'Dialog' element below the 'Standard key' element:
  In the 'New element' window, in the 'Type:' > 'Dialog' field
  - OR -
  In the 'Assign dialog' window, from the 'Dialog' > 'Standard' list



Detail editor 'Dialog', 'Overview'

In the detail editor of the 'Dialog' element, the following properties can be set:

- 'Access level': Access level required to execute this command.
- 'Dialog name': Indicator dialog in which the key is to appear or the dialog which is to be called up using the key.
- 'Dialog argument': Additional argument for calling up the indicator dialog. The selection depends on which dialog is configured.

The table below provides an overview of the views which can be assigned to a standard key. A view can be assigned to any standard key.

'Dialog name'	'Dialog argument'
Undefined	'Undefined / none'
Dialog 'Message viewer, List view'	'Undefined / none', 'Next category', 'Previous category', 'Jump to beginning', 'Jump to end', 'Switch to 'Fire Brigade message view'', 'Switch to 'Standard message view'', 'Switch to 'Extended message view'', 'Show active detectors', 'Switch all to 'manned'', 'Switch all to 'unmanned'', 'Switch to 'manned/unmanned''
Dialog 'Message viewer, Intervention text'	'Undefined / none', 'Jump back', 'Show messages'
Dialog 'Message viewer, Message summary'	'Reset selection'
Dialog 'Menu viewer, Main menu'	'Favorites'
Dialog 'Utility, Options'	'Undefined / none'
Dialog 'Utility, Detail'	'Undefined / none', 'Jump back', 'Show messages'
Dialog 'Config viewer, Topology'	'Undefined / none', 'Upper level', 'Lower level', 'Jump to beginning', 'Jump to end', 'Jump to linked element', 'Detection tree', 'Hardware tree', 'Control tree'
Dialog 'Admin viewer, List'	'Undefined / none', 'LED test', 'Set backlight intensity', 'Change language'
Dialog 'Admin viewer, Add user' Dialog 'Admin viewer, Delete user' Dialog 'Admin viewer, Edit user'	'Undefined / none'
Dialog 'Admin viewer, LED test'	'LED test'
Dialog 'Admin viewer, Login'	'Main menu'
Dialog 'Command viewer, Message display'	'Undefined / none', 'Execute command', 'On / Off', 'Test', 'Activate / Deactivate', 'Information', 'Configuration', 'Maintenance', 'All functions', 'Search for Categories', 'Address entry', 'Set system time', 'Search for Zone no.'
Dialog 'Command viewer, Element view'	'Undefined / none', 'Jump to beginning', 'Jump to end', 'Jump back', 'Execute command', 'Show messages'
Dialog 'Command viewer, Address entry' 'Dialog 'Command viewer, Command parameter' Dialog 'Command viewer, Zone no. entry'	'Undefined / none'
Dialog 'Event memory viewer, Event view' Dialog 'Event memory viewer, Time range entry'	'Undefined / none'
'Active dialog '	'Toggle message view'
Dialog 'Change language'	'Change language'
Dialog 'Admin viewer, Change display contrast'	'Change display contrast'
Dialog 'Utility, Messages'	'Undefined / none'

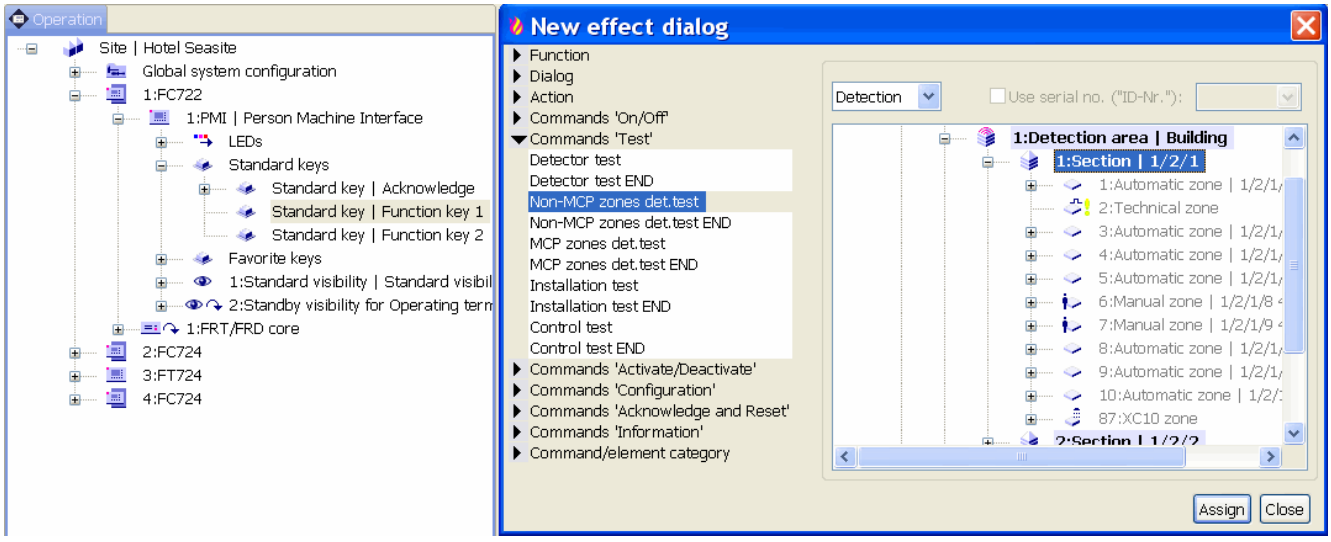
Assigning commands

The table below provides an overview of the commands which can be assigned to a standard key. A command can be assigned to any standard key.

Command	Effect	Link with
Commands 'On/Off'	'OFF' 'ON'	Hardware tree Detection tree Control tree Operation tree
	'Detector line OFF' 'Detector line ON'	Hardware tree
	'OFF/timer' 'Renovation mode' 'Non-MCP zones OFF' 'Non-MCP zones OFF/timer' 'Non-MCP zones ON' 'MCP zones OFF' 'MCP zones OFF/timer' 'MCP zones ON' 'All zones OFF' 'All zones OFF/timer' 'All zones ON' 'Fire related controls OFF' 'Fire related controls ON' 'Autom. exting. OFF' 'Autom. exting. ON' 'Autom.+man. exting. OFF' 'Autom.+man. exting. ON'	Detection tree
	'RT FIRE channels OFF' 'RT FIRE channels ON'	Control tree
Commands 'Test'	'Detector test' 'Detector test END' 'Non-MCP zones det.test' 'Non-MCP zones det.test END' 'MCP zones det.test' 'MCP zones det.test END' 'Installation test' 'Installation test END'	Detection tree
	'Control test' 'Control test END'	Control tree

Command	Effect	Link with
Commands 'Activate/Deactivate'	'Activate'	Detection tree Control tree
	'Deactivate'	Hardware tree Detection tree Control tree
	'Activate alarm indicator' 'Deactivate alarm indicator' 'Activate sprinkler 1' 'Activate sprinkler 2'	Detection tree
	'Activate/ALERT' 'Activate/EVAC' 'Activate/ALERT+EVAC' 'Time limited activation'	Control tree
Commands 'Configuration'	'Switch to MANNED' 'Switch to UNMANNED' 'Set PS MANNED' 'Set PS UNMANNED' 'Set PS'	Detection tree
Commands 'Acknowledge and Reset'	'Acknowledge' 'Reset' 'Acknowledge + Reset'	Station

Commands which can be assigned



'Assign dialog' window for assigning a function

To assign a function to the function keys, proceed as follows:

1. Select the 'Operation' task card.
2. In the tree view 'Station' > 'PMI' > 'Standard keys', and highlight 'Standard key'/'Function key 1' (or 'Function key 2').
3. Open the 'Assign dialog' window.
4. In the list, click on 'Commands 'Test'' and then 'Non-MCP zones det.test', for example.

   ⇨ The Detection tree is now shown. The elements that can be linked are highlighted.
5. Highlight 'Section', for example, and click on the 'Assign' button.

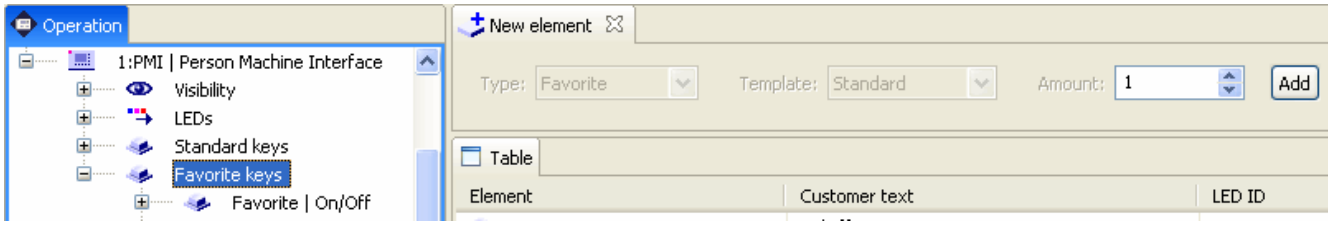
⇨ 'Standard key'/'Function key 1' is linked to 'Section'.

8.4.2.5 Favourite keys

The favorite keys are in the display menu. There is a maximum of eight favorite keys of which three are preconfigured. Frequently used functions can be assigned to the favorite keys.

Functions are:

- Views, e.g. message indicator, customer text view, fire department view.
- Commands, e.g. activate/deactivate, test, configuration ('Set PS MANNED', 'Switch to UNMANNED', etc.).



Task card 'Operation' with the tree view and window 'New Element'

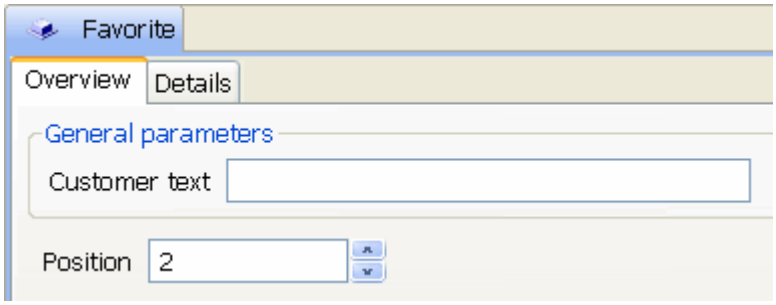
To create the favorite keys, proceed as follows:

1. Select the 'Operation' task card.
2. In the tree view, open 'Station' > 'PMI' and highlight 'Favorite keys'.
3. Open the 'New element' window.
4. In the 'Amount:' field, enter the number of 'Favorite' required and click on the 'Add' button.
5. Enter the customer text(s).
6. Highlight the 'Favorite' element you have just created.

Configuring view and assigning commands

The processes for configuring views and assigning commands are identical to that for the standard keys. See [→ 149]

Determining position of favorites



Detail editor 'Favorite', 'Overview'

In the 'Favorite' detail editor, determine the position of the favorites in the display (positions are counted from top left to bottom right). All favorite keys that are redefined must be given position 4 at least, otherwise the favorites will be overwritten by the BDV after conversion.

8.4.2.6 Changeover function

A command and the associated opposite command can be assigned to a standard key, e.g. switch off/switch on, activate/deactivate.

The command that is performed when a standard key configured with the changeover function is pressed depends on the current status of the LED corresponding to the position of this standard key:

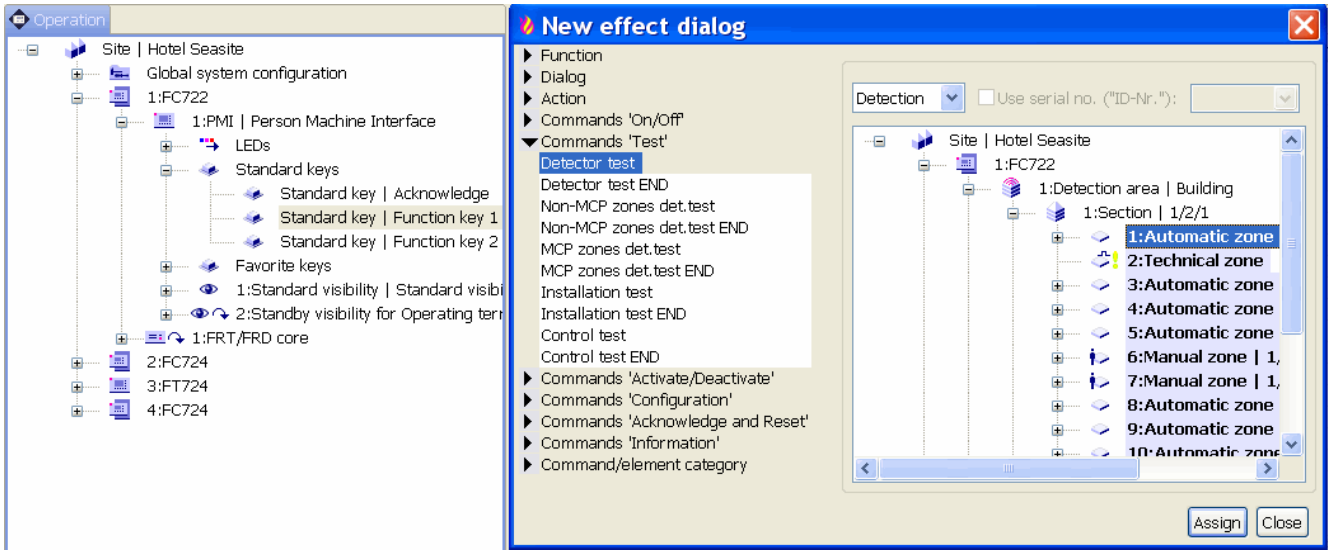
- LED inactive: the configured command is performed when the key is pressed.
- LED active: the configured opposite command is performed when the key is pressed.

  This means the LED must be configured so it is active when the command has been carried out.

Example:

- Standard key is assigned to 'Automatic zone' 2
- Command = 'Detector test'
- Opposite command = 'Detector test END'
- The LED is active if 'Automatic zone' 2 is in the 'Detector test' status.

Configuring the key for the changeover function

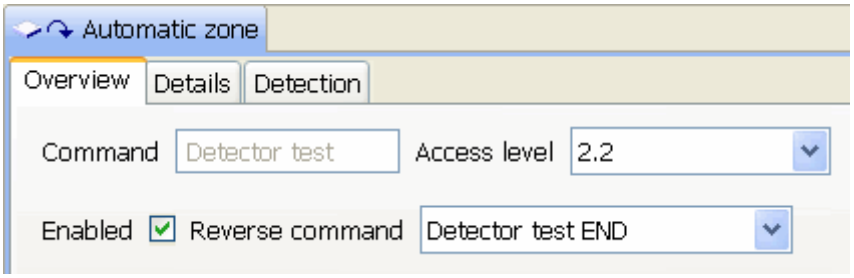


Window 'Assign dialog' for assigning the changeover function

To assign the changeover function to the function keys, proceed as follows:

1. Select the 'Operation' task card.
2. In the tree view 'Station' > 'PMI' > 'Standard keys', and highlight 'Standard key'/'Function key 1' (or 'Function key 2').
3. Open the 'Assign dialog' window.
4. In the list, click on a command such as 'Commands 'Test'' > 'Detector test'.
5. From the Detection tree, select a zone and click on the 'Assign' button.

⇨ 'Standard key'/'Function key 1' is linked to the zone.

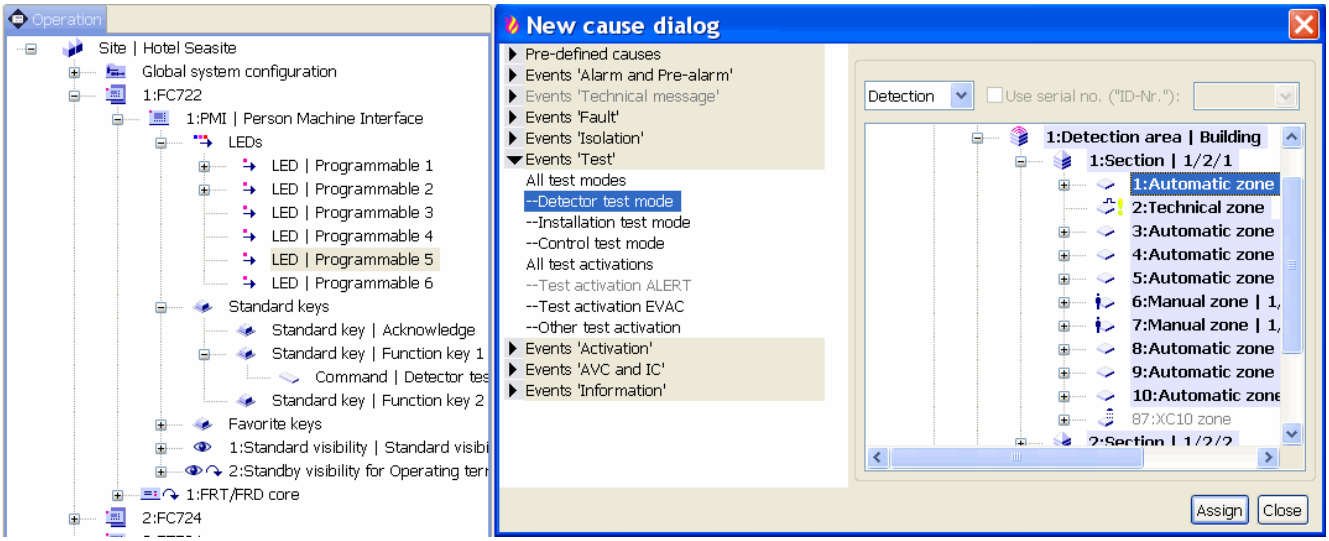


'Automatic zone', 'Overview' detail editor

In the tree view, select the zone linked to the key and, in the 'Automatic zone' detail editor ('Overview'), check the box for 'Enabled'. The 'Detector test' command appears in the 'Command' field and the 'Detector test END' opposite command appears in the 'Reverse command' field.

Configuring LED for the changeover function

So the changeover will function, the same zone as the key must be assigned to the LED.

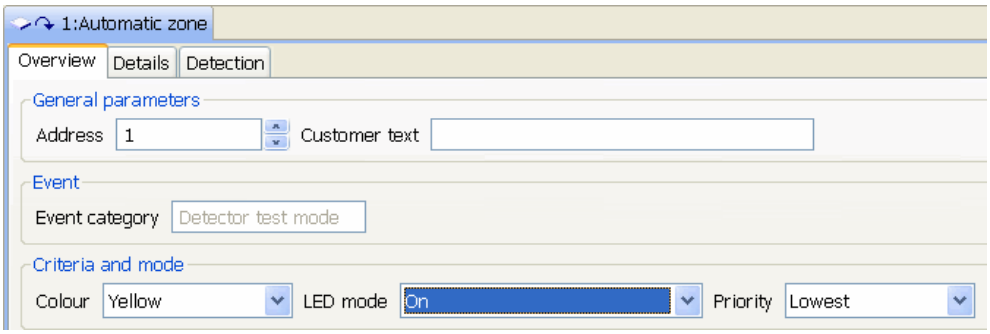


Window 'Assign dialog' for assigning the display

To assign the zone to the LED, proceed as follows:

1. In the tree view, open 'Station' > 'PMI' 'LEDs', and highlight 'LED'/'Programmable 5' (or 'LED'/'Programmable 6').
2. In the list in the 'Assign dialog' window, click on a command such as 'Events 'Test'' > 'Detector test mode'.
3. From the Detection tree, select the same zone and click on the 'Assign' button.

⇨ 'LED'/'Programmable 5' is linked to the zone.

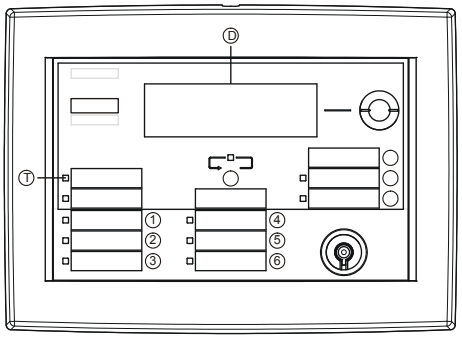


'Automatic zone', 'Overview' detail editor

Highlight the zone linked with the LED in the tree view. In the 'Automatic zone' detail editor ('Overview'), the configured event category and the color, mode, and display priority of the LED appear. With the 'On' mode set, the LED lights up when the zone is in the detector test.

