Honeywell

User Manual

WINFEM Advanced for DS 6700 / DS 6750
Item No. 013498

ℹ	P03178-20-0G0-06 2018-05-07	SWFAV.00.0V19.07 (WINFEM Advanced) ADS66.01.0V08.xx (DS 6700 / DS 6750)	Subject to change without notice

Contents

Abbreviation list

1TR140: Protocol used to send an SMS by landline.

Analog/PPP *or* (PSTN)PPP: Network protocol to establish connections via dial-up lines.

APN: Access Point Name, access point to the GPRS data network in cellular technology.

DHCP: Dynamic Host Configuration Protocol, allows the assignment of the network configuration of the transmission device by a server.

DNS: Domain Name System, an important network service. The main task is responding to queries regarding name display in the corresponding IP address.

NTP: Network Time Protocol, a standard for synchronizing clocks in computer systems.

POP3: Transmission protocol via which emails can be accessed from an email server.

PSTN: Public Switched Telephone Network, designation for the public wired telephone network.

SMSC: Short Message Service Center is a component of the cellular network. It enables messages from the SMS service to be saved, forwarded, converted and delivered.

SMTP: Simple Mail Transfer Protocol, protocol for exchanging and forwarding emails in networks.

TAP: Protocol for sending an SMS via the telephone network with special data format (8 data bits, no parity, 1 stop bit).

TAP 7n1: Protocol for sending an SMS via the telephone network with special data format (7 data bits, no parity, 1 stop bit).

UCP: Data protocol which can be used to exchange short messages between SMSC and other network participants.

UTC: Abbreviation for valid Universal Time.

Source: wikipedia.com

Introduction

The information in this manual may be changed at any time without notice and should not be considered as a guarantee on the part of Novar GmbH. Novar GmbH shall not be liable for any possible errors or inaccuracies that might be contained in this manual.

We would like to point out that, despite extensive test series, we cannot guarantee that this software will work without any problems, considering the numerous PC/hardware manufacturers and the resulting variety of hardware configurations.

WINFEM and *FEMAG* are trademarks of *Novar GmbH*.
Windows 98, Windows Me, Windows NT, Windows 2000, Windows XP and *Microsoft* are registered trademarks of *Microsoft Corporation.*
All other products referred to are trademarks of their owners.

Symbols used

You will find the following symbols in this manual, which are used to draw your attention to sections of particular importance:

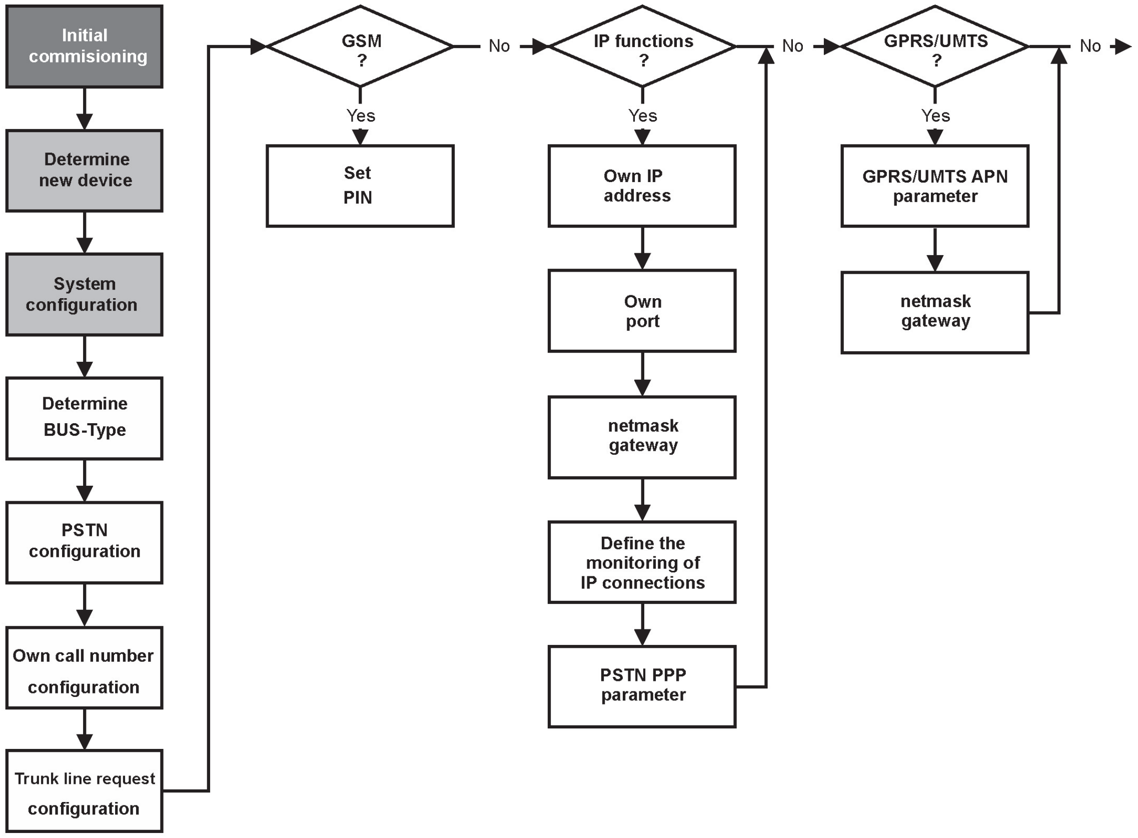
ℹ **Indicates important information on a topic, a procedure or other important information.**