8.4.3 Floor repeater terminal FT2010 and floor repeater display FT2011

Floor repeater terminal (FRT)



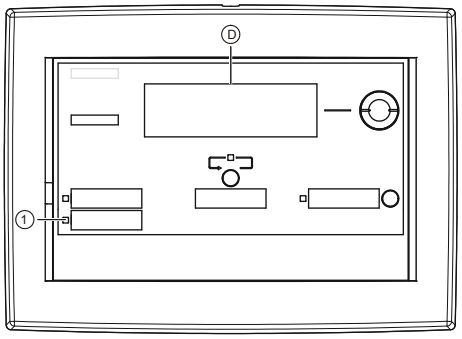
Person Machine Interface of floor repeater terminal

D	Display	1 to 6	LEDs and function keys, configurable
T	'General alarm' LED		

The following elements can be configured for the floor repeater terminal:

- Visibility
- Cause for activating LEDs 1 to 6
- Function keys 1 to 6

Floor repeater display (FRD)



Person Machine Interface of floor repeater display

D	Display	1	LED, configurable

The following elements can be configured for the floor repeater display:

- Visibility
- Cause for activating an LED

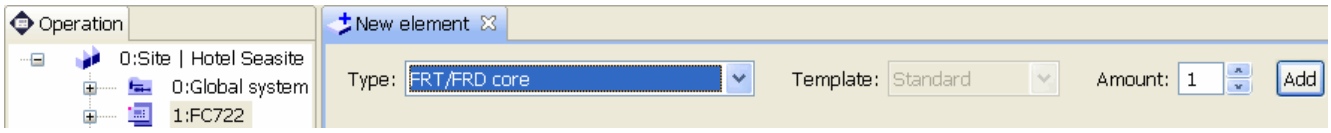
8.4.3.1 FT2010/FT2011 core and configuration groups

In order to configure the floor repeater terminal (FRT) or floor repeater display (FRD), in the task card 'Operation', for each C-NET line card (onboard/FCL2001) where floor repeater terminals or displays are connected to the C-NET line, an element 'FRT/FRD core' is created. 'FRT configuration group' elements can be created for the floor repeater terminals and 'FRD configuration group' for the floor repeater displays. Each of these elements can be linked to up to eight 'FRT' (FT2010) or 'FRD' (FT2011).

It is currently also possible to link 'FRT' or 'FRD' which are connected to another C-NET line card (onboard/FCL2001).

Only link channels that are connected to the C-NET line card (onboard/FCL2001) linked to the 'FRT/FRD core'.

Pre-configuration of the element 'FRT/FRD core'

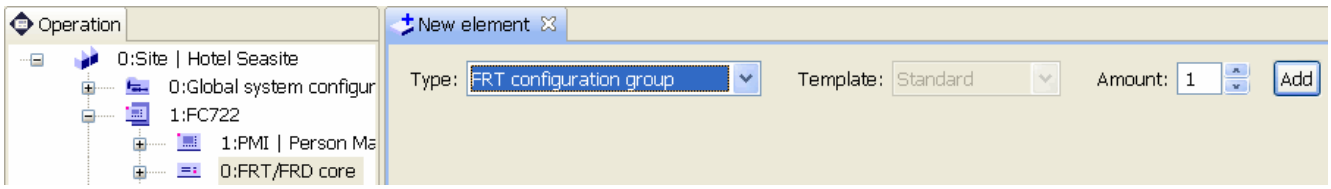


Window 'New element' for creating the element 'FT2010/FT2011 core'

To create the 'FRT/FRD core' elements, proceed as follows:

1. Select the 'Operation' task card.
2. Highlight the 'Station' in the tree view.
3. Open the 'New element' window.
4. Select the 'FRT/FRD core' element in the 'Type:' field.
5. Enter the number of elements required in the 'Amount:' field and click on the 'Add' button.

   ⇨ The 'FRT/FRD core' elements are created.



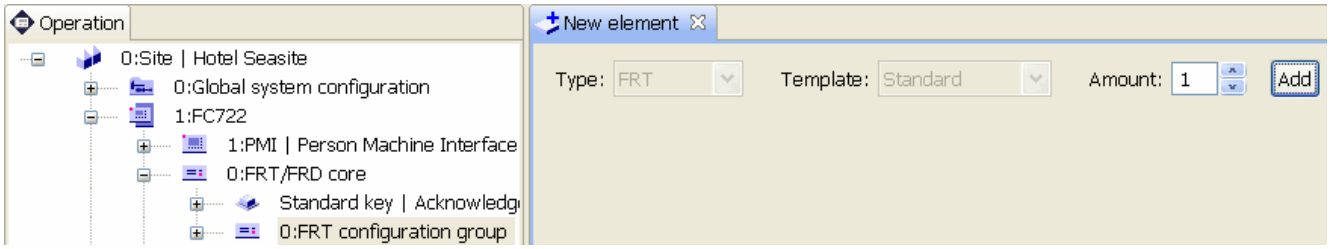
Window 'New element' for creating the element 'FRT (FRD) configuration group'

To create the 'FRT configuration group'/'FRD configuration group' elements, proceed as follows:

1. Highlight 'FRT/FRD core' in the tree view.
2. Select the 'FRT configuration group' or 'FRD configuration group' element in the 'Type:' field of the 'New element' window.

3. Enter the number of elements required in the 'Amount:' field and click on the 'Add' button.

   ⇨ The configuration groups are created along with the 'Visibility' and 'LEDs' elements.



Window 'New element' for creating the element 'FRT' or 'FRD'

To create the 'FRT'/'FRD' elements, proceed as follows:

1. Highlight 'FRT configuration group' or 'FRD configuration group' in the tree view.

   ⇨ The 'FRT'/'FRD' element can be viewed in the 'Type:' field of the 'New element' window.

2. Enter the number of elements required in the 'Amount:' field and click on the 'Add' button.

⇨ 'FRT'/'FRD' is created.

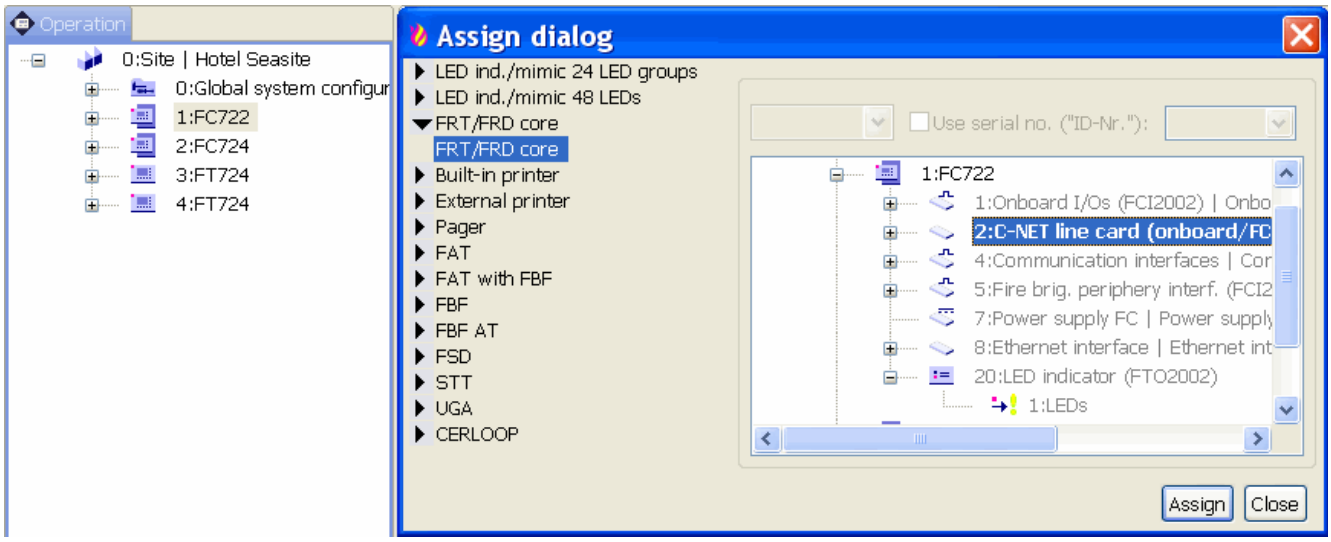
In a later step, once the hardware has been read in and is loaded in the Cerberus-Engineering-Tool, the elements still have to be linked to the hardware via the Assign function.

- 'FRT/FRD core' with 'C-NET line card (onboard/FCL2001)'
- 'FRT configuration group' with 'FRT channel' or
  'FRD configuration group' with 'FRD channel'.

When the hardware has already been read in

It is currently also possible to link 'FRT' or 'FRD' which are connected to another C-NET line card (onboard/FCL2001).

Only link channels that are connected to the C-NET line card (onboard/FCL2001) linked to the 'FRT/FRD core'.

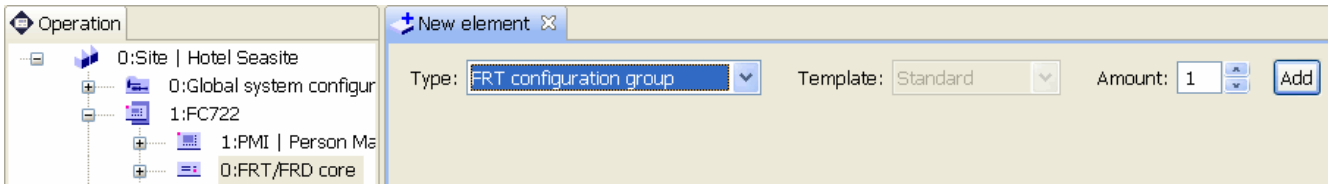


Window 'Assign dialog' for creating and linking the element 'FRT/FRD core'

To create the elements 'FRT/FRD core' and link them to the C-NET line card (onboard/FCL2001), proceed as follows:

1. Select the 'Operation' task card.
2. Highlight the 'Station' in the tree view.
3. Open the 'Assign dialog' window.
   ⇨ "FRT/FRD core' is highlighted and in Hardware tree the element 'C-NET line card (onboard/FCL2001)' is highlighted.
4. Click on the 'Assign' button.

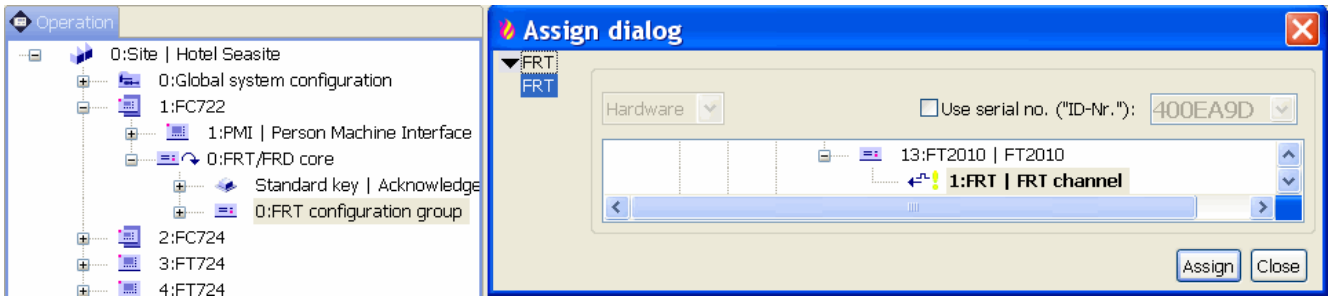
⇨ 'FRT/FRD core' is created and linked to the C-NET line card (onboard/FCL2001).



Window 'New element' for creating the element 'FRT (FRD) configuration group'

To create the 'FRT configuration group'/'FRD configuration group' elements, proceed as follows:

1. Highlight 'FRT/FRD core' in the tree view.
2. Select the 'FRT configuration group' or 'FRD configuration group' element in the 'Type:' field of the 'New element' window.
3. Enter the number of elements required in the 'Amount:' field and click on the 'Add' button.
   ⇨ The configuration groups are created along with the 'Visibility' and 'LEDs' elements.



Window 'Assign dialog' for creating and linking the element 'FRT' or 'FRD'

To link the configuration groups with the channel of the FT2010 or FT2011 device, proceed as follows:

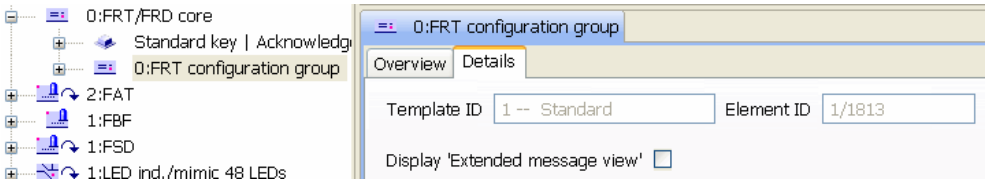
1. Highlight 'FRT configuration group' or 'FRD configuration group' in the tree view.

   ⇨ In the 'Assign dialog' window, 'FRT' or 'FRD' is highlighted and the Hardware tree is displayed. The 'FRT' or 'FRD' element of the 'FT2010' or 'FT2011' device is highlighted.

2. Select the element and click on the 'Assign' button.

⇨ The configuration group is linked with the channel of the FT2010 or FT2011 device.

Views in the Person Machine Interface display



Detail editor of configuration group

In the detail editor of the configuration group, users can select between the normal 2-line view or the extended 4-line view.

Checkmark removed	Normal 2-line view
Checkmark set	Extended 4-line view

'Display Extended message view' in detail editor

8.4.3.2 Visibility

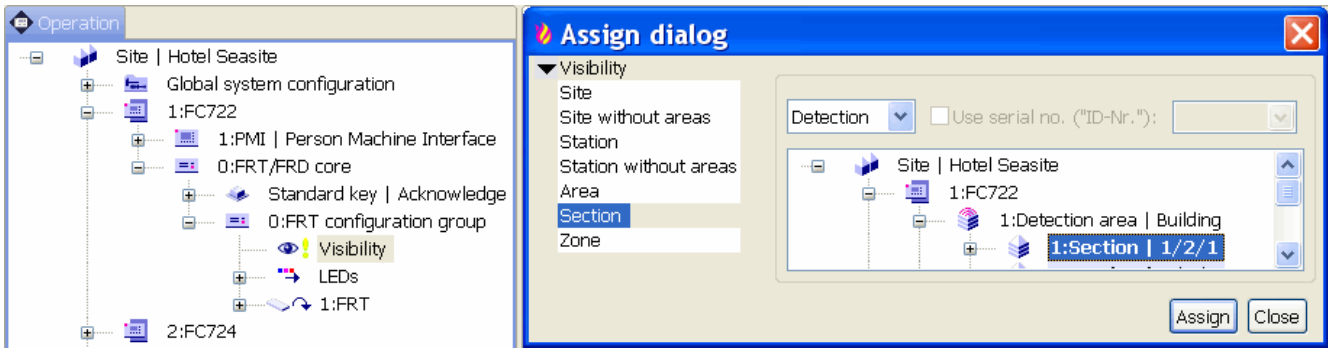
Display

The 'Visibility' element can be used to determine which events can be shown in the display for the floor repeater terminal (FRT) and floor repeater display (FRD).

The following selection is available:

- 'Site': Visibility for the entire Site
- 'Site without areas': Visibility for all events from the Hardware tree of the Site
- 'Station': Visibility for a Station within the Site, with all areas in this Station
- 'Station without areas': Visibility for all events from the Hardware tree of the Station
- 'Area': Visibility for an Area within a control panel
- 'Section': Visibility for an Section within a control panel
- 'Zone': Visibility for a Zone within a control panel

This can be restricted further, so that for example only the alarm and fault event categories are displayed instead of all events of an area.



'Assign dialog' window for linking the visibility

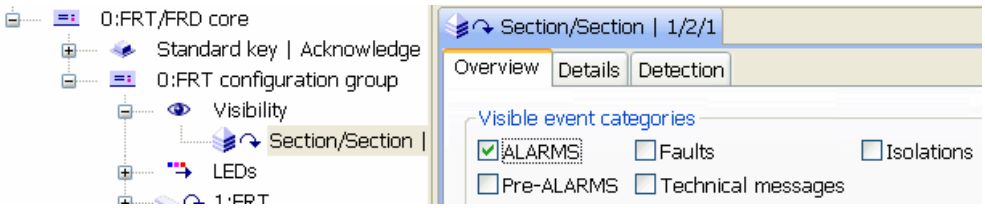
To link the visibility, proceed as follows:

1. Select the 'Operation' task card.
2. Open 'Station' > 'FRT/FRD core' > 'FRT configuration group' or 'FRD configuration group' in the tree view.
3. Highlight 'Visibility '.
4. Open the 'Assign dialog' window.

   ⇨ The event categories of 'Visibility' are displayed.
5. Select the event category and the corresponding 'Station', 'Area', 'Section', or 'Zone' element, and click on the 'Assign' button.

⇨ 'Visibility' is linked to the element.

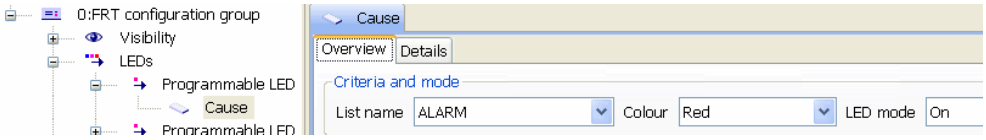
One or more event categories can be selected in the detail editor of the linked elements (place checkmark).



'Section' detail editor for selecting certain event categories

8.4.3.3 LEDs

The LEDs on the Person Machine Interface signal events and conditions. In addition, the LEDs support the operator's orientation.



'LED programmable', 'Cause' detail editor

The following LEDs properties can be configured:

- Criterion that should activate the LED
- Colour of the LED
- LED mode when LED is activated

The table below provides an overview of the properties that can be configured, with their characteristics.

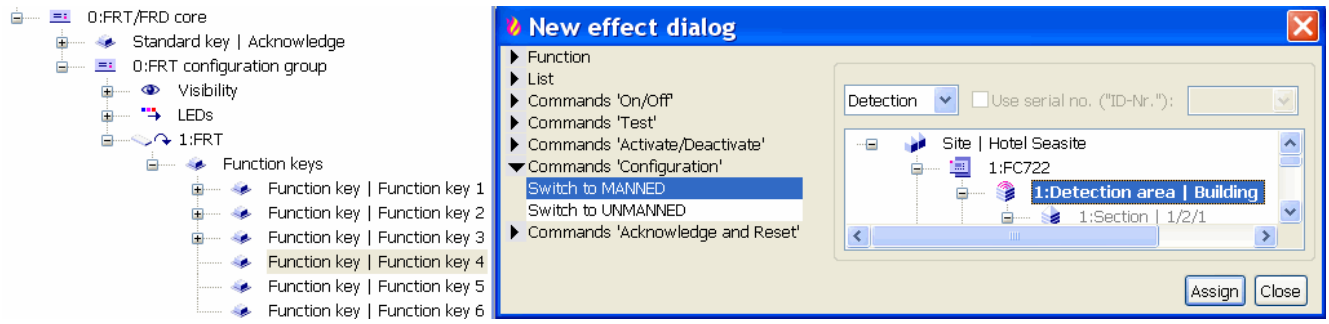
List name	Colour	LED mode
• 'ALARM' • 'Alarm delay off' • 'FAULT' • 'ISOLATION' • 'PRE-ALARM' • 'TECHNICAL' • 'Undefined'	• LED 1: Red, Yellow • LED 2: Red, Yellow • LED 3: Yellow • LED 4: Green, Yellow • LED 5: Green, yellow • LED 6: Yellow	• 'Intermittent' • 'Intermittent, fast' • 'Intermittent, short period' • 'Off' • 'On'

Assignable LED causes

The visibility must be configured on the corresponding category, so that the LED becomes active.

8.4.3.4 Function keys

Frequently used commands can be assigned to the function keys, e.g.: Activate/Deactivate, Test, Configuration ('Set PS MANNED', 'Switch to UNMANNED', etc.).



'Assign dialog' window for assigning a function

To assign a function to the function keys, proceed as follows:

1. Select the 'Operation' task card.
2. In the tree view, open 'Station' > 'FRT/FRD core' > in the 'FRT configuration group' > 'FRT' > 'Function keys' example.
3. Highlight the corresponding 'Function key'.
4. Open the 'Assign dialog' window.
5. In the window, select 'Commands 'Configuration'', for example, followed by a function.

   ⇨ The Detection tree is now shown. The elements that can be linked are highlighted.
6. Highlight 'Area', for example, and click on the 'Assign' button.

⇨ 'Function key' is linked to 'Area'.

Assigning commands

Commands are assigned in the same way as with standard keys. See [→ 149]

The visibility must also be configured on the corresponding category, so that the function key becomes active.

8.4.4 LED indicator FTO2002 and mimic display driver FT2001

The following devices can be used as a mimic display:

- LED indicator FTO2002: For installation in the control panel. This contains 24 LED groups with one red and one yellow LED each.
- Mimic display driver FT2001: It controls up to 48 LEDs that are installed on a ground plan panel. Communication is via the C-NET.

  The mimic display driver has:
  – Two control outputs for local buzzer and 'LED 'System ON"
  – Two inputs for 'Silence buzzer' and 'START LED test'

There are two elements for creating the mimic display in the 'Operation' task card:

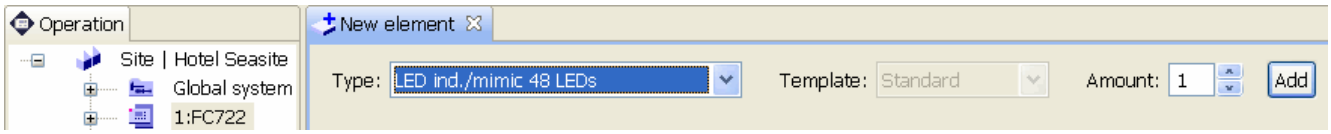
- 'LED ind./mimic 24 LED groups'

  The 'LED ind./mimic 24 LED groups' element can be used to configure the visibility of each LED group (red/yellow) for a section or zone.
- 'LED ind./mimic 48 LEDs'

  Each LED can assign any event to the 'LED ind./mimic 48 LEDs' element.