VdS **Notes concerning programming/installation in accordance with VdS guidelines.**

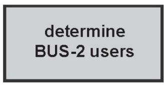
BSI **Programming/installation instructions in accordance with BSI technical guidelines.**

EN **Information on European standards.**

Process outline



Legend:

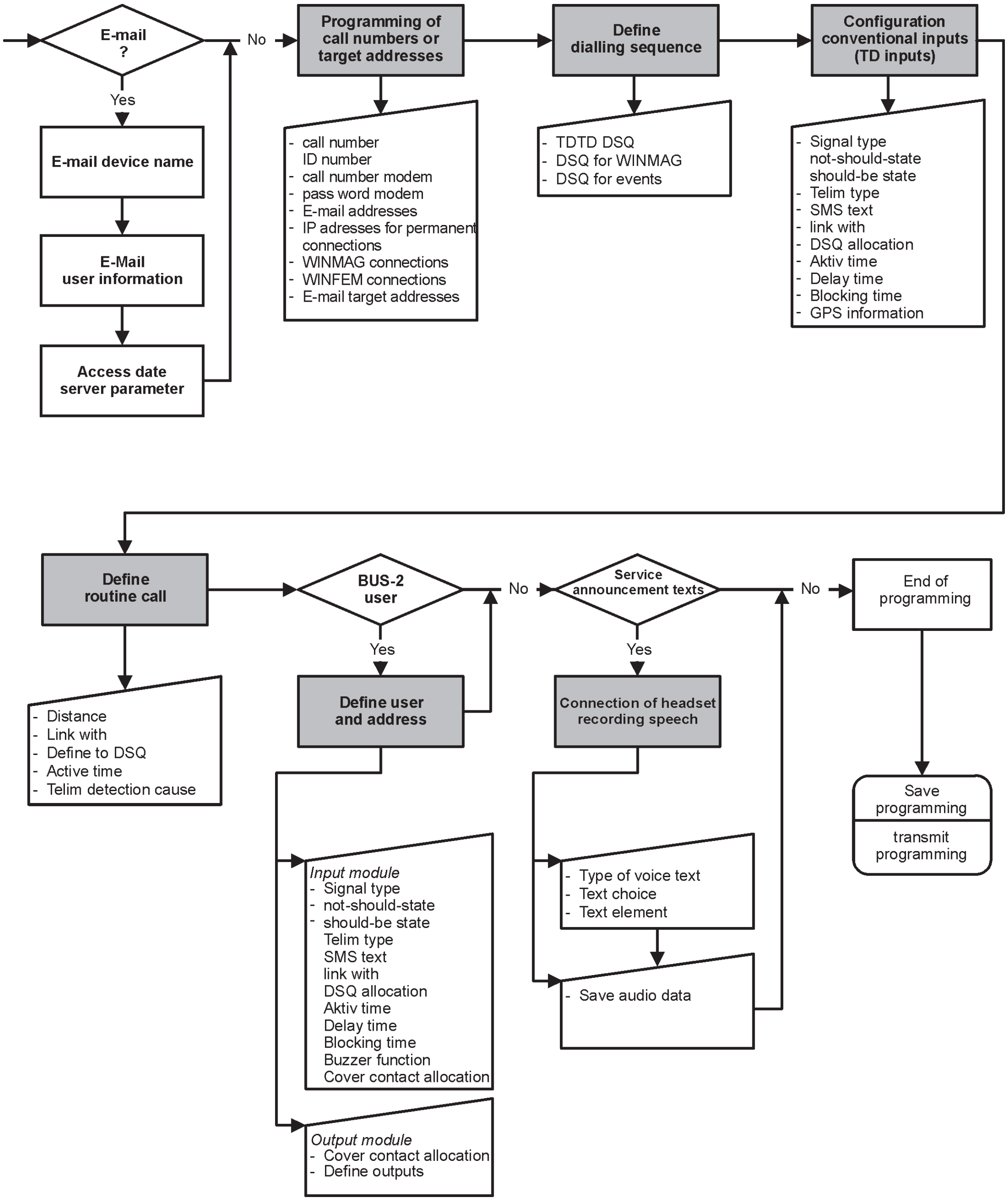


Basic function
This is a programming function that is absolutely necessary for the following programming or for the operation of the central control unit.

Function selection
If no changes are to be made on these parameters for the system to be programmed, this function can be skipped.

Optional function
This function must only be programmed if this is necessary due to the system configuration or system operating mode.

Function parameter
Possible selection or parameter within a function.


E-mail ?
No
Yes
E-mail device name
E-Mail user information
Access date server parameter
Programming of call numbers or target addresses
- call number
ID number
- call number modem
- pass word modem
- E-mail addresses
- IP adresses for permanent connections
- WINMAG connections
- WINFEM connections
- E-mail target addresses
Define dialling sequence
- TDTD DSQ
- DSQ for WINMAG
- DSQ for events
Configuration conventional inputs (TD inputs)
- Signal type
not-should-state
should-be state
- Telim type
- SMS text
- link with
- DSQ allocation
- Aktiv time
- Delay time
- Blocking time
- GPS information
Define routine call
- Distance
- Link with
- Define to DSQ
- Active time
- Telim detection cause
BUS-2 user
No
Yes
Define user and address
Input module
- Signal type
- not-should-state
- should-be state
Telim type
SMS text
link with
DSQ allocation
Aktiv time
Delay time
Blocking time
Buzzer function
Cover contact allocation
Output module
- Cover contact allocation
- Define outputs
Service announcement texts
No
Yes
Connection of headset recording speech
- Type of voice text
- Text choice
- Text element
- Save audio data
End of programming
Save programming
transmit programming

1. Basic information about WINFEM Advanced