Both elements must be produced.

Pre-configuration



Window 'New element' for creating the mimic display

To create the mimic display, proceed as follows:

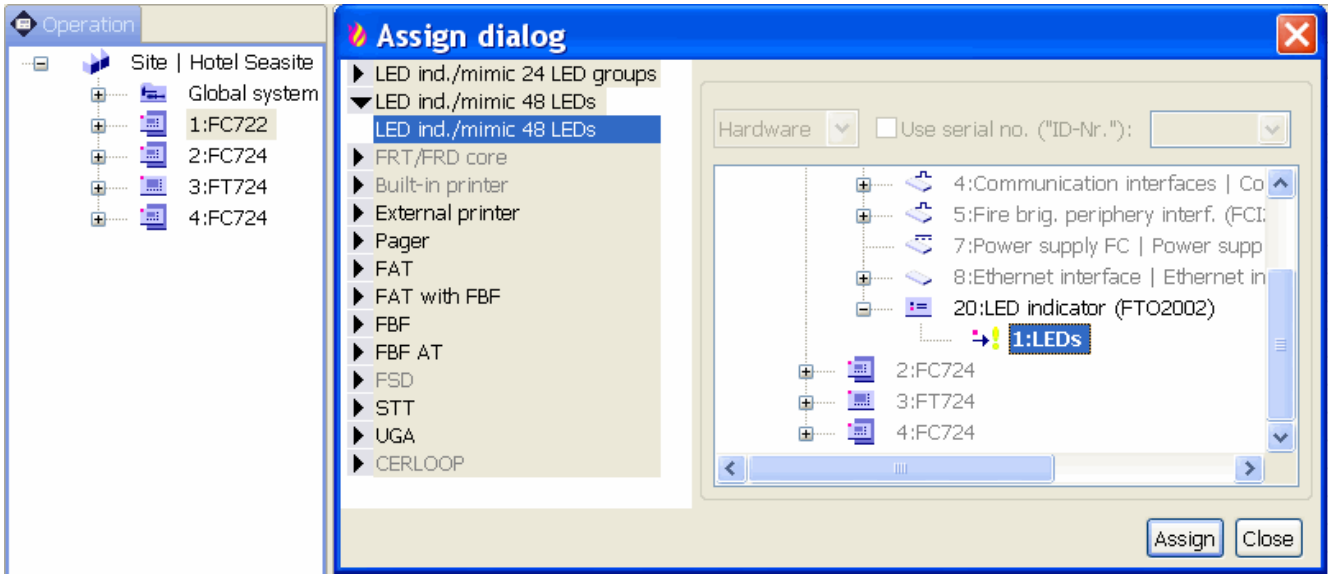
1. Select the 'Operation' task card.
2. Highlight the 'Station' in the tree view.
3. Open the 'New element' window.
4. Select, for example, the 'LED ind./mimic 48 LEDs' element in the 'Type:' field.
5. Enter the number of elements required in the 'Amount:' field and click on the 'Add' button.

⇨ The 'LED ind./mimic 48 LEDs' elements are created.

- Enter the customer text(s).

In a later step once the hardware has been read in and is loaded in Cerberus-Engineering-Tool, the hardware must still be linked via the Assign function.

When the hardware has already been read in



Window 'Assign dialog' for creating and linking the mimic display

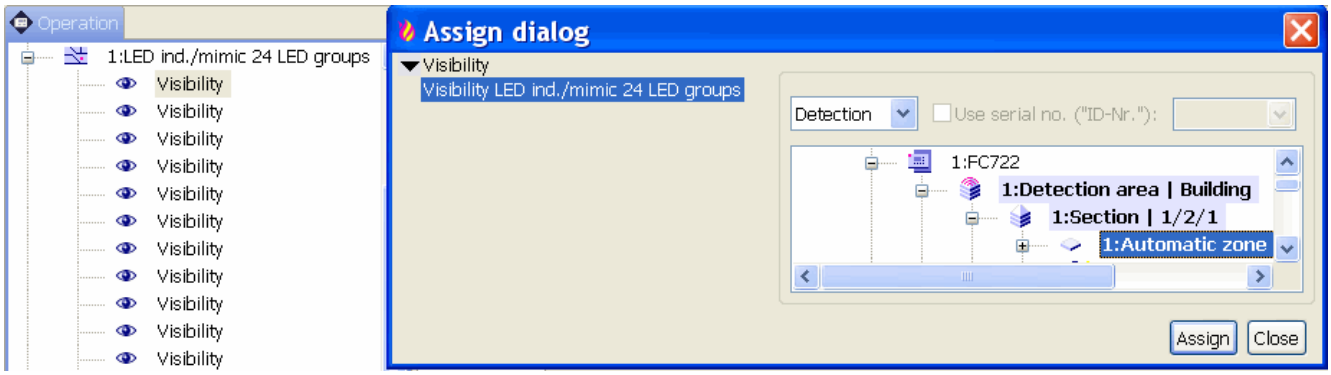
To create and link the mimic display, proceed as follows:

1. Select the 'Operation' task card.
2. Highlight the 'Station' in the tree view.
3. Open the 'Assign dialog' window.
4. Highlight 'LED ind./mimic 48 LEDs', for example.
5. In the hardware tree, select the corresponding 'LEDs' element (LED indicator FTO2002) or 'LEDs/outputs' (FT2001).
6. Click on the 'Assign' button.

⇨ The mimic display is created and linked with the hardware.

8.4.4.1 Element 'LED ind./mimic 24 LED groups'

Assigning events



Window 'Assign dialog' for linking a 'Visibility' of the element 'LED ind./mimic 24 LED groups' with an event

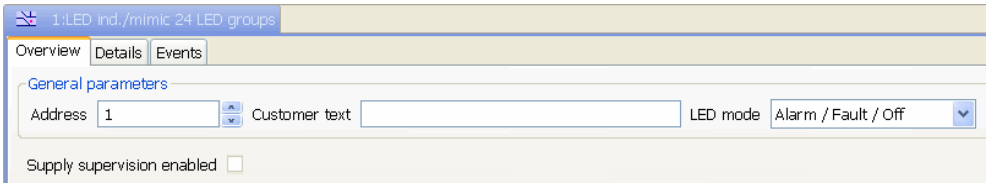
To link the 'LED ind./mimic 24 LED groups' element with an event, proceed as follows:

1. Select the 'Operation' task card.
2. Open 'LED ind./mimic 24 LED groups' in the tree view.
3. Highlight a 'Visibility' element.
4. 'LED ind./mimic 24 LED groups' is highlighted at the left of the window.
5. In the Detection tree, select the Section or the Zone.
6. Click on the 'Assign' button.

⇨ The 'Visibility' element of LED ind./mimic 24 LED groups' is linked to the section or zone.

- Repeat these steps for each 'Visibility' element (each 'Visibility' element corresponds to one of the 24 LED groups, from top to bottom).

Features



Detail editor 'LED ind./mimic 24 LED groups', 'Overview'

In the detail editor of the 'LED ind./mimic 24 LED groups' element, the following properties can be set:

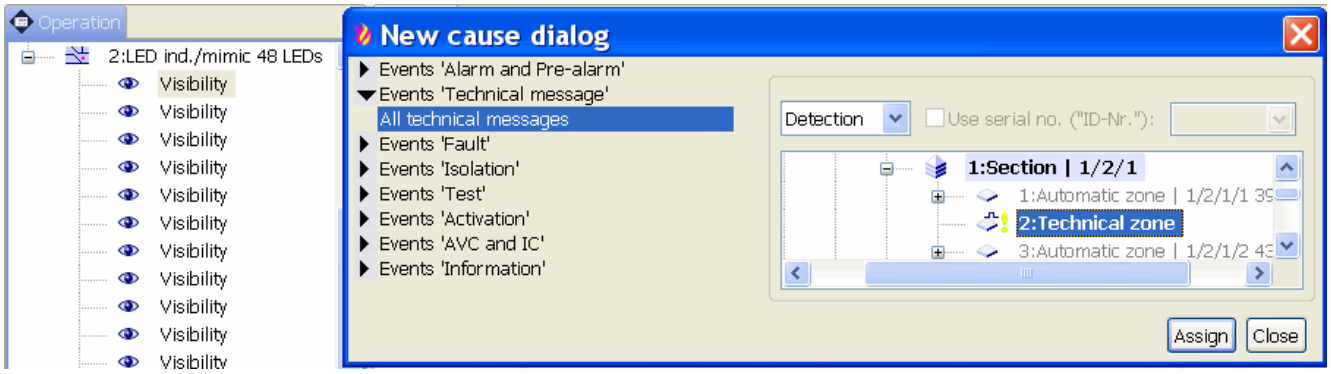
- 'LED mode': Defines which statuses for the referenced element are indicated by the LEDs in an LED group.

  Alarm and fault:
  – Red LED: alarm (activation in Fire/Evac controls) -> LED permanently on.
  – Yellow LED: fault -> LED intermittent
  Alarm, fault and off:
  – Red LED: alarm (activation in Fire/Evac controls) -> LED permanently on.
  – Yellow LED: fault -> LED intermittent, Off -> LED permanently on.
  Note: the criterion is met when at least one event of the corresponding event category occurs in the referenced element or in its sub-tree.

- 'Supply supervision enabled': Defines whether a local supply that is to be monitored is present.

8.4.4.2 Element 'LED ind./mimic 48 LEDs'

Assigning events



Window 'Assign dialog' for linking a 'Visibility' of the element 'LED ind./mimic 48 LEDs' with an event

To link the 'LED ind./mimic 48 LEDs' element with an event, proceed as follows:

1. Select the 'Operation' task card.
2. Open 'LED ind./mimic 48 LEDs' in the tree view.
3. Highlight a 'Visibility' element.
4. In the 'Assign dialog' window, highlight an event category, e.g., 'All technical messages'.
5. Select an element from the tree you want, e.g., 'Technical zone' from the Detection tree.
6. Click on the 'Assign' button.

   ⇨ The 'Visibility' element of 'LED ind./mimic 48 LEDs' is linked to the event category.
7. Repeat these steps for each 'Visibility' element (each 'Visibility' element corresponds to one of the 48 LEDs, from top to bottom).

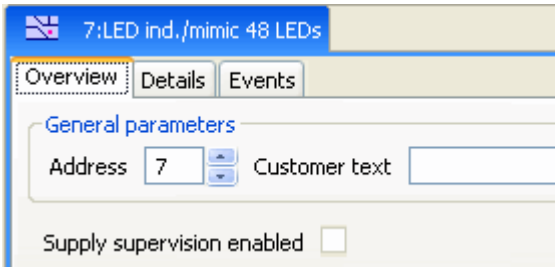
The table below provides an overview of the events which can be assigned to an LED. An event can be assigned to any LED.

Event category	Cause	Link with
Outputs with confirmation	All Fire ALARMS '--All autom. Fire ALARMS '----Autom. First ALARM '----General autom. Fire ALARM '----Exting. pre-alarm (Aut. Fire AL.) '----Exting. discharged (Aut. Fire AL.) '--Manual Fire ALARM All Pre-ALARMS	Hardware tree Detection tree
	'--Degraded Fire ALARM	Hardware tree
Events 'Technical message'	All technical messages	Detection tree Operation tree
Events 'Fault'	All faults '--Other fault '--All system faults '----System fault: general connection fault '----System fault: module '----Other system fault '--Mains failure '--Battery failure '--Emergency power operation	Hardware tree Detection tree Control tree Operation tree Network tree
Events 'Isolation'	All isolations '--Other isolation '--Temporary isolation '--Alarm evaluation OFF '--Sub-system isolation '--Automatic extinguishing release OFF '--Autom.+man. extinguishing release OFF '--Renovation mode "--Not ready '--Fire related controls OFF '--RT FIRE channels OFF '--Sounders OFF	Detection tree
Events 'Test'	All test modes '--Detector test mode '--Installation test mode '--Control test mode All test activations '--Test activation ALERT '--Test activation EVAC '--Other test activation	Detection tree Control tree

Event category	Cause	Link with
Events 'Activation'	All activations '--Activation/ALERT '--Activation/EVAC '--Other activation '--Activation/confirmed '--Activation/NOT active '--Activation/unexpected	Detection tree Control tree Operation tree
Events 'AVC and IC'	AVC, Fire ALARM AVC, Pre-ALARM	Detection tree
	IC, Technical IC, Fault IC, Isolation IC, Test IC, Activation IC, Information	Station
Events 'Information'	Manned operation Unmanned operation Service information: Service required Access level <> default level '--Access level 1 '--Access level 2.1 '--Access level 2.2 '--Access level 3 Expiry reminder of time lim. isol. Other information Visibility	Hardware tree Detection tree

Events which can be assigned

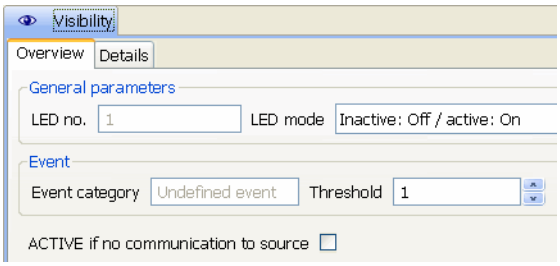
Features



Detail editor 'LED ind./mimic 48 LEDs', 'Overview'

In the detail editor of the 'LED ind./mimic 48 LEDs' element, the following properties can be set:

- 'Supply supervision enabled': Defines whether a local supply that is to be monitored is present.

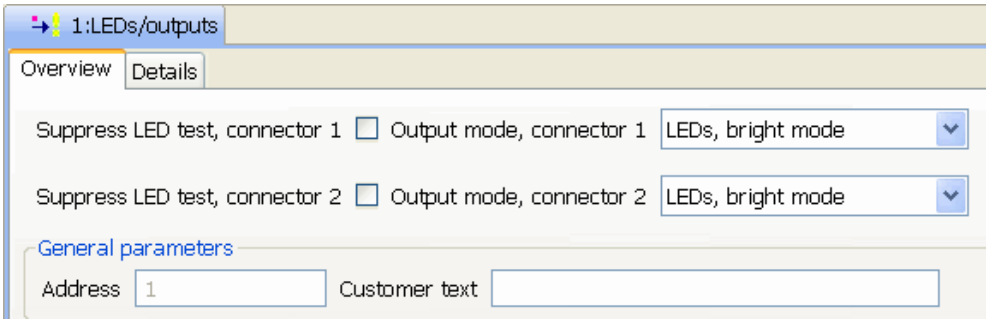


'Visibility', 'Overview' detail editor

In the detail editor of the 'Visibility' element, the following properties can be set:

- 'LED mode': Defines the mode of the LED in an active or inactive status.
- 'Threshold': Defines how many events from the defined event category need to be active at the same time in the assigned element or its subtree for the cause to be considered active by the control.
- 'ACTIVE if no communication to source': Defines the cause's default status (active or quiet) in the event of communication to the station where the referenced element is stored being interrupted.

8.4.4.3 Configuring mimic display driver FT2001



Detail editor 'LEDs/outputs'

In the detail editor the following properties can be set:

- 'Suppress LED test, connector 1', 'Suppress LED test, connector 2'

  Blocks the triggering of an LED test of the outputs on connection 1 or 2 via the local input (checkmark placed).

- 'Output mode, connector 1', 'Output mode, connector 2'

  Active mode of outputs connected to connection 1 or 2:
  – 'LEDs, bright mode'
  – 'LEDs, dimmed mode'
  – 'Relays'

See also

Element 'LED ind./mimic 48 LEDs' [→ 169]

8.4.5 Event printer

An event printer can be connected to a Station as an integrated variant or remote variant. It is connected via a communication module. The event printer logs all the site events which have the visibility that it is configured for.

Recommended printer:

Variants	Printer type	Interface
Integrated	FTO2001	RS232 interface
Remote	Fujitsu DL3750+	RS232 interface or Ethernet interface
Remote	Any printer or IBM ProPrint log	RS232 interface (no printer monitoring)

For remote printer Fujitsu DL3750+ see also document A6V10224853, external printer, information relating to application.

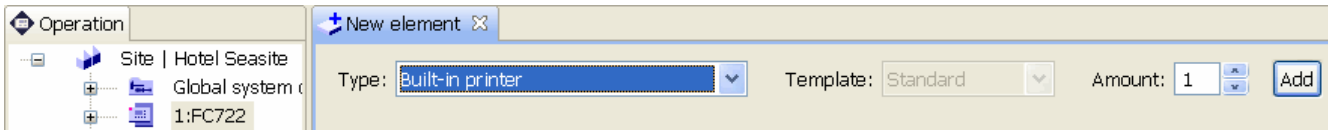
!	*NOTICE*
	Overvoltage Device defect ● The RS232 module may only be inserted or removed when the Station is current-free.

The RS232 and RS845 interfaces are read in when the Station is started up.

A distinction is made in the 'Operation' task card between two elements which have to be created and linked to the hardware:

- 'Built-in printer'
- 'External printer'

Pre-configuration



Window 'New element' for creating the printer

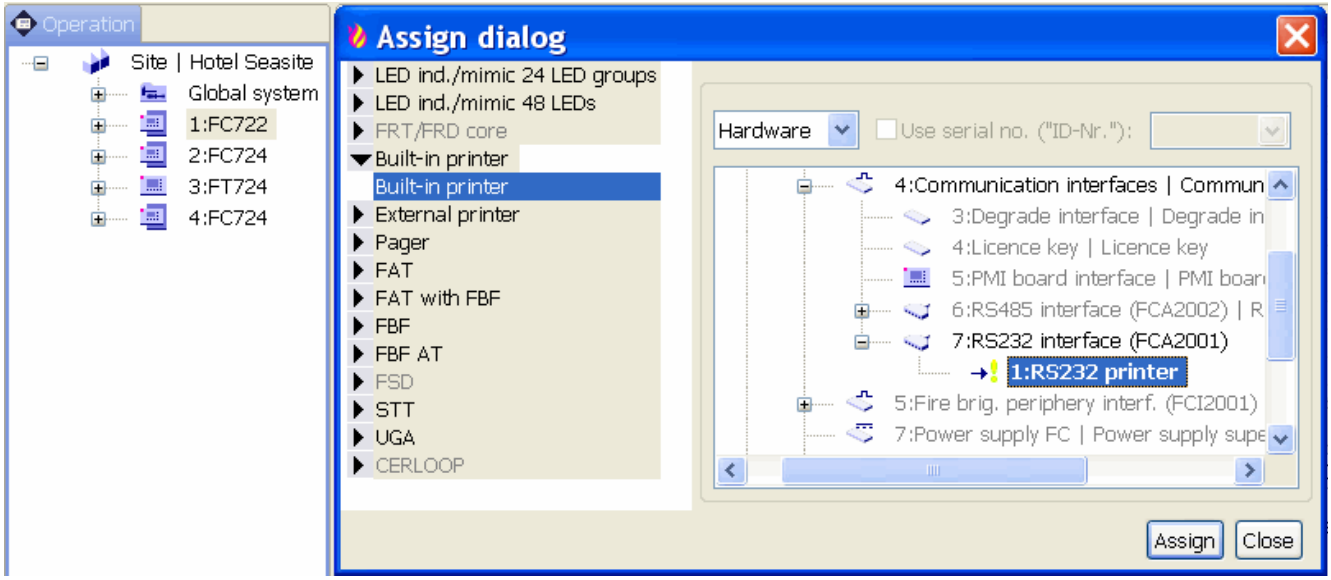
To create the 'Built-in printer'/'External printer' element, proceed as follows:

1. Select the 'Operation' task card.
2. In the tree view, highlight the 'Station' with the interface to which the printer is connected.
3. Open the 'New element' window.
4. In the 'Type:' field, select the 'Built-in printer'/'External printer' element and click on the 'Add' button.

⇨ The element is created.

In a later step, once the hardware has been read in and is loaded in the Cerberus-Engineering-Tool, the element still has to be linked to the hardware via the Assign function.

When the hardware has already been read in



Window 'Assign dialog' for creating and linking the element 'RS232 printer' or 'Ethernet printer'

To create the 'Built-in printer'/'External printer' element and link it to the hardware, proceed as follows:

1. Select the 'Operation' task card.
2. In the tree view, highlight the 'Station' with the interface to which the printer is connected.
3. Open the 'Assign dialog' window.
4. In the 'Assign dialog' window, select 'Built-in printer'/'External printer'.
   ⇨ In the Hardware tree, the 'RS232 printer'/'Ethernet printer' element is highlighted under 'RS232 interface (FCA2001)'/'Ethernet interface'.
5. Highlight the element and click on the 'Assign' button.

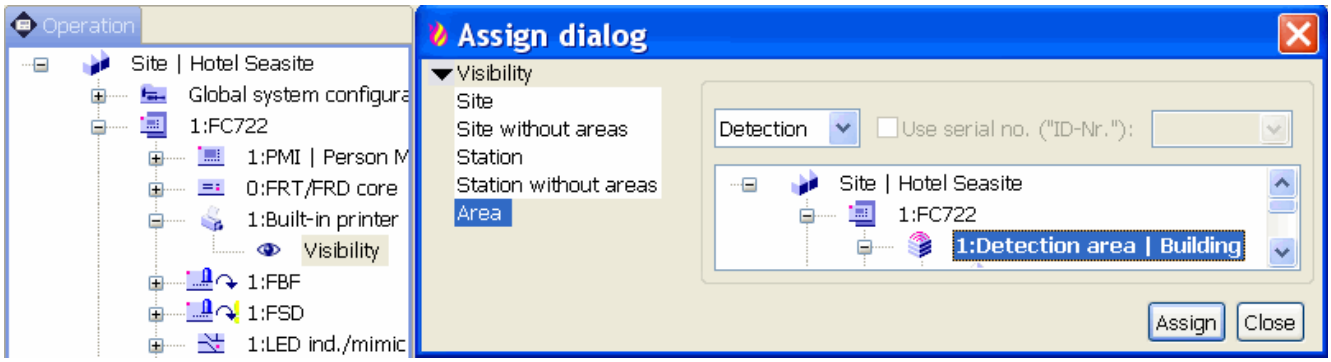
⇨ The element is created and linked with the hardware.

Visibility configuration

In the 'Visibility' element, it is possible to define which stations and areas can be logged in the printer to be configured.

The following selection is available:

- 'Site': Visibility across the entire site
- 'Site without areas': Visibility for all events from the Hardware tree for the site.
- 'Station': Visibility for a Station within the site, with all areas in this Station
- 'Station without areas': Visibility for all events from the Hardware tree of the Station
- 'Area': Visibility for an area within a control panel



'Assign dialog' window for linking the visibility

To configure the visibility, proceed as follows:

1. Select the 'Operation' task card.
2. In the tree view, open 'Built-in printer'/'External printer' and highlight 'Visibility'.
3. Open the 'Assign dialog' window.

   ⇨ 'Visibility' list and Hardware tree or detection tree are displayed.
4. Select the site, station, or area and click on the 'Assign' button (you can link the visibility to several elements).

⇨ 'Visibility' is linked to the corresponding element.

8.4.6 Fire department periphery [DE]

The fire department periphery comprises the following devices:

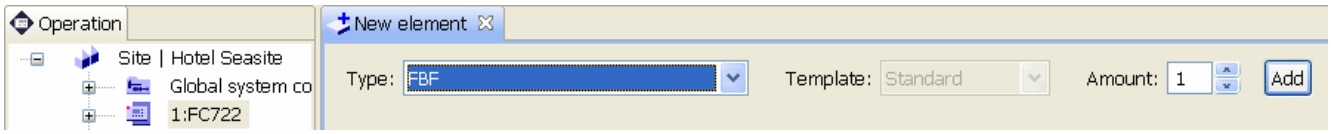
- FBF: fire department operating panel
- FSD: fire department key depot
- FAT: fire department indication panel
- FAT with FBF: fire department indication panel with fire department operating panel
- FSE: releasing element (see [→ 85])

The devices are connected as follows:

- FSD is assigned to the fire department periphery module FCI2001.
- FBF can either be connected via the fire department periphery module FCI2001 or an RS485 interface.
- FAT and FAT with FBF are connected to the Station via an RS485 serial interface.

To configure the devices, the logical element must be created in the 'Operation' task card and linked with the corresponding hardware element.

Pre-configuration



'New element' window for creating the logical element

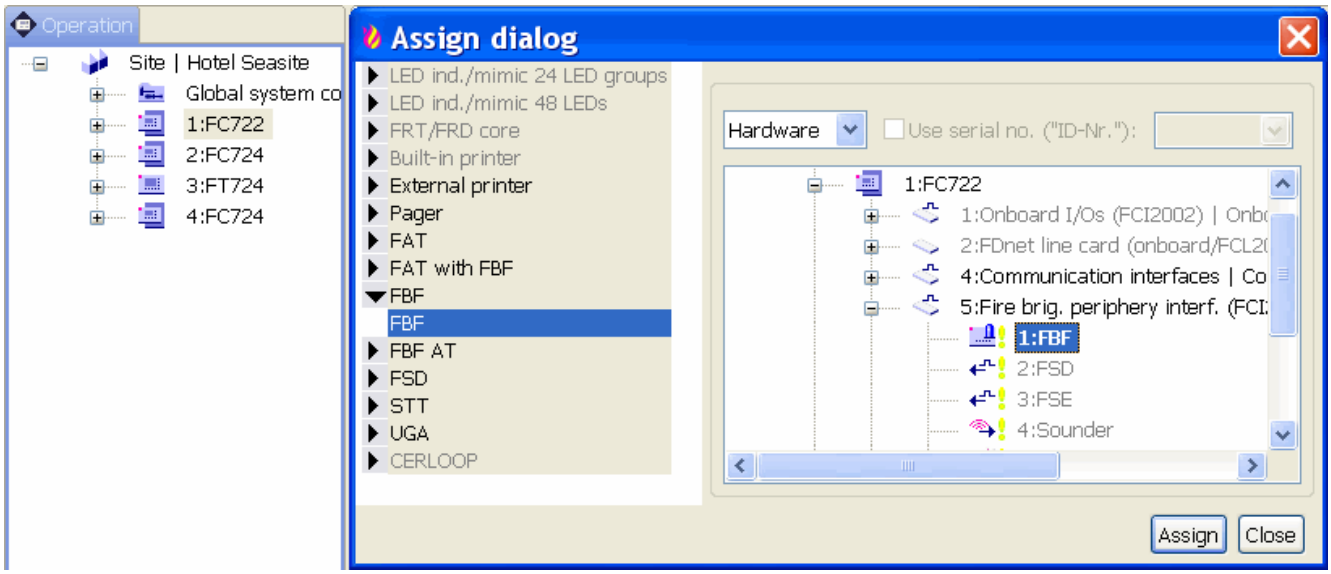
To create the logical element, proceed as follows:

1. Select the 'Operation' task card.
2. Highlight the 'Station' in the tree view.
3. Open the 'New element' window.
4. In the 'Type:' field, select the element (FBF, FSD, FAT, FAT with FBF) and click on the 'Add' button.

   ⇨ The element is created.
5. Enter the customer text(s).

In a later step, once the hardware has been read in and is loaded in the Cerberus-Engineering-Tool, the element still has to be linked to the hardware via the Assign function.

When the hardware has already been read in



'Assign dialog' window for creating and linking the logical element

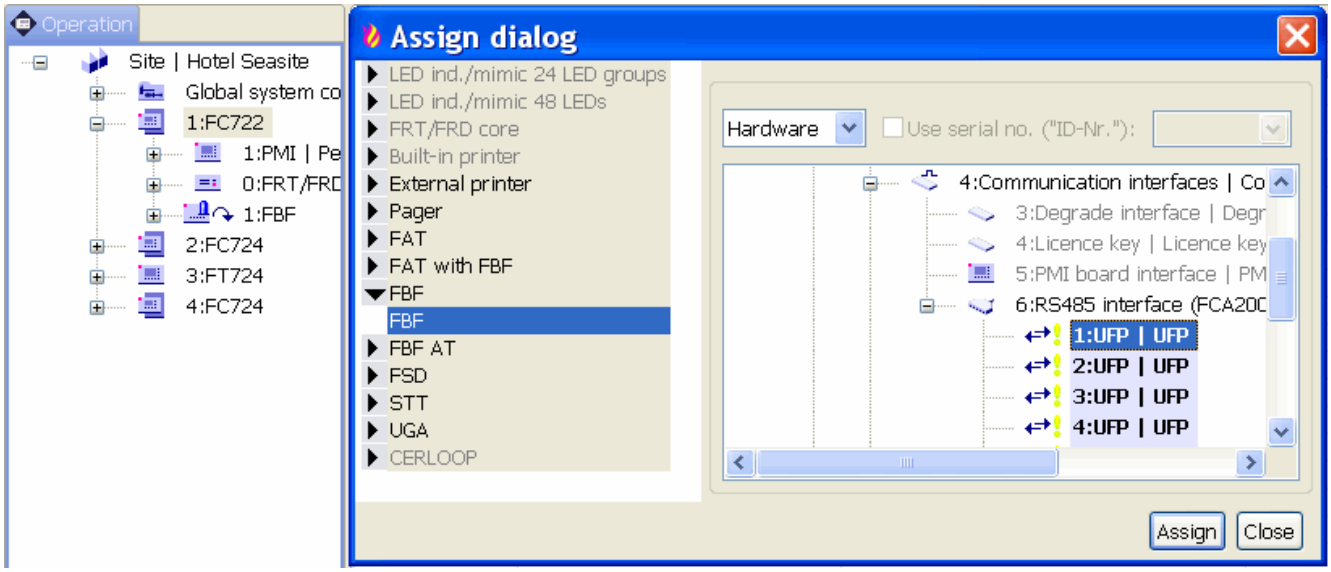
To create the device logical element and link it to the fire department periphery module, proceed as follows:

1. Select the 'Operation' task card.
2. Highlight the 'Station' in the tree view.
3. Open the 'Assign dialog' window.
4. Select the corresponding element (FBF, FSD, FAT, FAT with FBF) in the list.

   ⇨ The Hardware tree is shown.
5. Highlight the relevant element in 'Fire brig. periphery interf. (FCI2001)'.
6. Click on the 'Assign' button.

⇨ The element is created and linked with the hardware.

Connecting with RS485



'Assign dialog' window for creating and linking with the RS485 interface

To create the logical FBF or FAT element and link it to the RS485 interface (FCA2002), proceed as follows:

1. Select the 'Operation' task card.
2. Highlight the 'Station' in the tree view.
3. Open the 'Assign dialog' window.
4. Select the corresponding element (FBF or FBF) in the list.

   ⇨ The Hardware tree is shown.
5. Highlight a 'UFP' element in 'RS485 interface (FCA2002)'.
6. Click on the 'Assign' button.

⇨ The element is created and linked to the RS485 interface (FCA2002).

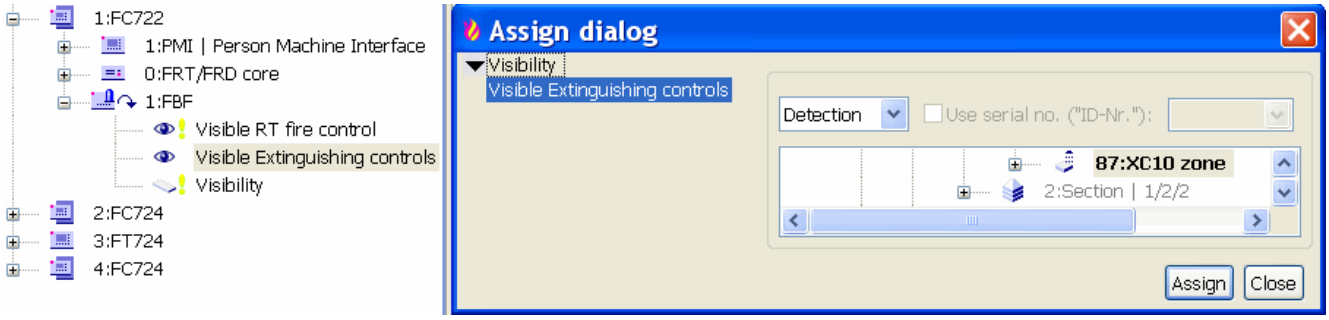
Configuring visibility

The following visibilities can be configured:

- Fire department operating panel FBF:
  - Visibility on the remote transmission control FIRE
  - Visibility on the extinguishing controls
  - Visibility:
    'Site': Visibility across the entire site
    'Area': Visibility for an area within a control panel
    'Station': Visibility for a Station within the site, with all areas in this Station
- Fire department key depot FSD:
  - Visibility on the remote transmission control FIRE

- Fire department indication panel FAT:
  - Visibility:
    'Site': Visibility across the entire site
    'Site without areas': Visibility for all events from the Hardware tree for the site.
    'Station': Visibility for a Station within the site, with all areas in this Station
    'Station without areas': Visibility for all events from the Hardware tree of the Station
    'Area': Visibility for an area within a control panel
- Fire department indication panel FAT with fire department operating panel FBF:
  - same visibilities as FAT and/or FBF

The visibilities for 'Site', 'Area', and 'Station' can be restricted further so that, for example, only the alarm and fault event categories are displayed instead of all events for an area.

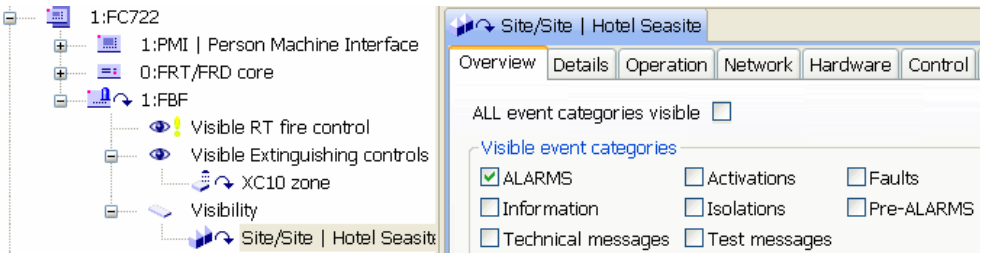


Configuring visibility of logical elements

To configure the visibility, proceed as follows:

1. Select the 'Operation' task card.
2. In the tree view open the element to be configured, e.g. 'FBF'.
3. Highlight an element, e.g., 'Visible Extinguishing controls'.
4. Open the 'Assign dialog' window.
   ⇨ 'Visible Extinguishing controls' is highlighted:
5. Select the corresponding element in the control tree and click on the 'Assign' button.

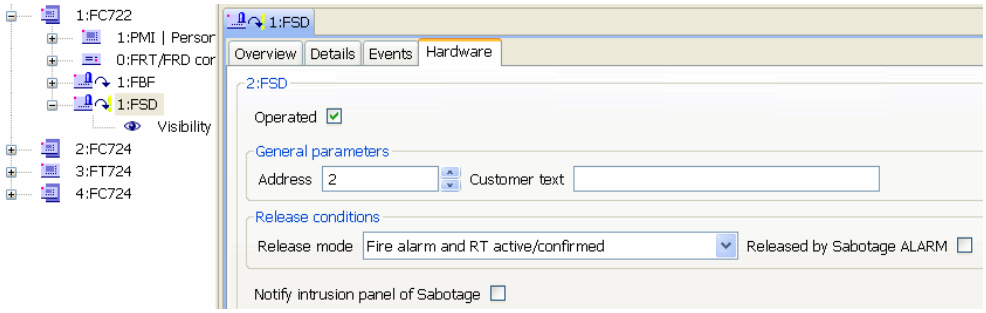
⇨ 'Visible Extinguishing controls' is linked to the element.



'FBF' detail editor for selecting certain event categories

One or more event categories can be selected in the detail editor of the linked elements (remove checkmark from 'ALL event categories visible').

Operation of the fire department key depot (FSD)



'FSD', 'Hardware' detail editor

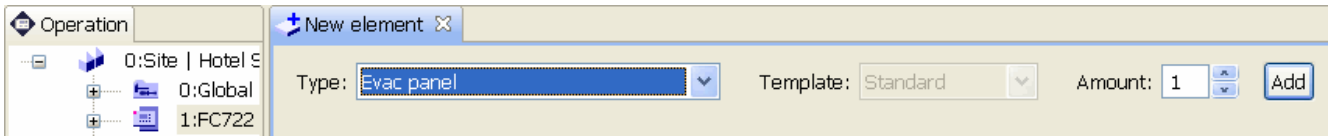
In the detail editor ('Hardware'), there are special settings for the fire department key depot FSD if the box in the 'Operated' field contains a checkmark:

- 'Release mode': You can select when the fire department key depot is to be unlocked:
  - 'RT active/confirmed'
  - 'Fire alarm and RT active/confirmed'
  - 'RT active/confirmed or RT active/unexpected'
- 'Released by Sabotage ALARM': If the box contains a checkmark, the fire department key depot is also unlocked by a sabotage alarm.
  The sabotage alarm is activated by a door contact fitted in the Station. For service purposes, the function can be switched off at the Person Machine Interface before the Station is opened.
- 'Notify intrusion panel of Sabotage': If the box contains a checkmark, the specific output for notifying an intrusion detection system is activated in the event of an FSD sabotage message.

8.4.7 EVAC panel [NL]

The EVAC panel is an operating and indication unit for manual evacuation control, integrated in the Person Machine Interface of the control panel or remotely connected via an RS485 interface. The EVAC panel consists of a master and up to four slaves. Master and slave both have up to ten indicators for the evacuation zones. Both the universal and 2-stage evacuation control are suited to automatic evacuation.

'Evac panel': Creating and linking to the hardware

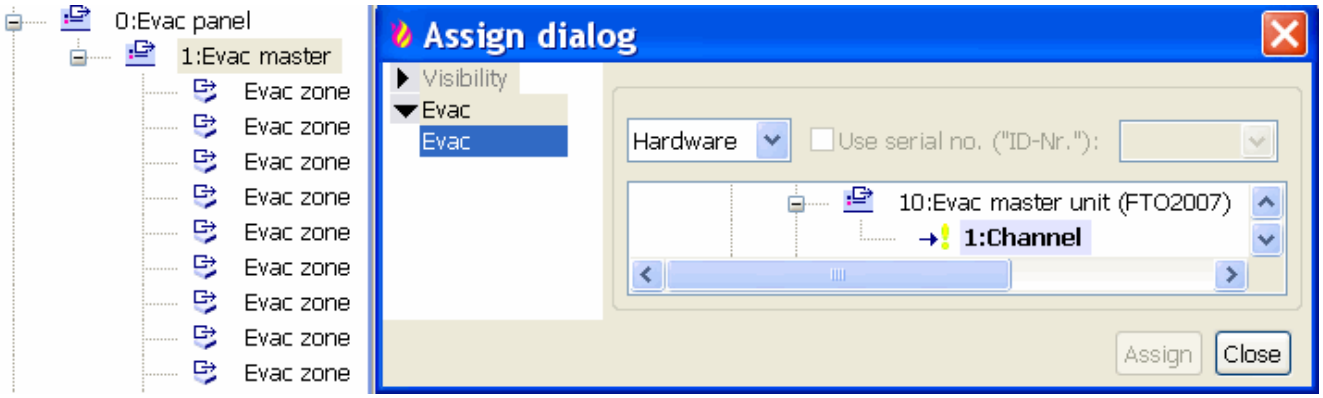


Window 'New element' for creating the element 'Evac panel'

To create the 'Evac panel' element, proceed as follows:

1. Select the 'Operation' task card.
2. Highlight the 'Station' in the tree view.
3. Open the 'New element' window.
4. In the 'Type:' field, select the 'Evac panel' element and click on the 'Add' button.

⇨ The 'Evac panel' element is created along with the 'Evac master' element.



Window 'Assign dialog' for linking the element 'Evac master'

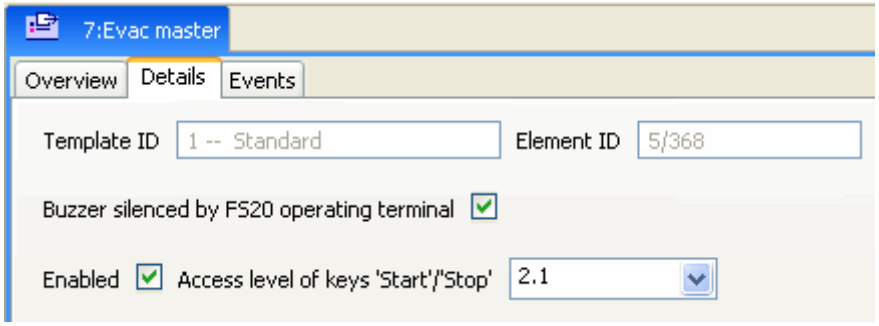
To link the 'Evac master' element to the hardware, proceed as follows:

1. Highlight the 'Evac master' element in the tree view.
2. Open the 'Assign dialog' window.

   ⇨ The hardware tree is depicted. The 'Channel' element that can be linked is highlighted in the 'Evac master unit (FTO2007)' element.
3. Click on the 'Assign' button.

⇨ 'Evac master' is linked to 'Channel'.

Properties of the 'Evac master' element

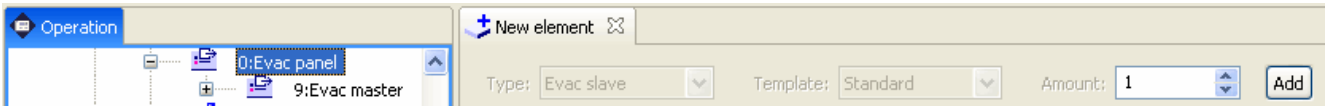


Detail editor 'Evac master', 'Details'

In the detail editor of the 'Evac master' element ('Details'), the following properties can be set:

- 'Buzzer silenced by FS720 operating terminal': Defines whether silencing the buzzer on theFS720 operating terminal also silences the buzzer of the Evac panel.
- 'Access level of keys 'Start'/'Stop'': Defines the access level required to execute the functions of the 'Start' and 'Stop' keys.