The transmission devices DS 6700 / DS 6750 are programmed completely using the PC program WINFEM Advanced. The software running under the operating systems Windows uses the graphic possibilities for display and operation. The entire system programming and all object entries can be made directly on the PC, using the mouse as a convenient tool. The programming software permits quick and well-structured programming of the transmission device as well as storage and printout of the object-specific data and is equipped with a comprehensive plausibility check function. It is also possible to read out the complete configuration and the event memory of the transmission device with WINFEM Advanced.
The documents available to you here describe the transmission device's stand alone functions and how to program them. If the transmission device is used as an integration component within a hazard detection system, please consult Sections 1.5 to 1.7.
Transmission of the programming data for the transmission device's stand alone functions is performed via the direct (local) connection between the PC and the transmission device. A usual USB cable (A plug to B plug) is required as connection cable.
Remote programming via the public telephone network is also possible in conjunction with an analog modem on the PC which is connected to the transmission device. Remote configuration via a TCP/IP (Ethernet) network or via GPRS/UMTS (3G) is also possible.

In order to eliminate input errors, it is recommended to create precise documentation of the installed system components using WINFEM Advanced prior to programming.
The parameters required for programming, e.g. participant addresses, should be defined prior to programming.

We assume that you are familiar with the basic handling and use of your PC/laptop and Windows. If that is not the case, please consult the documentation which accompanies your PC/laptop or Windows operating system.

1.1 System requirements PC/laptop

- PC/Laptop, IBM-compatible as of Pentium 400 MHz,
  we recommend 1000 MHz
- 128 MB RAM min, we recommend 256 MB RAM
- Operating system *Windows 7 / 8 / 10, (32/64 bit).*
- 100 MB min. free space on the hard disk
- swap file managed by Windows
- graphics card and monitor with a resolution of 1024 x 768 pixels min.
- mouse or other Windows-compatible pointer
- 1 free USB connection or 1 free serial connection (COM)
- software WINFEM Advanced

Deactivate the "Power down mode" (stand-by mode) of the laptop/PC since problems with the data transfer might occur otherwise.

1.2 Installation of WINFEM Advanced

For detailed information about the installation of WINFEM Advanced, please read the WINFEM Advanced (P03170-26-000-xx) installation manual.