'Evac slave': Creating and linking to the hardware

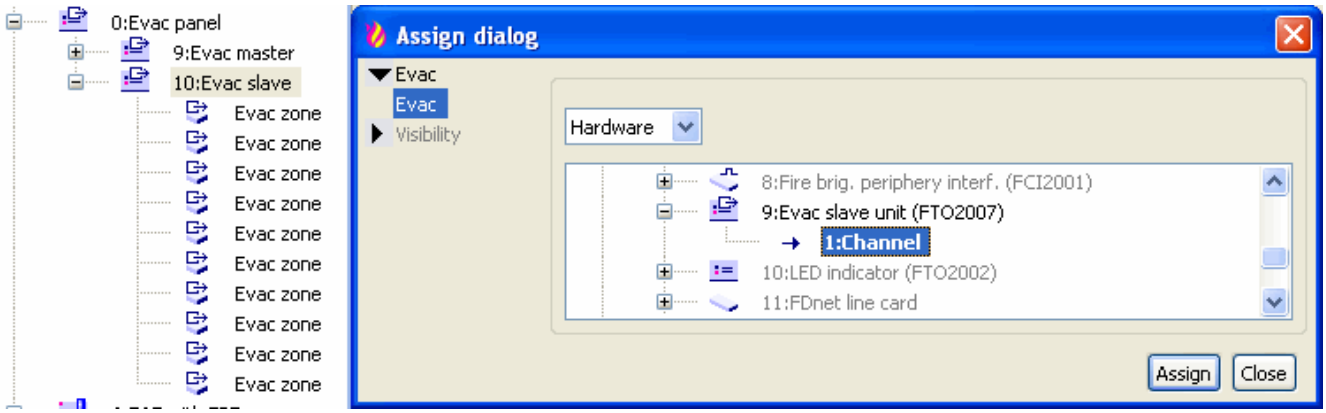


Window 'New element' for creating the element 'Evac slave'

To create the 'Evac slave' element, proceed as follows:

1. Select the 'Operation' task card.
2. Highlight the 'Evac panel' element in the tree view.
3. Open the 'New element' window.
4. The 'Evac slave' element is selected in the 'Type' field. Click on the 'Add' button.

⇨ The required number of 'Evac slave' elements are created.



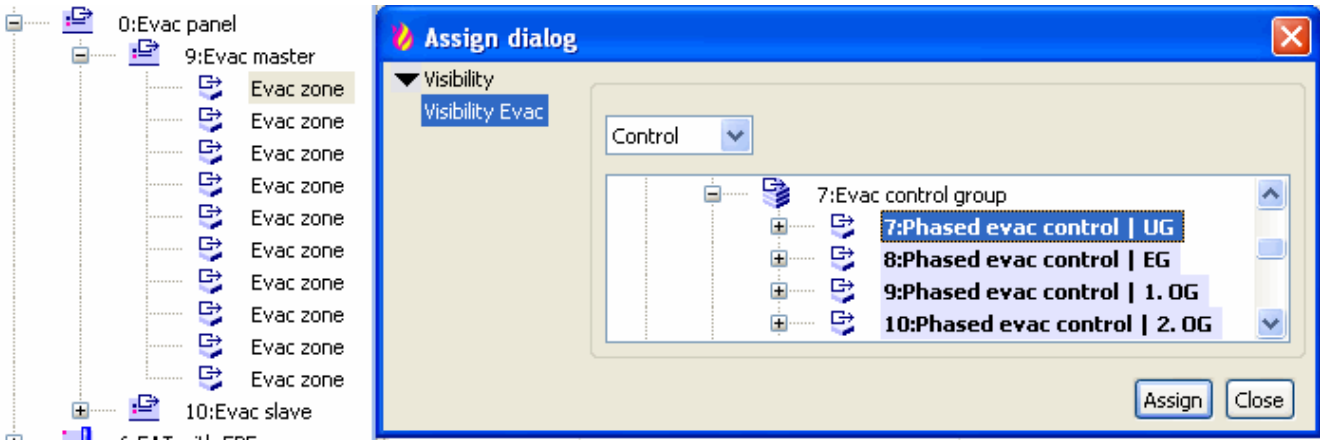
Window 'Assign dialog' for linking the element 'Evac slave'

To link the 'Evac slave' element to the hardware, proceed as follows:

1. In the tree view, highlight the 'Evac slave' element that you have just created.
2. Open the 'Assign dialog' window.
   ⇨ The hardware tree is depicted. The 'Channel' element that can be linked is highlighted in the 'Evac slave unit (FTO2007)' element.
3. Click on the 'Assign' button.

⇨ 'Evac slave' is linked to 'Channel'.

Linking EVAC panel with evac control



Window 'Assign dialog' for linking EVAC panel with evac control

To link an 'Evac zone' element with the evac control, proceed as follows:

1. In the tree view, highlight an 'Evac zone' element in 'Evac master' or 'Evac slave'.
2. Open the 'Assign dialog' window.
   ⇨ The control tree is depicted. The 'Universal evac control'/'Phased evac control' elements that can be linked are highlighted.
3. Click on the 'Assign' button.
   ⇨ 'Evac zone' is linked to 'Universal evac control' or 'Phased evac control'.
4. Repeat these steps for each 'Evac zone' element (each 'Evac zone' element corresponds to one of the ten evacuation zones, from top to bottom).

See also

Events which can be assigned

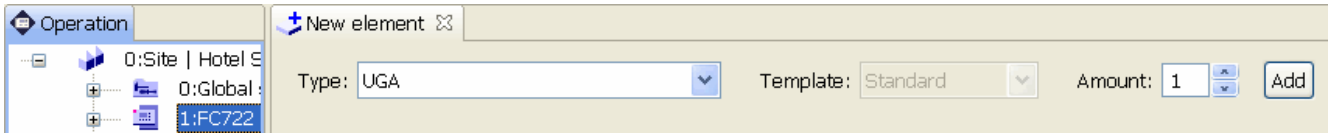
Effect of element 'Universal evac control' [→ 109]

8.4.8 Alarming equipment (UGA) [FR]

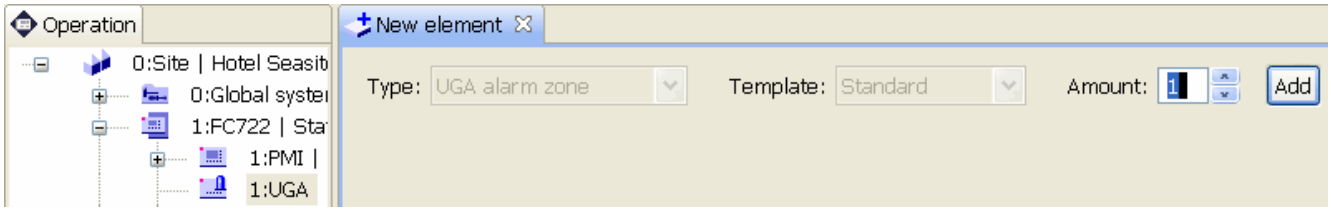
The alarming equipment (UGA) is an operating and indication unit for four alarm zones. The unit has its own control for the alarm devices by alarm zone and its own degraded mode behavior. The alarming equipment is linked to the control panel via an RS485 interface.

To configure the alarming equipment (UGA), the 'UGA' element must be created in the 'Operation' task card and linked to the hardware. Up to four alarm zones can be configured for the alarming equipment.

Creating alarming equipment (UGA) and linking it to the hardware



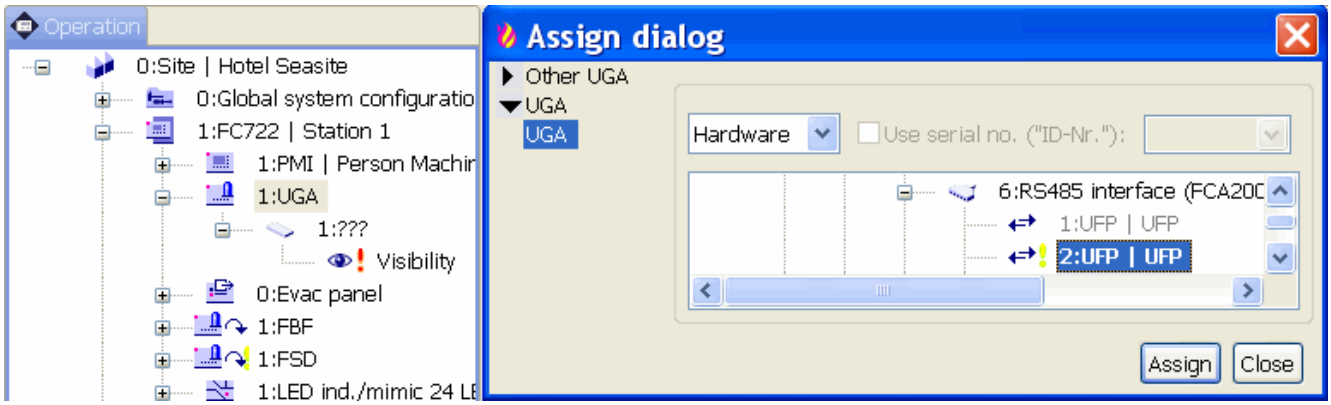
Window 'New element' for creating the elements 'UGA'



Window 'New element' for creating the elements 'UGA alarm zone'

To create the 'UGA' and 'UGA alarm zone' elements, proceed as follows:

1. Select the 'Operation' task card.
2. Highlight the 'Station' in the tree view.
3. Open the 'New element' window.
4. Select the 'UGA' element in the 'Type:' field.
5. Enter the number of elements required in the 'Amount:' field and click on the 'Add' button.
   ⇨ The 'UGA' elements are created.
6. In the tree view, highlight the 'UGA' element you have just created.
   ⇨ The 'UGA alarm zone' element is displayed in the 'Type:' field of the 'New element' window.
7. Enter the number of elements required in the 'Amount:' field and click on the 'Add' button.
8. Enter the customer text(s).



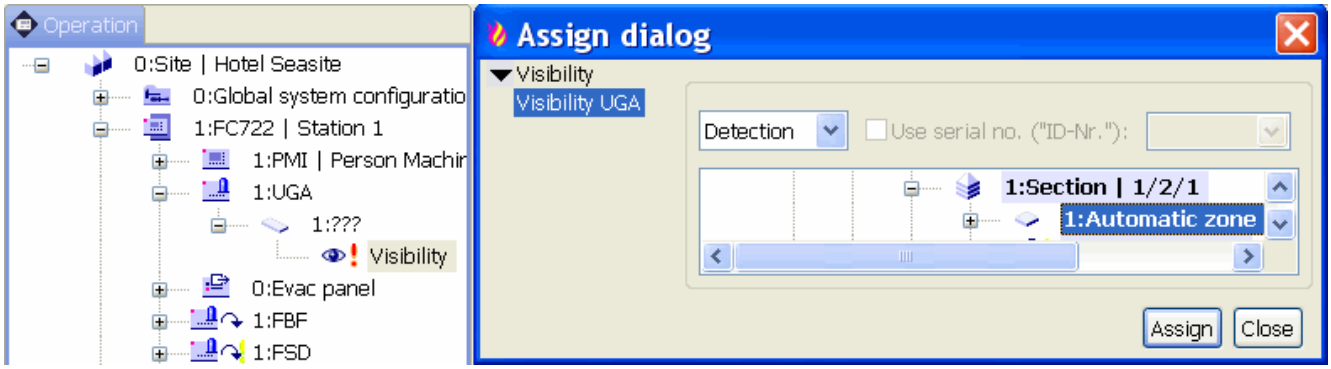
Window 'Assign dialog' for linking the element 'UGA'

To link the 'UGA' elements to the 'UFP' RS485 channel, proceed as follows:

1. Highlight the 'UGA' element in the tree view.
2. Open the 'Assign dialog' window and highlight 'UGA'.
   ⇨ The hardware tree is depicted. The elements that can be linked are highlighted.
3. Select the 'UFP' element.
4. Click on the 'Assign' button.

⇨ 'UGA' is linked to 'UFP'.

Linking the UGA alarm zone with the Area, Section, or Zone



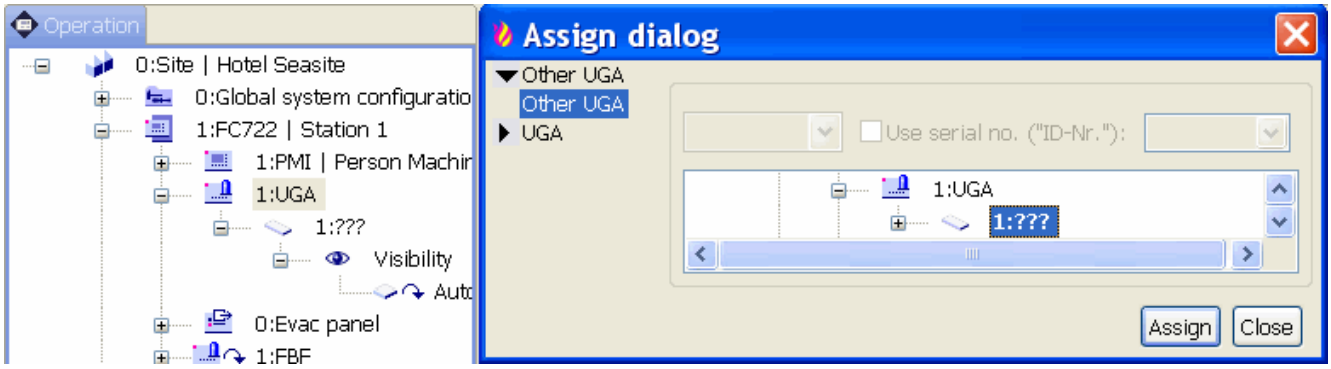
Window 'Assign dialog' for linking the UGA alarm zone

1. Select the 'Operation' task card.
2. In the tree view, open 'UGA' > 'UGA alarm zone' and highlight 'Visibility'.
3. Open the 'Assign dialog' window.
   ⇨ 'Visibility UGA' is highlighted:
4. In the Detection tree, select the relevant 'Area', 'Section', or 'Zone' element.
5. Click on the 'Assign' button.

⇨ 'Visibility' is linked to the corresponding element.

UGA master-slave principle

If UGA 1 is connected to Station 1, then UGA 2, which behaves like a remote UGA 1, can be connected to Station 2. UGA 2 displays the same information as UGA 1, and carrying out operation on UGA 2 has the same effect as carrying out operation directly on UGA 1.



Window 'Assign dialog' for linking the UGA slave alarm zone with the UGA master alarm zone

To link the UGA slave alarm zone to the UGA master alarm zone, proceed as follows:

1. Select the 'Operation' task card.
2. In the tree view, open the second Station and highlight '2:UGA'.
3. Open the 'Assign dialog' window.
   ⇨ 'Other UGA' is highlighted:
4. In the tree, open the first Station and highlight '1:UGA alarm zone'.
5. Click on the 'Assign' button.

⇨ '2:UGA' is linked to '1: UGA alarm zone'.

8.5 'Network' task card

This chapter deals with all aspects related to using networks in an FS720 system. This includes:

- Networking several stations with one another using the C-WEB protocol
- Access to networked stations with:
  - Cerberus-Engineering-Tool
  - Cerberus-Remote
- Networking with BACnet clients, e.g. to integrate an FS720 sub-system in a management station, using the BACnet protocol.

FS720 stations

The stations differ according to their networking and functions:

- Standalone

  Standalone station with local connection for the PC only.

- SAFEDLINK

  Participants in the SAFEDLINK sub-net with local connection for the PC.

- Ethernet

  Participants in the Ethernet sub-net without local connection for the PC.

- CAP

  Connection station between the SAFEDLINK and Ethernet sub-nets and / or central point of access for remote access, e.g. using Cerberus-Engineering-Tool.

Type of access

Access to the stations, e.g. with Cerberus-Engineering-Tool, may take the following forms:

- 'Local connection'

  The PC is connected to the station directly. Cerberus-Engineering-Tool can be used to establish a connection to the station that automatically assigns an IP address to the PC.

- 'Remote access'

  The PC or a BACnet client is linked to the CAP station via an Ethernet network. The PC's IP address must be set manually.

Responsibility for the IP network

When configuring IP addresses in the network, the following distinctions are made:

- Private network

  Fire detection installations are normally equipped with their own cabling. The settings for the networks are defined automatically (recommended). The IP addresses come from a reserved range for private networks.

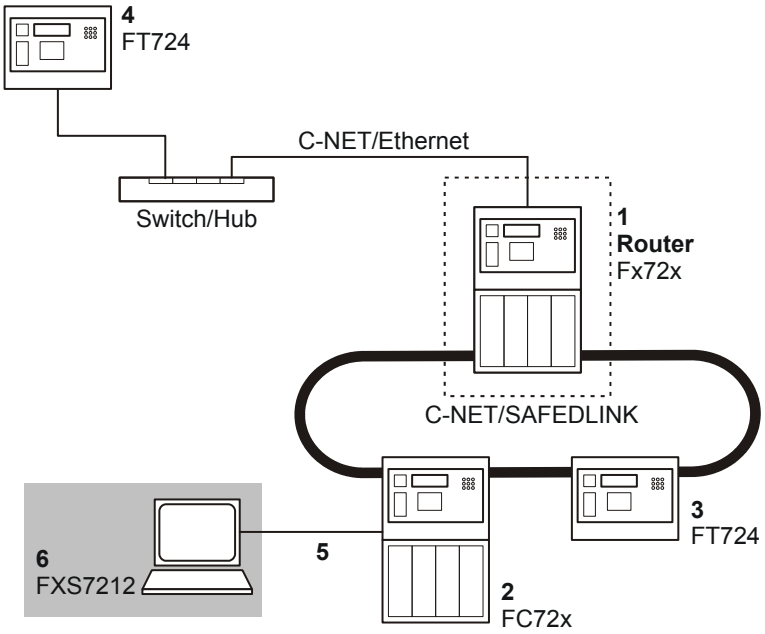
- External network

  Fire detection installations can be incorporated into an existing IT infrastructure as sub-nets (public network). In these cases, the IP settings must be performed according to the IT administrator's instructions.

8.5.1 Stations in the network

Stations can be networked in two ways:

- Via SAFEDLINK (standard for the operation according to EN 54-2)
- Via Ethernet (option for special applications)



SAFEDLINK and Ethernet sub-nets

	Device	Device ID	IP address SAFEDLINK	IP address Ethernet	Network mask
1	Station 1 (CAP station)	1	192.168.0.1	192.168.1.1	255.255.255.0
2	Station 2	2	192.168.0.2	-	255.255.255.0
3	Station 3	3	192.168.0.3	-	255.255.255.0
4	Station 4	4	-	192.168.1.4	255.255.255.0

Automatic addressing for the local sub-net

FS720 uses a simple mechanism for the automatic assignment of IP addresses:

- The last digit of the IP addresses SAFEDLINK and Ethernet includes the device ID number.
- Station 1 is the CAP station and the Ethernet IP address is 192.168.1.1 by default.

- The default gateway is always the IP address of the CAP station in the same sub-net.

There is always a DHCP server for the Cerberus-Engineering-Tool local connection running on all SAFEDLINK stations. The corresponding SAFEDLINK station contains the IP address 192.168.200.1.

	Device	IP address SAFEDLINK	Network mask
2	SAFEDLINK station	192.168.200.1	
5	Cerberus-Engineering-Tool sub-net	192.168.200.0	255.255.255.0
6	PC with Cerberus-Engineering-Tool	192.168.200.5	

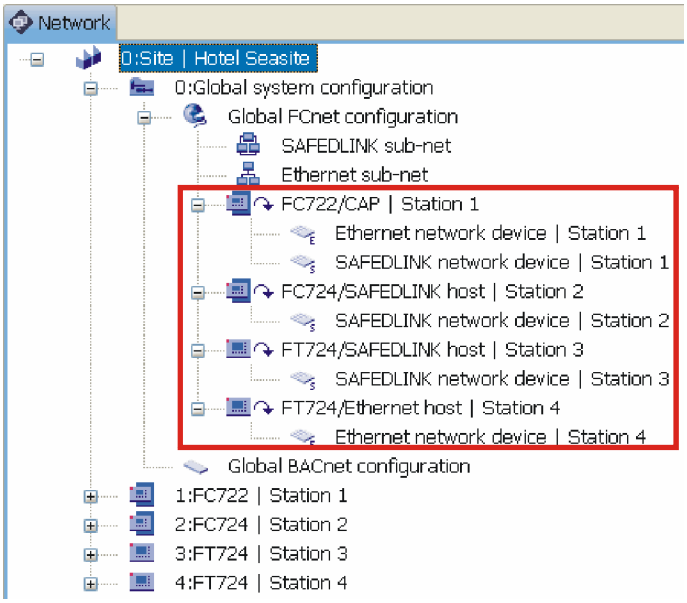
Automatic addressing for directly connecting the PC

8.5.2 Global C-WEB configuration

8.5.2.1 Creating a station

In order to create networked stations, the sub-net (SAFEDLINK or Ethernet) must be selected. If a stand-alone station is created first and several stations are then added to the system, the stand-alone station automatically adopts the network of the first station added.

When stations are created, references for the stations are generated in the 'Network' task card, e.g., 'FC724/SAFEDLINK host'. These can be found in the 'Global FCnet configuration' element. A 'SAFEDLINK sub-net' or 'Ethernet sub-net' element is also created for every network used.



Network tree with the station references

See also

Creating a station [→ 39]

8.5.2.2 Defining a station as CAP

One selected station is defined as the CAP (Central Access Point). In its function as an IP router, the CAP station links the SAFEDLINK and Ethernet and also enables Ethernet-based remote access (using Cerberus-Engineering-Tool) or BACnet clients to be connected.

The CAP station is created by converting the 'Fx72x/SAFEDLINK host' or 'Fx72x/Ethernet host' reference to 'Fx72x/CAP'.

Note: As an IP router, the CAP station prevents private addresses from the SAFEDLINK sub-net being disclosed in a public network (sub-net is not "announced"). The partners on the Ethernet must therefore recognize the CAP station as a default gateway or as a route gateway to the SAFEDLINK sub-net.

To define the CAP station, proceed as follows:

1. In the tree view of the 'Network' task card, open the 'Global system configuration' > 'Global C-WEB configuration' elements.
2. Highlight the reference of the station required.
3. Click on the 'Network' > 'Convert to CAP' menu item.

⇨ The reference changes to 'Fx72x/CAP'.

Rules for station conversions:

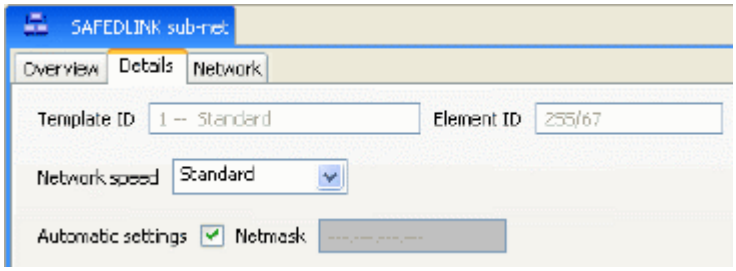
A 'Fx72x/SAFEDLINK host' element can be converted via 'Fx72x/CAP' to an 'Fx72x/Ethernet host' element and vice versa.

'Fx72x/SAFEDLINK host' or 'Fx72x/Ethernet host' can be converted to 'Fx72x/CAP'.

'Fx72x/CAP' can be changed to 'Fx72x/SAFEDLINK host' or 'Fx72x/Ethernet host'.

8.5.2.3 Network speed of the SAFEDLINK

Be default, the Network speed is set for high cable qualities (standard). If using lower cable quality or if using very long cables (and if problems arise), the 'Low' speed must be adjusted.



'SAFEDLINK sub-net' detail editor, details

To set the network speed, proceed as follows:

1. In the tree view of the 'Network' task card, open the 'Global system configuration' > 'Global C-WEB configuration' elements.
2. Highlight 'SAFEDLINK sub-net '.
3. In the detail editor, select 'Details' and in the 'Network speed' list field select the 'Low' setting.

⇨ The network speed is now set for low cable qualities.

8.5.2.4 Manual allocation of addresses in the sub-nets

The IP addresses can be assigned manually.

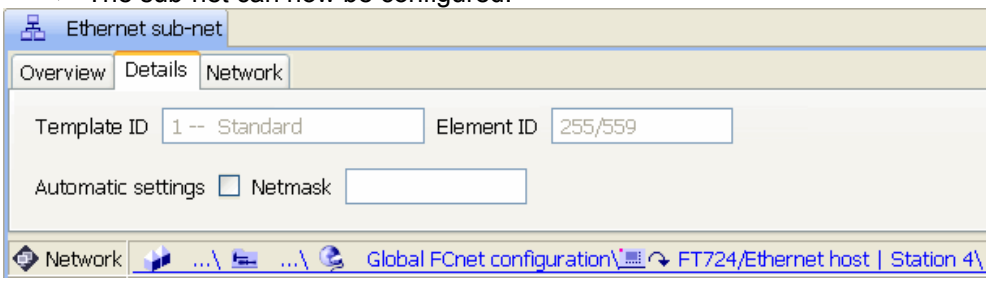
If the Ethernet sub-net is incorporated in an existing IT infrastructure, i.e. in a public network, the settings for the sub-net mask and IP address must be performed manually following the IT administrator's instruction.

The following instructions apply to both networks (taking the example of the Ethernet).

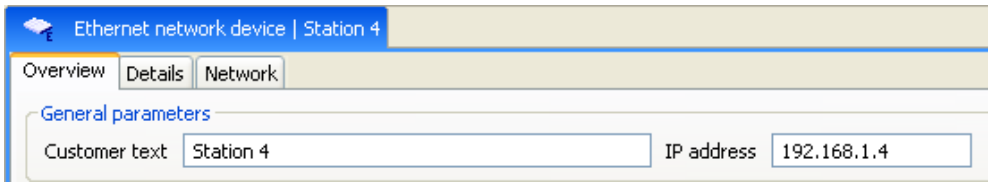
To configure the sub-net, proceed as follows:

1. In the tree view of the 'Network' task card, open the 'Global system configuration' > 'Global C-WEB configuration ' elements.
2. Highlight 'SAFEDLINK sub-net' or 'Ethernet sub-net'.
3. In the detail editor, 'Details', remove the checkmark for 'Automatic settings'.

   ⇨ The sub-net can now be configured.

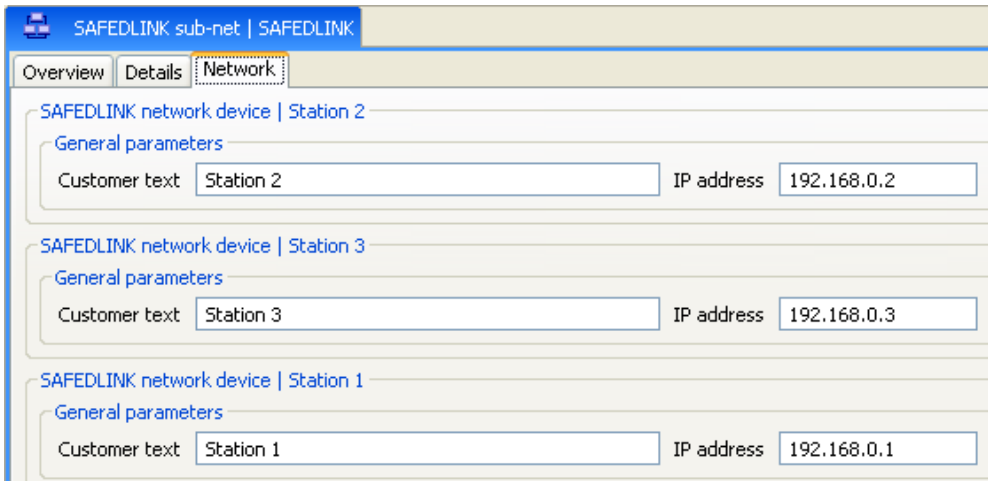


4. Enter the network mask (4 groups of digits, separated by dots) in the 'Netmask' field.
5. Open all 'Host' in the tree view (Fx72x/CAP, Fx72x/SAFEDLINK, Fx72x/Ethernet).
6. Highlight all 'Network device' one after the other (SAFEDLINK, Ethernet).



7. In the detail editor, 'Overview', enter the customer text and the IP address.

   An overview of the IP addresses of all stations can be displayed by sub-net.



In the detail editor, 'Network', with respect to the 'SAFEDLINK sub-net' or 'Ethernet sub-net' elements, the 'Network device' are listed (station 4 in our example can be found under 'Ethernet sub-net').

8.5.2.5 Enabling remote access

Proceed as follows to approve global remote access for Cerberus-Engineering-Tool or Cerberus-Remote:

1. In the tree view of the 'Network' task card, open the 'Global system configuration' element.
2. Highlight 'Global C-WEB configuration'.
3. In the detail editor ('Overview'), select the 'CAP/Ethernet' setting from the 'Remote access' list field.

⇨ Global remote access for Cerberus-Engineering-Tool or Cerberus-Remote is approved.

Activating remote access has an effect on how the CAP station behaves by not starting the DHCP server in the station, and in the 'Connect' window of the Cerberus-Engineering-Tool or Cerberus-Remote, where other selections appear - 'Connection to CAP…' - with different addressing variants.

Special case: standalone station

When setting 'CAP/Ethernet' in the 'Remote access' list field, the 'Global C-WEB configuration' element is marked with an error because there is no network configuration and the standalone station is not defined as CAP.

To define the station as CAP, proceed as follows:

1. In the tree view of the 'Network' task card, open the 'Global system configuration' element.
2. Highlight 'Global C-WEB configuration '.
3. Click on the 'Network' > 'Create CAP configuration' menu item.

⇨ 'Global C-WEB configuration' is linked to the standalone station as CAP.

8.5.2.6 Standard CAP station gateway

The default gateway only has to be set if Cerberus-Remote or Cerberus-Engineering-Tool is to access the FS720 fire detection installation remotely, but is located in a different sub-net to the CAP station itself (i.e. if additional IP routers are being used).

To configure the default gateway in the CAP station, proceed as follows:

1. In the tree view of the 'Network' task card, open the 'Global system configuration' > 'Global C-WEB configuration' elements.
2. Highlight 'Fx72x/CAP'.
3. In the detail editor, 'Overview', enter the IP address for a 'Default gateway'.

8.5.3 Network settings on the PC

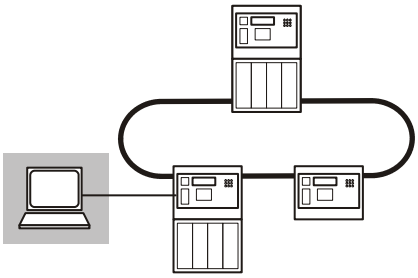
In order to allow Cerberus-Engineering-Tool or Cerberus-Remote to communicate with Stations in the C-WEB (SAFEDLINK and Ethernet), the PC must be set up as a network participant.

The following interfaces can be used on the PC:

- Private network connection (Ethernet)
- External USB/Ethernet adapter (if available)

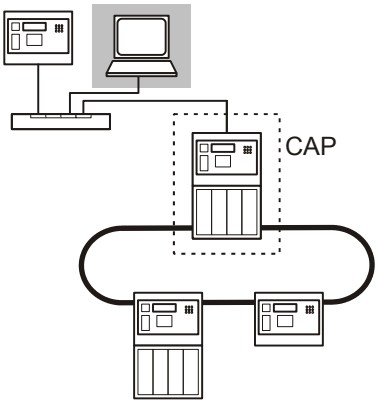
Standard types of access

Local connection to Station



- Tool sub-net: 192.168.200.0
- Route to SAFEDLINK sub-net via Station: 192.168.200.1

Remote access via CAP station



- No tool sub-net
- Route to SAFEDLINK sub-net via CAP station: 192.168.1.1

8.5.3.1 Settings for local connection

As a rule, Cerberus-Engineering-Tool can be connected directly to a standalone station or SAFEDLINK station without any extra settings. A DHCP server, which automatically assigns an IP address to the PC, also runs on the free Ethernet interface of these stations.

A default gateway is also entered so that the other stations in the SAFEDLINK sub-net can also be reached. The entry can however be overwritten by other interfaces, e.g. by the wireless network connection. In order to now see all the networked SAFEDLINK stations, an entry is needed in the PC network interface's route table.

Adding a route to the SAFEDLINK sub-net

The route entry is only needed if using more than one interface in the PC, e.g.:

- Wired Ethernet interface
- Wireless interface
- USB adapter

Users need administrator rights on the PC to add a route.

To add a route, proceed as follows:

1. Click the 'Start' button in the Windows toolbar and select 'Run'.
2. Enter the cmd command in the open 'Run' window and click the 'OK' button.
   ⇨ Cmd.exe is run.
3. Enter the following command:
   route add -p 192.168.0.0 mask 255.255.255.0 192.168.200.1 metric 99
   and press <Enter>.
   Note: The interface must be available, switched on and online (very important with USB adapter in particular), otherwise the following error message appears:
   'C:\Documents and Settings\username\Desktop>route add -p 192.168.0.0 mask 255.255.255.0 192.168.200.1 metric 99
   The route addition failed: Either the interface index is wrong or the gateway does not lie on the same network as the interface. Check the IP Address Table for the machine.'

8.5.3.2

The settings of the PC network interface have to be adapted for remote access via the CAP Station. The IP address for the PC now has to be adjusted manually and the route to the SAFEDLINK sub-net now has to pass via the CAP Station.

Adding another route to the SAFEDLINK sub-net

To add the route to the SAFEDLINK sub-net, proceed as follows:

1. Click 'Start' > 'Run'.
2. Enter the 'cmd' command in the open 'Run' window and click the 'OK' button.
   ⇨ Cmd.exe is run.
3. Enter the following command:
   route add -p 192.168.0.0 mask 255.255.255.0 **192.168.1.1** *metric 99*
   and press the Enter key.

The process of changing the route entries in the PC is not always a smooth one. We have found that Cerberus-Engineering-Tool has to be restarted after this process so that the new settings actually take effect. If quickly moving the connection from one Station to another, you may also have to explicitly close the old Cerberus-Engineering-Tool connection using 'Disconnect'; otherwise the 'Connect' dialog will not appear.

Presetting of the PC if user does not have administrator rights

If the person using Cerberus-Engineering-Tool does not have administrator rights on his or her PC, he or she should ask an IT administrator to perform the setting. Using the routes mentioned, all SAFEDLINK Stations can be seen in the standard configurations anyway, firstly using a local connection and secondly via the CAP Station, which can also be connected using an alternative setting for the PC's IP address.

The following limitations apply:

- Standard configurations for private networks only
- The SAFEDLINK sub-net is always 192.168.0.0 (can also be set manually)
- The Ethernet sub-net is always 192.168.1.0 (can also be set manually)
- The CAP Station must always be number 1 due to its address as a gateway
- Routes can only be entered if the corresponding connection to the network is established, e.g. on a test system in the office. They are then retained until deleted again by a command.

Setting IP addresses for the PC

These settings are suited for the above-mentioned presetting. When an 'Alternative Configuration' is defined, the PC will spend one minute searching for a DHCP server and only then will it switch to the alternative address.

A user with administrator rights for his or her PC can of course define an IP address directly in the 'General' view.

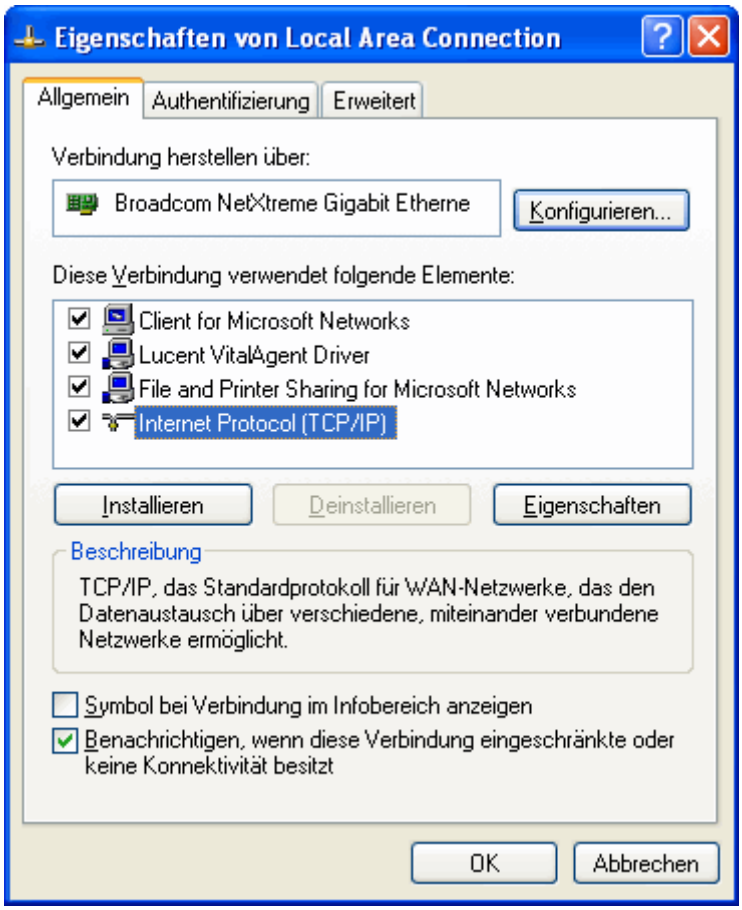
To set the network settings, proceed as follows:

1. Click the 'Start' button in the Windows toolbar and select 'Settings' > 'Network connections' > 'Local Area Connection'.

   ⇨ The 'Status of Local Area Connection' window opens.

2. Click the 'Properties' button in the 'General' view.

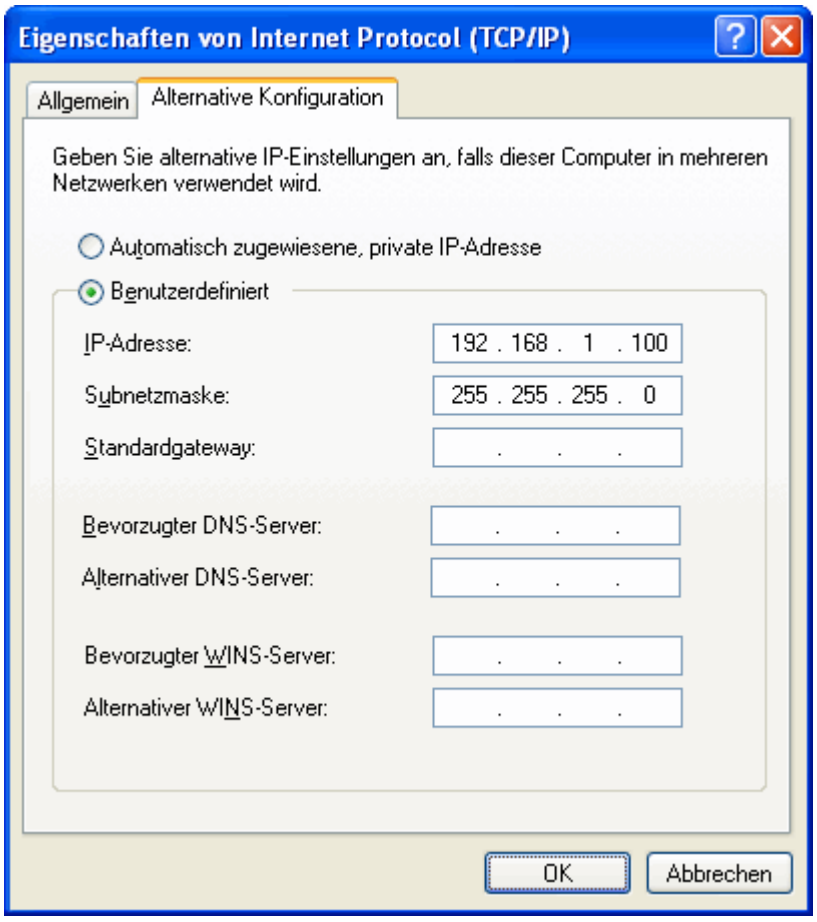
   ⇨ The 'Properties of Local Area Connection' window opens.



3. Highlight the 'Internet Protocol (TCP/IP)' connection in the 'General' view and click the 'Properties' button.

   ⇨ The 'Properties of Internet Protocol (TCP/IP)' window opens.

4. Leave the 'Obtain IP address automatically' option selected and click the 'Alternative configuration' button.



5. Select the 'User-defined' option, enter values for 'IP address' and 'Sub-net-mask' and click the 'OK' button.

⇨ The network settings for remote access are complete.

8.5.3.3 Diagnosis for IP settings on the PC

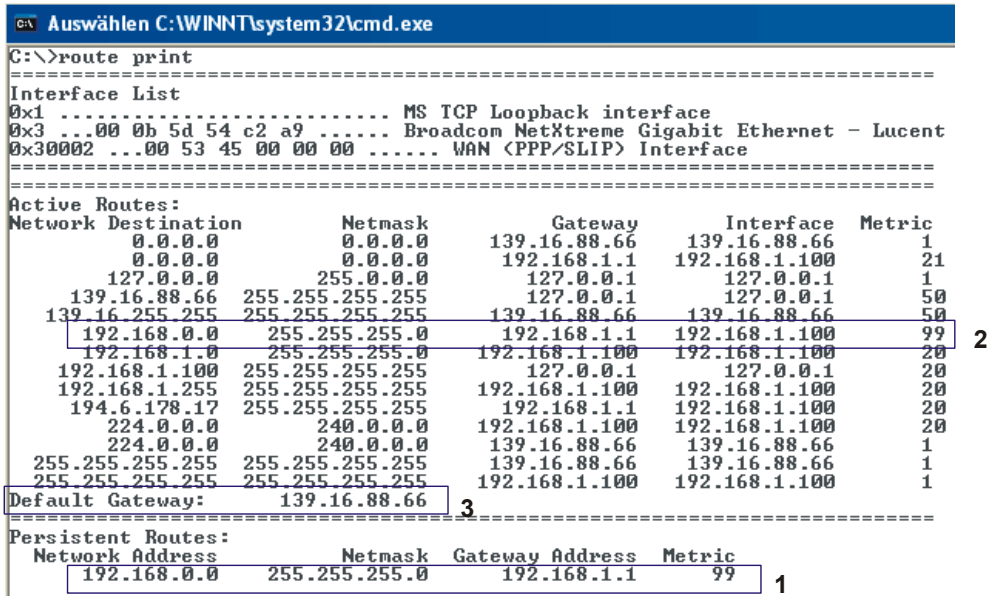
Routes in PC

The routes used by the PC can be displayed. This allows the user to see whether the gateway entries or routes required are effective.