1.3 Multi-tasking

Although Windows is a multi-tasking operating system, WINFEM Advanced should be the only application running when making transmissions the PC to the system or vice versa. If the task is changed during a transmission, this might cause transmission errors or the transmission might be aborted.

1.4 Device programming using WINFEM Advanced

The programming software WINFEM “Advanced” version V19.xx or higher is required for programming performance features which are available as of firmware version V07.xx of the transmission devices DS 6700 (item no. 057864) and DS 6750 (item no. 057865)!
Older transmission devices can be programmed after specifying the respective device type and software version number (see Section 5.1).

1.5 DS 6700 / DS 6750 a integration module in hazard detection systems in compatibility mode

In compatible hazard detection control panels, the transmission device can be installed as an integrated module via BUS-2 or I-BUS. In this case, the transmission device is programmed as BUS-2 or I-BUS user in the framework of the control panel programming. The programming data are transmitted via the programming interface of the hazard detection control panels (e.g. BUS-2). Only the range of functions of the transmission device DGA 2400 is supported.
The parameters required for use of the new performance features cannot be directly programmed and stored using WINFEM Advanced during control panel programming, (please note the instructions on configuration in Section 6.1).

If the transmission device is used as an integration component in a hazard detection system and performance features are to be used that are not supported by the hazard detection system, they have to be implemented via the stand alone part of the transmission device.

1.6 DS 6750 extended compatibility mode in hazard detection system

When using this option, MB control panels connected via BUS-2 and I-BUS can transmit alarm notifications via Ethernet (IP connections). Email and AWAG (dialler and transmission device) functionalities can also be used.
Due to the fact that these transmission paths and protocols with BUS-2 and I-BUS use connection technology as used in older hazard detection systems are not configurable in the corresponding hazard detection systems, that is performed using a conversion table in the transmission device DS 6750. Both devices must be configured separately even with different versions of WINFEM in some cases (e.g. for older MB control panel types). Refer to the section 18.1 for information on programming and the conversion table

1.7 DS 6700 / DS 6750 as integration module in hazard detection control panels in IACP RS-232 mode

As of version V03.xx, the transmission device can be integrated into hazard detection control panels via the V.24 interface of the hazard detection control panel and the serial S1 (RS-232) interface of the transmission device. A list of the compatible control panels and the software versions required is to be found in the installation Instructions of the transmission device. In this type of connection, the IP and speech functions are directly programmable via WINFEM Advanced. The input criteria for the conventional detector group inputs (E1-E8) can be used simultaneously.

Only the USB connection of the transmission device is used in this configuration to connect the WINFEM Advanced to the IPC. Direct connection via the control panel's V.24 is not possible because the interface is occupied (please note the connection instructions in the installation connection instructions for the transmission device!).

2. WINFEM Advanced installation

The programming software for WINFEM Advanced is on the enclosed CD. The CD also contains the entire documentation of the hazard detection control panel and the transmission device in Acrobat Reader format (.pdf) as well as the Adobe Acrobat Reader program. Please observe the notes in the end user license agreement of Adobe Acrobat Reader.

2.1 Installing WINFEM Advanced

The following section describes the installation from a CD.

1. Insert the WINFEM Advanced CD into your CD-ROM drive.

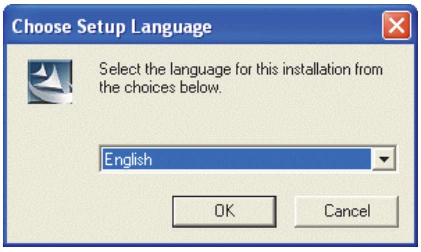
2. Click the "Start" button in the Windows task bar. Click on **"Settings"** ▸ **"Control panel"**, double click on **"Software"**. Click the **"Install" button** on the **"Install/Uninstall" tab**.

   Windows automatically looks for an installation program on CD. If the installation file is not found automatically, file "setup.exe" must be entered manually via "Browse". The file is located directly in the root directory of the CD.
   Click on **"Finish"** to start the installation.

3. The installation program for WINFEM Advanced is started.

   First you will be asked to choose the language for the installation procedure.

   Confirm your selection with "OK".



Choose Setup Language

Select the language for this installation from the choices below.