To display the routes on the PC, proceed as follows:

1. Click the 'Start' button in the Windows toolbar and select 'Run'.
2. Enter the cmd command in the open 'Run' window and click the 'OK' button.

   ⇨ Cmd.exe is run.
3. Enter the following command:
   route print
   and press <Enter>.



Routes in PC

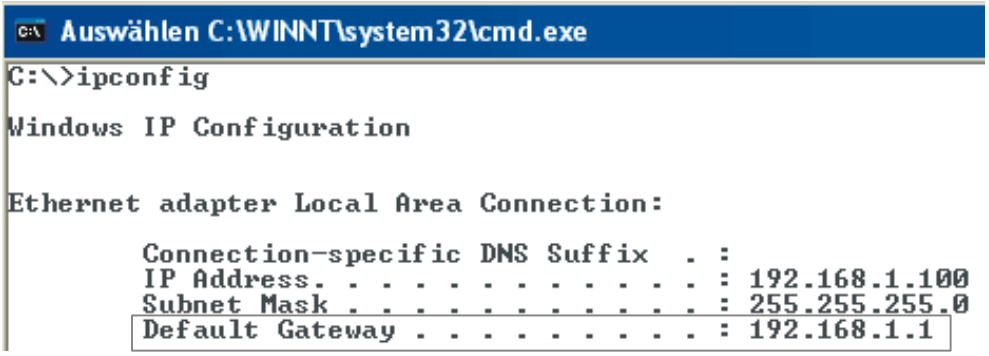
The defined routes are entered as 'Persistent Routes' (1) and the route used can be seen under 'Active Routes' (2). The current default gateway entry is also listed (3).

IP configuration in the PC

The actively available Ethernet interfaces on the PC can be displayed. This allows interfering default gateway entries to be seen for example.

To define the IP configuration, proceed as follows:

1. Click the 'Start' button in the Windows toolbar and select 'Run'.
2. Enter the cmd command in the open 'Run' window and click the 'OK' button.
   ⇨ Cmd.exe is run.
3. Enter the following command:
   ipconfig
   and press <Enter>.



IP configuration in the PC

8.5.4 Establishing connection between PC and C-WEB

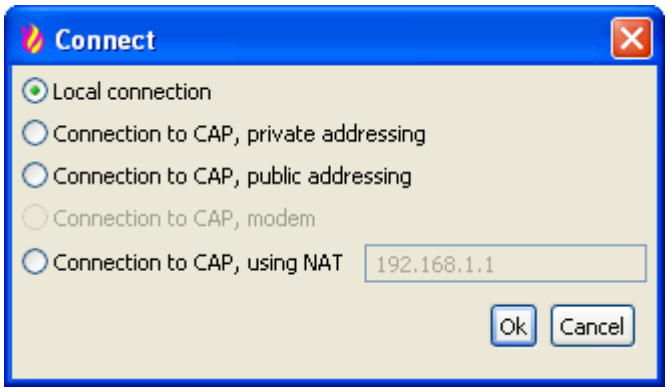
The connection can be established using the following menu items:

- For the Cerberus-Engineering-Tool
  - 'Commissioning' > 'Download site configuration'
  - 'Commissioning' > 'Upload site configuration'
  - 'Commissioning' > 'Upload site event memory'
  - 'Commissioning' > 'Upload site log files'
- For the Cerberus-Remote
  - 'Cerberus-Remote ' > 'Connect'

The 'Connect' window opens when executing a command.

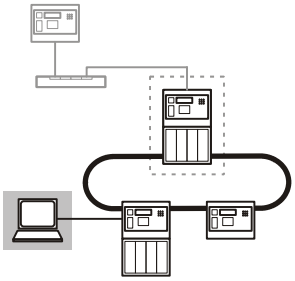
The types of connection available for selection changes when:

- using a CAP station
- also using Ethernet stations
- enabling for remote access
- changing over to manual issuing of addresses



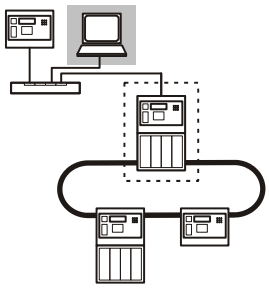
'Connect' window for selecting the connection

- 'Local connection'
  (no remote access)



The PC is connected to the station directly (standard). An automatic IP address is used.

- 'Connection to CAP, private addressing'
  (no remote access)
- 'Connection to CAP, public addressing'
  (remote access enabled)
- 'Connection to CAP, using NAT'
  (remote access enabled)



The PC is connected to the CAP station. Local IP addresses are used and produced automatically.

The PC is connected to the CAP station. External IP addresses are used and must be configured.

The Cerberus-Engineering-Tool is connected to the CAP station. The user must set the IP address (e.g. 139.16.90.1).

!	*NOTICE*
	It is essential that the DHCP server of an FS720 station never runs in a public network. A direct connection must never therefore be made between a SAFEDLINK station or a CAP station without remote access and the external network. An incorrect DHCP server of this kind will cause the public network (e.g. Intranet) to crash very quickly!

8.5.5 Connecting management stations using BACnet/Ethernet

Management stations or other sub-systems are connected to FS720 using BACnet/Ethernet. Since FS720 makes its data available to other partners via BACnet in its role as a server, these are usually known as BACnet clients.

BACnet is a communication protocol used in building automation. BACnet acts as an inter-network and requires its own logical IDs (BACnet device ID) for the stations, so that each station is uniquely recognized as a BACnet participant. There are two parts to the BACnet device ID: a 'Device' object type and an instance number.

The entry for a BACnet device ID in the Cerberus-Engineering-Tool is always made as a decimal figure for the instance number; the object type is added internally. Device IDs must be configured at the following points:

- BACnet client configuration, BACnet device ID (consultation with partner required)
- BACnet device object, address (= BACnet device ID, is unique within FS720)

The logical device IDs must be unique in the complete inter-network. Managing the IDs is a challenge for engineering, because both the FS720 sub-system and the management stations (which may integrate other sub-systems in addition to FS720, e.g. HVP systems) have Cerberus-Engineering-Tool.

A few points to clarify things:

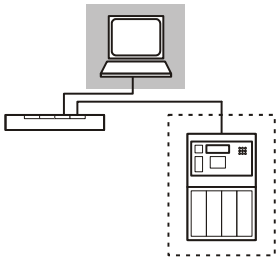
- A BACnet client is connected to the FS720 sub-system via the Ethernet interface of the Central Access Point (CAP), usually via hub/switch.
- Every single station that is to use the BACnet protocol must be enabled with a license key (L2).
- When the BACnet protocol is used, BACnet communication first has to be enabled and then other globally used information configured. These actions must be agreed with a management station integrator.
- The preset values (defaults) are suitable for most cases and should only be changed if really necessary. This includes e.g. the UDP port number.
- The BACnet clients have to be defined and configured because in a security system access to the system has to be limited to authorized clients.

Cerberus-Engineering-Tool can change the FS720 configuration to SiB-X export format so that a BACnet client can import this data. The automatic IP addresses are missing from the SiB-X export file because they are first produced in the stations. During the import process, a note may appear indicating that the content may not be consistent; any conflicts are then displayed in the Cerberus-Engineering-Tool (warning to prevent duplicate addresses being allocated). These can be corrected manually if the IP addresses are to be used in the SiB-X export file.

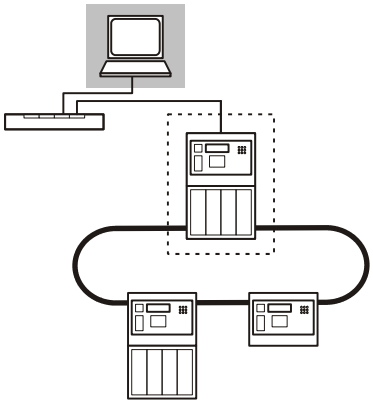
8.5.5.1 Configuration options for BACnet

The management station is shown as a PC marked in gray. Cerberus-Engineering-Tool may also be connected in parallel to this.

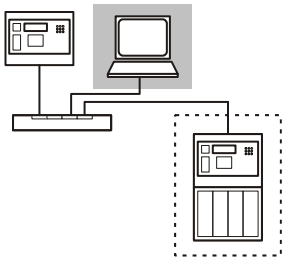
Standalone CAP station



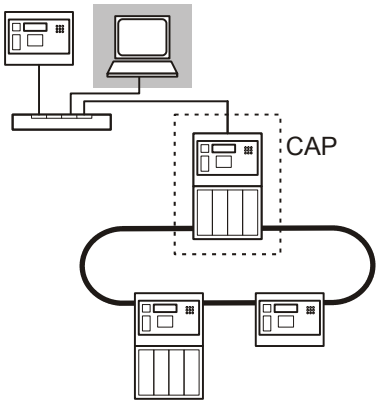
CAP station with SAFEDLINK



CAP station with Ethernet



CAP station with Ethernet and SAFEDLINK



The PC or Unix station needs a permanently assigned IP address and a gateway entry or the route entry to the SAFEDLINK sub-net via the CAP station.

Recommendations for BACnet configuration

This recommendation is a summary of the points that should be noted for BACnet integration when configuring the network and providing access for Cerberus-Engineering-Tool.

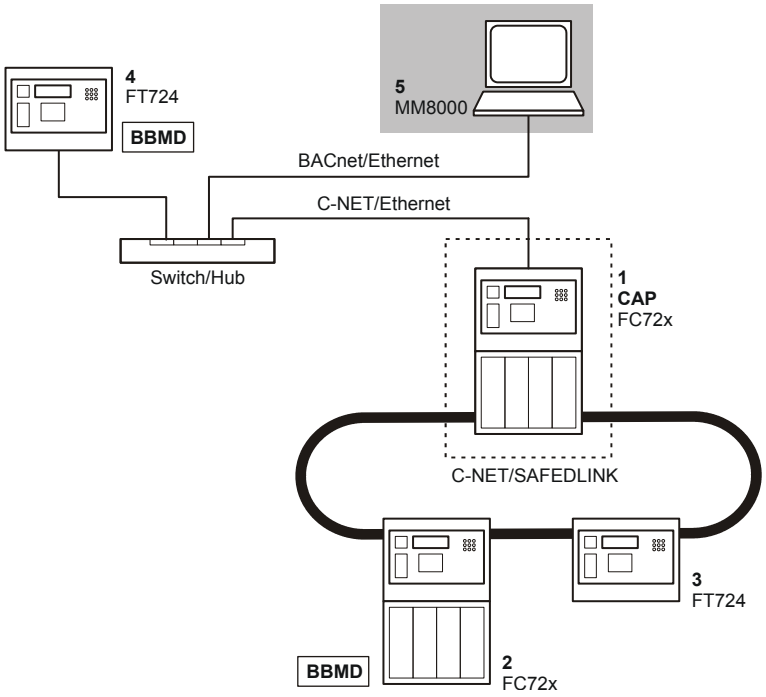
- Always activate remote access to be sure that there are no DHCP servers running on the CAP station.
- Select manual allocation of addresses so that these are included in the SiB-X export format. The predefined local addresses can be used.

- Only select external addresses for Ethernet; SAFEDLINK remains the local sub-net.
- The CAP station should be number 1 if there are no administration rights on the PC.

8.5.5.2 Planning BACnet configuration

Configuration complexity increases when using BACnet. We would therefore seriously recommend first producing a small overview plan.

- Enter the necessary IP addresses of the BACnet devices and CAP
- Each BACnet device needs a unique BACnet device ID.
- Each sub-net needs a BBMD (for explanation, see below) and an entry there for the other BBMDs and their IP addresses
- Each FS720 station must recognize the BACnet clients with their device IDs



BACnet

	Device	Device ID	IP address SAFEDLINK	IP address Ethernet	Gateway	Network mask
1	Station 1 (CAP-Station)	1	192.168.0.1	192.168.1.1		
2	Station 2 (BBMD)	2	192.168.0.2	-		
3	Station 3	3	192.168.0.3	-		
4	Station 4 (BBMD)	4	-	192.168.1.4		
5	BACnet client	444	-	192.168.1.50	192.168.1.1	255.255.255.0

Example of overview plan

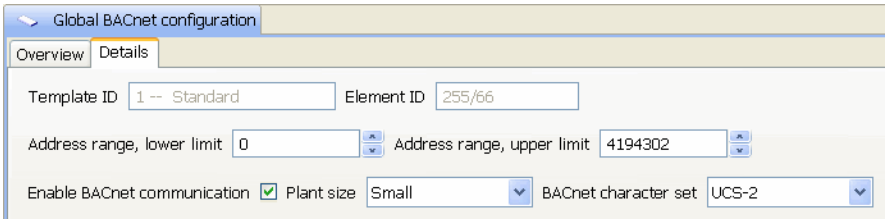
8.5.6 Global BACnet configuration

8.5.6.1 Enabling BACnet communication

BACnet communication must be enabled for the BACnet to be configured. To do so, proceed as follows:

1. In the tree view of the 'Network' task card, open the 'Global system configuration' element.
2. Highlight 'Global BACnet configuration '.
3. In the detail editor ('Details') remove the checkmark from the box for 'Enable BACnet communication'.

   ⇨ BACnet communication is enabled and additional fields can be configured.



'Global BACnet configuration' detail editor, 'Details'

8.5.6.2 Global BACnet settings

The values to be entered in the detail editor must be agreed with the management station integrator:

- ’Address range, lower limit'/’Address range, upper limit ':

  Range for device ID values for identifying the FS720 stations in BACnet. The address range is only used for organizational purposes and is exported in SiB-X format.

- 'Plant size' (used for optimization purposes):
  - Compact: up to 5 stations
  - Medium: up to 10 stations
  - Large: more than 10 stations

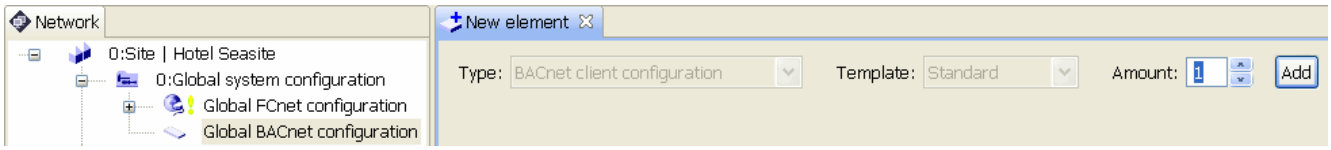
- ’BACnet character set':

  character set to be used in the BACnet protocol for text strings. FS720 functions internally with Unicode in UTF-8 format.
  Selectable character sets:
  - UCS-2 (Unicode 2 bytes)
  - ANSI (X3.4 = ASCII 7 bits)
  - ISO Latin 1 (8 bits)

- Substitute character: this character replaces other characters in text strings that are not featured in the selected BACnet character set (default always '?', another configuration has no impact).

8.5.6.3 Configuring BACnet clients

To allow the BACnet client to be configured, in the tree view of the task card 'Network', the element 'BACnet client configuration' is created. This element defines the management stations or third-party devices that are accepted by the FS720 system. This element and its customer text is also used internally in the history in order to log all actions initiated by a management station. A BACnet client is identified by the BACnet device ID.

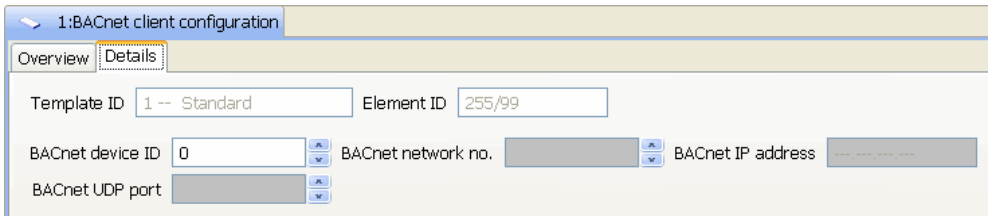


Window 'New element' for creating the element 'BACnet client configuration'

To create the 'BACnet client configuration' element, proceed as follows:

1. In the tree view of the 'Network' task card, open the 'Global system configuration' element and highlight 'Global BACnet configuration'.
2. Open the 'New element' window.
3. Create the 'BACnet client configuration' element for each BACnet client.
4. Enter the customer text.

Properties of the 'BACnet client configuration' element

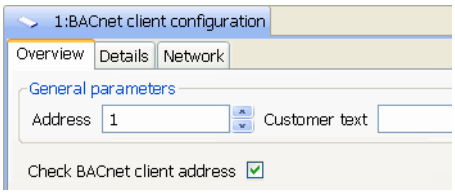


'BACnet client configuration' detail editor, details

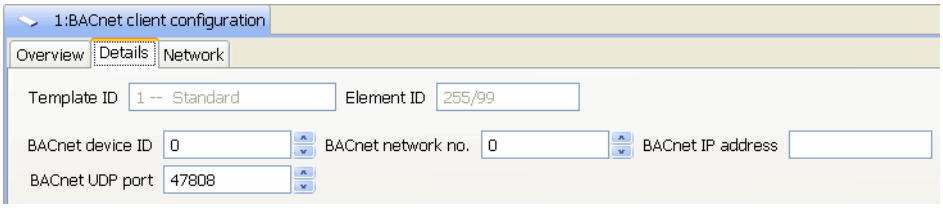
In the 'BACnet client configuration' detail editor ('Details') the BACnet device ID that has been assigned to the client must be entered. This step must be agreed with the management station integrator. The other fields relating to BACnet can only be used if the BACnet client has a fixed IP address, i.e. if a DHCP server is not being used.

If, in addition to BACnet device ID, 'BACnet network no.', 'BACnet IP address' and 'BACnet UDP port' are also being used to identify the BACnet client, these properties can be modified by agreement with the management station integrator.

- To do this, in the detail editor 'BACnet client configuration' ('Overview'), remove the check mark from the box for 'Check BACnet client address'.
  - The fields are activated.



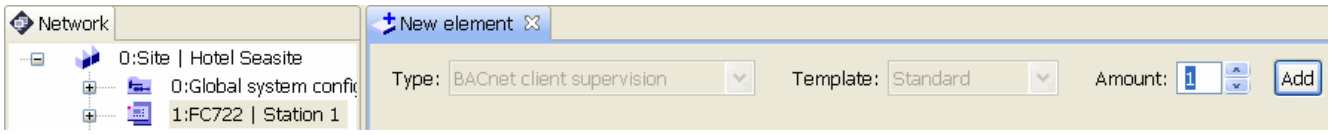
'BACnet client configuration' detail editor, overview



'BACnet client configuration' detail editor, details

8.5.6.4 Monitoring the BACnet client

Stations can monitor the connection to the BACnet client. For this purpose each station is assigned the element 'BACnet client supervision'. This element triggers a fault message if the connection to the BACnet client is interrupted.

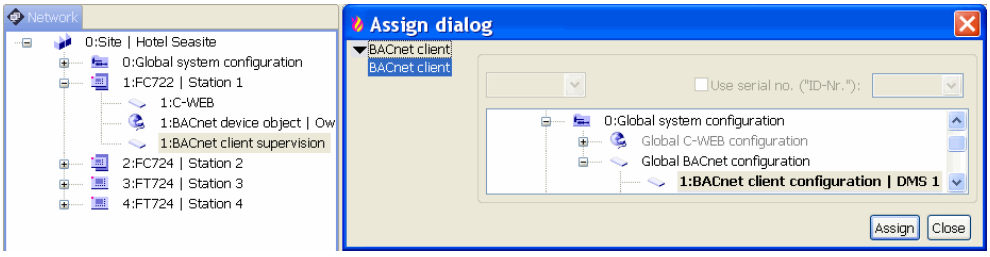


Window 'New element' for creating the element 'BACnet client supervision'

To create the 'BACnet client supervision' element, proceed as follows:

1. In the tree view of the 'Network' task card, highlight a 'Station'.
2. Open the 'New element' window.
3. Create the 'BACnet client supervision' element for each BACnet client you want to monitor.

The 'BACnet client supervision' elements must then be linked to the corresponding 'BACnet client configuration' elements.

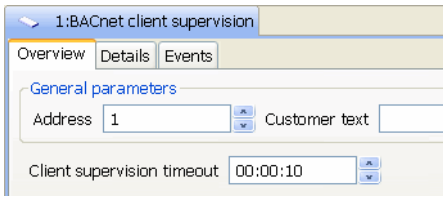


Window 'Assign dialog' for linking the element 'BACnet client supervision'

1. Highlight the 'BACnet client supervision' element in the tree view.
2. Open the 'Assign dialog' window.

   ⇨ The 'BACnet client configuration' elements are highlighted in the list.
3. Select the corresponding element and click on the 'Assign' button.

Properties of the 'BACnet client supervision' element



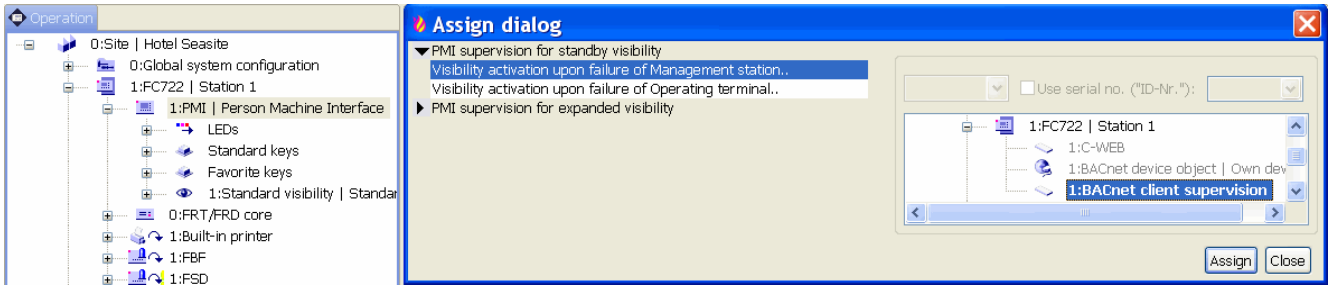
'BACnet client supervision' detail editor, 'Overview'

In the detail editor 'BACnet client supervision' ('Overview'), the time after which a fault message is displayed is defined in 'Client supervision timeout'.

The time period must agree with the BACnet client's query cycle, with which the BACnet client regularly queries the station's system status. Consult the management station integrator to find out the interval between queries. The value to be set in the 'Client supervision timeout' field corresponds to at least 1.1x the value of the query cycle.

Standby visibility for Management station

The standby visibility mode can be assigned to a Person Machine Interface for the management station. This visibility is automatically selected if the assigned management station fails.



Window 'Assign dialog' for creating and linking standby visibility

To create and link standby visibility, proceed as follows:

1. Select the 'Operation' task card.
2. Highlight 'PMI' in the tree view.
3. Open the 'Assign dialog' window.
4. In the 'PMI supervision for standby visibility' list, select the element 'Visibility activation upon failure of Management station..'.

   ⇨ The 'BACnet client supervision' element is highlighted.
5. Click on the 'Assign' button.

   ⇨ The 'Standby visibility for Management station' element is created.
6. Highlight it. In the 'Visibility' list in the 'Assign dialog' window, select the appropriate visibility and click on the 'Assign' button.

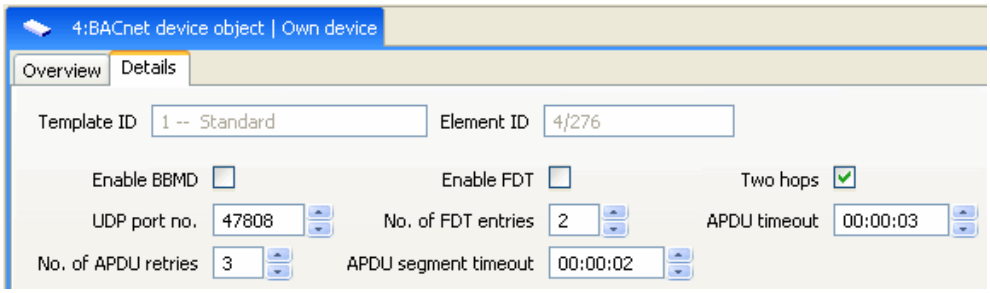
8.5.7 FS720 BACnet device configuration

8.5.7.1 BACnet device object

In the tree view of the 'Network' task card, each station contains a 'BACnet device object' element. It is used to identify the station in the BACnet inter-network.

- In the detail editor ('Overview'), the 'BACnet device object' element contains an address and predefined customer text ('Own device'). The address is used directly as a 'BACnet device ID' and should, therefore, fall within the address range that has been specified in the global settings for BACnet.
- Under 'Details' in the detail editor, you will find the configuration of the BACnet stack, including the BBMD function and the properties of the device object for BACnet transaction control.

The general description of the configurable fields is followed by a description of the basics for making decisions relating to setting values.



'BACnet device object' detail editor, 'Details'

BACnet transaction control

The properties of the device object for BACnet transaction control are set following agreement with the management station integrator. They must be set in all stations and should be consistent for the entire installation. The following properties can be adapted:

- 'APDU timeout'

  Defines the timeout for the BACnet transaction control. The value can be increased if large numbers of pending events are to be expected or if complex BACnet client polling is performed. One indication of this is an increase in aborted transactions as a result of the time being exceeded. The maximum value is however set to 10 seconds so that the time for an initial alarm is not jeopardized by a repetition should a collision occur.

- 'APDU segment timeout'

  Defines the timeout that is used to request another part of a segmented BACnet message (SBT BACnet stack internal).

- 'No. of APDU retries'

  Defines the maximum number of repetitions for a BACnet transaction. Fewer repetitions increase the risk of messages not being transmitted due to collisions or other problems whereas a larger number has a negative impact if a partner can no longer be reached.

Configuration of the BACnet communications stack, including BBMD function

As a rule there is just one value that has to be defined on all stations:

- 'UDP port no.'

  Defines the number of the UDP port used for BACnet communication. The default 47808 (0xbac0) corresponds to the standard. All participants, including the BACnet clients, must use the same number.

The BBMD configuration in contrast needs only be made for one station per IP sub-net. If using stations on the Ethernet this must be agreed with the BACnet clients if they are in the same IP sub-net.

If using stations on the SAFEDLINK, it would be beneficial if it were the CAP, but in MP1.3 it MUST be a different station, i.e. a SAFEDLINK station.

Configuration includes:

- 'Enable BBMD'

  Enables the BBMD (BACnet Broadcast Management Device) functionality. This is a BACnet function for the exchange of broadcast messages between different IP sub-nets. If BBMD is enabled, then there is a 'BDT entry' and/or 'Enable FDT' is set to active.

- 'Two hops'

  Selects either 'unicast' as the standard procedure for a partner BBMD (actively set) or 'direct broadcast' if the IP routers are configured such that they pass on broadcasts for other sub-nets (inactively set). The CAP for example cannot do this.

- 'Enable FDT'

  Enables remote BACnet devices to register in the 'Foreign Device Table' (FDT) of the BBMD. This is required if there is no separate BBMD in their sub-nets.

- 'No. of FDT entries'

  Defines the maximum number of FDT entries ('Foreign Device Table').

BBMD is a BACnet function that is required exactly once for each sub-net. One device assumes this function and must recognize its partners in the other sub-nets (BDT entries). Exception: One single device in a sub-net without this BBMD function can also register as a third-party device with a BBMD in another sub-net (dynamic FDT entry).

Searching for a SAFEDLINK station

To search for a station that is not the CAP, proceed as follows:

1. In the tree view of the 'Network' task card, open the 'Global system configuration' > 'Global FCnet configuration' elements.
2. Highlight an 'Fx72x'/'SAFEDLINK host' and search for the relevant station via the 'Network' hyperlink in the detail editor. This can also be done using the customer text provided that this is set uniquely.

   ⇨ The SAFEDLINK station is highlighted.

3. Open the SAFEDLINK station.

Configuring a SAFEDLINK station as BBMD

To configure the station as BBMD, proceed as follows:

1. Highlight 'BACnet device object '.
2. Select 'Details' in the detail editor.
3. Check the box for 'Enable BBMD' to enable the BACnet function.
4. Only check the box for 'Enable FDT' if a BACnet client has to register in this BBMD (following agreement).
5. Leave 'Two hops' selected. Together with the default in the 'Broadcast distribution mask' for 'BDT entries', this configuration always functions without problems.
6. The number in 'No. of FDT entries' corresponds to the maximum supported by FS720.

Configuring all stations

- The value for 'APDU timeout' should be agreed with the management station integrator. We would recommend 10 seconds with MM8000.
- The value for 'APDU segment timeout' should also be agreed. We would recommend 5 seconds.
- The value for 'No. of APDU retries' corresponds to the BACnet standard and does not need to be changed.
- The 'UDP port no.' setting corresponds to the standard (47808 = 0xbac0). It only needs changing if the entire system expects it to.

8.5.7.2 Partner BBMD entry (BDT entry)

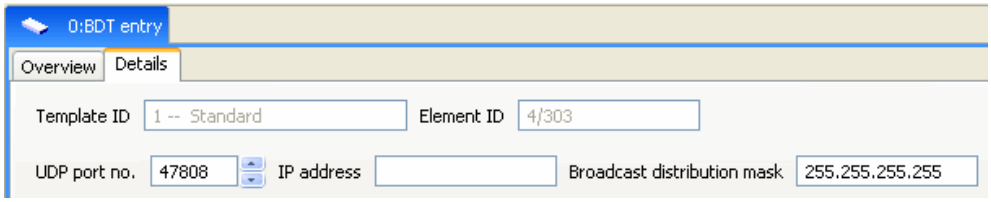
'BDT entry' elements can be added to the 'BACnet device object' element when the BBMD function is activated. This element defines the management station or the third-party device acting as BBMD in its sub-net. A 'BDT entry' element is required for each sub-net with its own BBMD.

'BDT entry': Creating

To create 'BDT entry', proceed as follows:

1. Highlight 'BACnet device object '.
2. Open the 'New element' window.
3. Create the 'BDT entry' element for each BBMD.

'BDT entry': Configuring



'BDT entry' detail editor, 'Details'

To configure 'BDT entry', proceed as follows:

1. Highlight 'BDT entry '.
2. Select 'Details' in the detail editor.
3. Set the agreed IP address for the BACnet client.
4. Leave the predefined values for 'UDP port no.' and 'Broadcast distribution mask' unchanged. The port number of the client must match its own, and the mask value matches the pre-setting for 'Two hops'.

8.5.7.3 BACnet Notification Class Element

All stations contain a list of 20 pre-defined entries under 'BACnet Notification Class element' in the detail editor. Each entry stands for a BACnet notification class and has one unique address and one customer text within a station. The addresses are used in the BACnet object ID as instance numbers. The customer text provides information on which elements of the application are represented by this notification class. The internal assignment cannot be changed. The settings should only be changed according to a management station integrator's specification, and only when the behavior of different sub-systems has to be adapted to a superordinate system.

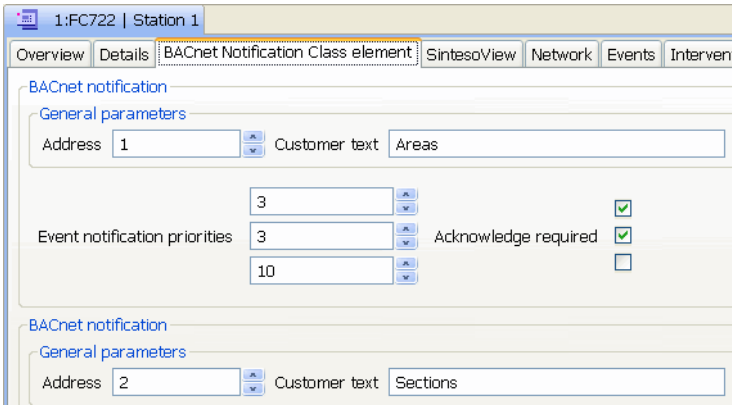
Address	Customer text	Address	Customer text
1	Areas	11	Lines
2	Sections	12	Devices
3	Zones	13	Channels (phys.)
4	Sensors	14	System
5	Control groups	15	UGA
6	Controls	16	AVC
7	Causes/Effects	17	IC
8	Channels (log.)	18	-
9	Stations	19	-
10	Module/Submodules	20	-

Notification classes

Later on users define per notification class the priority of an event message per status change and which of these changes can be acknowledged at a management station.

The following status changes are defined (in this sequence):

- 'to-offnormal': Entry of an event
- 'to-fault': Entry of a fault
- 'to-normal': normal operation re-established



'Fx72x' detail editor, 'BACnet Notification Class element'

To configure 'BACnet Notification Class element', proceed as follows:

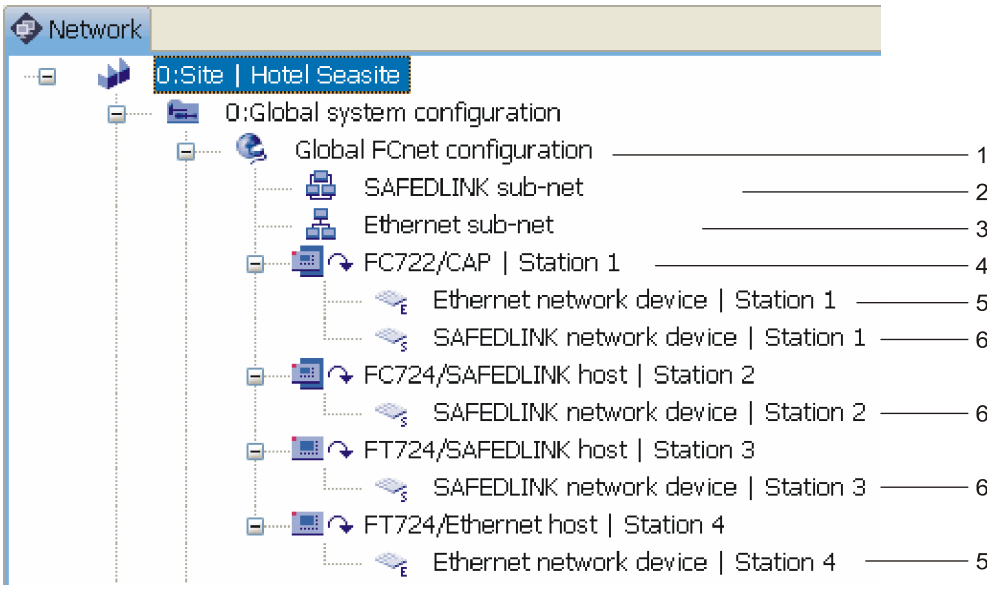
1. In the 'Network' task card, highlight all the 'Fx72x' stations one after the other.
2. Select 'BACnet Notification Class element' in the detail editor.
3. Set the priorities for each event notification.
4. Check the box for 'Acknowledge required' wherever acknowledgement is required for status changes.

The following should be noted for the FS720 fire detection system:

- Internally the FS720 fire detection system only processes the acknowledgements for the 'to-offnormal' and 'to-fault' status changes. The 'to-normal' status change can also be supported with acknowledgement for BACnet clients.
- The priorities for the event messages should be selected from the 0 to 63 range that is intended for 'LifeSafety' applications. The highest priority starts at 0 and the lowest ends at 255.
- There are no predefined entries for the recipients of event messages; these must be entered by the BACnet clients at runtime.

8.5.8 Checklist for network configuration and BACnet

The overview described in this chapter shows the settings that are generally to be adapted or checked for BACnet integration. The overview can be used as a checklist. The first part covers the network settings and the second part the BACnet settings.

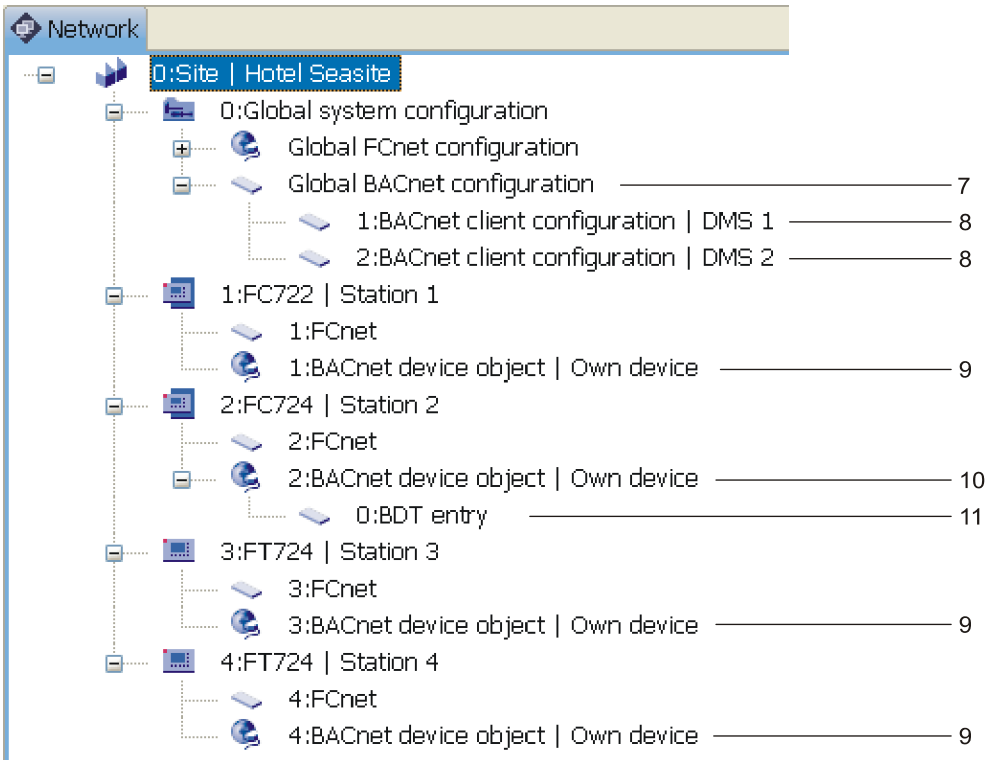


Checklist for network configuration

No.	Setting options	Values	Range, [IP example]
1	'Remote access'	**CAP/Ethernet**	None, CAP/Ethernet
2	'Automatic settings' SAFEDLINK sub-net 'Netmask' 'Network speed'	**inactive** **set** Standard	active, inactive [255.255.255.0] standard, slow
3	'Automatic settings' Ethernet sub-net 'Netmask'	**inactive** **set**	active, inactive [255.255.255.0]
4	'Default gateway' for CAP station	**set**	[192.168.1.234]
5	'IP address' for Ethernet interface	**set**	[192.168.1.xxx]
6	'IP address' for SAFEDLINK interface	**set**	[192.168.0.xxx]

Values shown in bold deviate from the default or should be defined.

Here, 'Automatic settings' are set to inactive because only values entered manually are exported in SiB-X export format.



Checklist for BACnet configuration

No.	Setting options	Values	Range, [IP example]
7	'Enable BACnet communication' 'Plant size' 'BACnet character set' 'Address range, lower limit' 'Address range, upper limit'	**active** small UCS-2 0 4194302	active, inactive small, medium, large UCS-2, ISO-Latin 1, ANSI 0 … 4194302 0 … 4194302
7	'BACnet client configuration': Creating	-	maximum 2 clients

No.	Setting options	Values	Range, [IP example]
8	'BACnet device ID' 'BACnet network no.' 'BACnet UDP port' 'BACnet IP address'	**set** 0 47808 -	0 … 4194302 = local network 1024 … 65535 [empty]
9	'UDP port no.' on every station 'APDU timeout' 'No. of APDU retries' 'APDU segment timeout'	47808 **00:00:10** 2 **00:00:05**	1024 … 65535 3 … 20 s 3 … 6 2 … 10 s
10	'Enable BBMD' on one station 'Enable FDT' 'Two hops' 'No. of FDT entries'	**active** inactive active 2	active, inactive active, inactive active, inactive 2 … 8
(9)	'UDP port no.' 'APDU timeout' 'No. of APDU retries' 'APDU segment timeout'	47808 **00:00:10** 3 **00:00:05**	1024 … 65535 3 … 20 s 3 … 6 2 … 10 s
11	'IP address' for partner BBMD UDP port no.' 'Broadcast distribution mask'	**set** 47808 default	[192.168.1.234] 1024 … 65535 255.255.255.255

Values shown in bold deviate from the default or should be defined.

Checklist in the event of problems with integration

Cause	What must be done
Communication fault between a BACnet client and the C-WEB station(s); e.g. displayed on MM8000	Check the following points: License key L2 is available in all stations BACnet communication is enabled in all stations BACnet clients (device ID) are correctly configured IP addresses are set correctly in all stations and on the PC Routes are set correctly on the PC
Communication fault between Cerberus-Engineering-Tool and the station(s)	Check the following points: Station is enabled IP addresses are set correctly in the station and on the PC Routes are set correctly on the PC Special case: once the station has been changed to CAP, its address and route changes
A large number of transactions are aborted (analysis with network analyzer, e.g. Wireshark: 'Abort' – 'timeout' message)	APDU timeout set too low (min 6s) on stations and management station

Reading the license on a station's Person Machine Interface:

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 appears. The main menu then appears on the display with the function numbers in brackets.
3. Select the 'Topology' > 'Hardware tree' menu items.
4. Select the 'Station' > 'Communication interfaces' > 'Licence key' elements
5. Press the 'More options' softkey.
6. Select the 'Show details' menu item.
7. Scroll through the list until 'Property (33) License-Type' is reached

⇨ 'value' = 'S-Class' corresponds to L2 or 'C-Class' corresponds to L1 otherwise 'UNDEFINED' for no license (RealTimeClock, e.g., for time master)

9 Index

Issued by
Siemens Switzerland Ltd
Industry Sector
Building Technologies Division
International Headquarters
Gubelstrasse 22
CH-6301 Zug
Tel. +41 41-724 24 24
Fax +41 41-724 35 22

www.siemens.com/buildingtechnologies