English

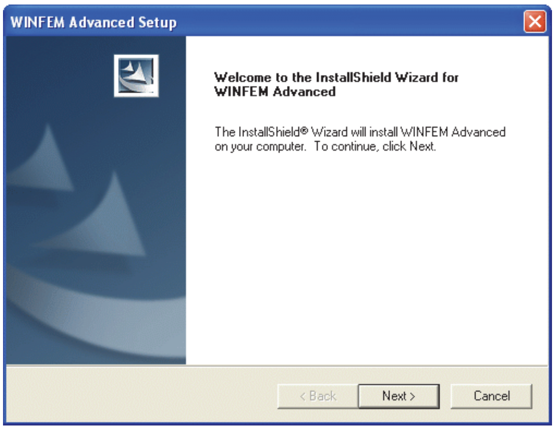
4. The InstallShield prepares the installation of WINFEM Advanced and then starts the actual installation of WINFEM.

   During the installation process, a window opens in which you are prompted to select the installation directory.

   Factory setting for the installation:
   C:\Honeywell\WINFEM Advanced

   Recommendation: press Next to accept.

   Because of the changed structure of the data, user and rights in Windows 7, WINFEM Advanced from Version 07 on will be installed in the “Honeywell” folder and no longer in the “Programs” folder.



WINFEM Advanced Setup

Welcome to the InstallShield Wizard for WINFEM Advanced

The InstallShield® Wizard will install WINFEM Advanced on your computer. To continue, click Next.

When you have selected the installation directory, click "Next" to continue.

Then you will be requested to specify the program directory from which WINFEM Advanced can be started. Click "Next" to confirm.
Now you are asked whether the entries are valid or whether you want to make any changes. If no changes are to be made, start the copying process by clicking "Next".
WINFEM Advanced indicates when the installation has been completed successfully. Click "Finish" to complete the installation.

Additional dialog when updating a WINFEM Advanced version (or when file "setup.exe” is selected once again):

- Modify/repair program

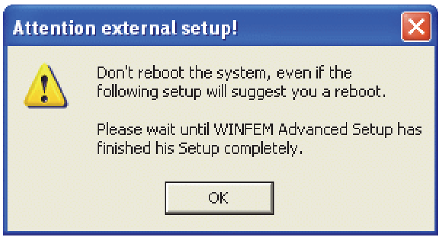
These two menu items perform the same function within the WINFEM Advanced installation. With this function, the "new" WINFEM Advanced is installed in the WINFEM Advanced directory which already exists. You don't have to specify the installation directory manually in this case, since the installation program finds the installation directory automatically.

- Remove

This function uninstalls WINFEM Advanced. Configuration and programming data are not deleted in this case.
Start the action required by clicking "Next".

5. The further steps of the installation are identical for new installations and updates.

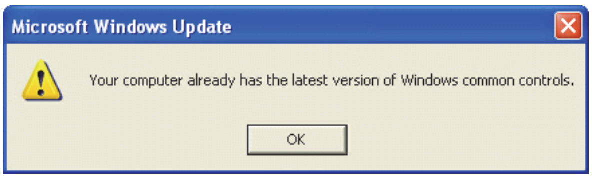
6. **Important!**



Attention external setup!

Don't reboot the system, even if the following setup will suggest you a reboot.

Please wait until WINFEM Advanced Setup has finished his Setup completely.



Microsoft Windows Update

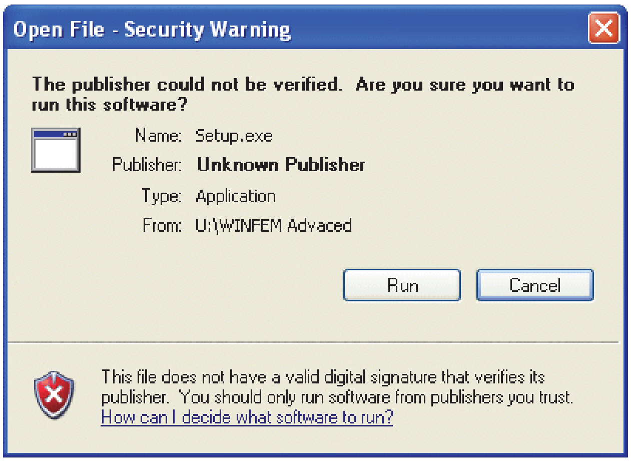
Your computer already has the latest version of Windows common controls.

During the installation of the Windows driver files, you may be prompted to restart (boot) the system. Do not restart (reboot) the system but wait until all installation routines have been completed.

For the registration of the new driver files in Windows, it is necessary to restart the computer when the WINFEM installation has been completed.

2.2 Installation under Windows

Due to the security settings within WINDOWS, a security warning might be output when the installation of WINFEM Advanced is made from a "non-local" drive, e.g. a network drive.



Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

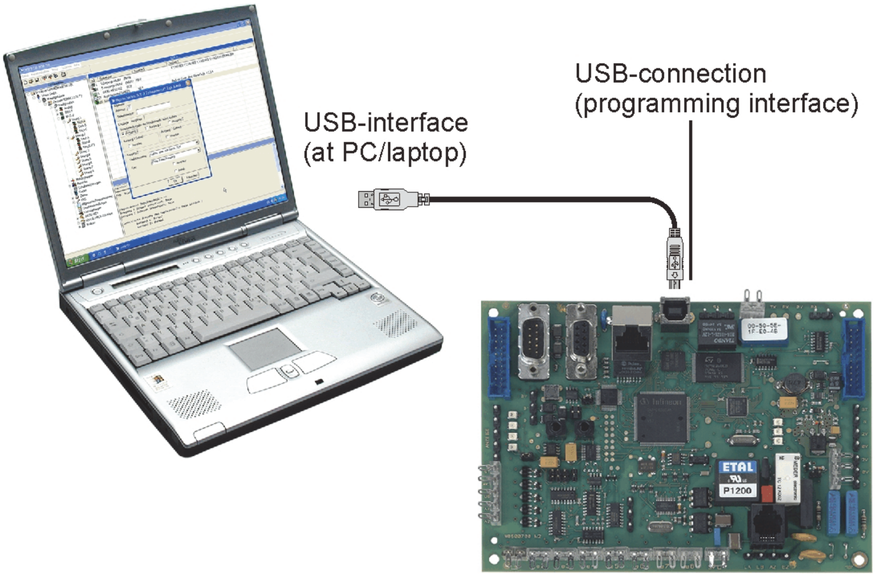
Name: Setup.exe
Publisher: **Unknown Publisher**
Type: Application
From: U:\WINFEM Advaced

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?

This warning is generated directly by WINDOWS. If you know where the file comes from (e.g. download from our homepage), this warning can be skipped for the installation of WINFEM Advanced.

3. Connecting a PC/laptop to the transmission device

The connection is made via the USB connection of the transmission device.



How to proceed to connect a PC/laptop to the USB connection:

1. - Supply operating voltage (+12V DC) to the transmission device.

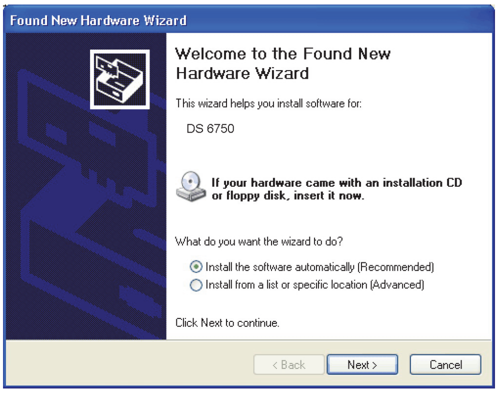
2. - Switch PC/laptop on

3. - Start WINFEM

4. - Connect USB cable (A-plug to B-plug) to the PC/laptop and the transmission device.

3.1 Notes on the USB driver

When connecting the transmission device via the USB connection, you might be requested to install the hardware driver (USB driver) for the connected transmission device. Please follow the instructions of the wizard and have it look for a suitable driver for the device. (example):



Welcome to the Found New Hardware Wizard

This wizard helps you install software for:

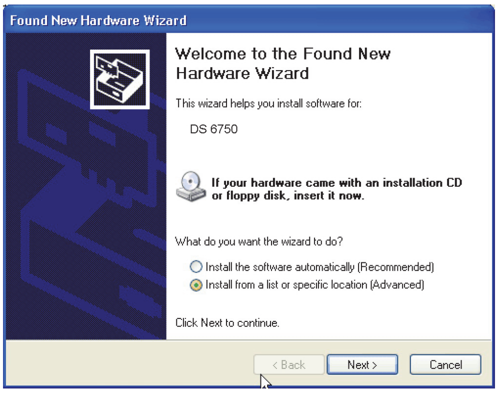
DS 6750

If your hardware came with an installation CD or floppy disk, insert it now.

What do you want the wizard to do?

● Install the software automatically (Recommended)
○ Install from a list or specific location (Advanced)

Click Next to continue.



Welcome to the Found New Hardware Wizard

This wizard helps you install software for:

DS 6750

If your hardware came with an installation CD or floppy disk, insert it now.

What do you want the wizard to do?

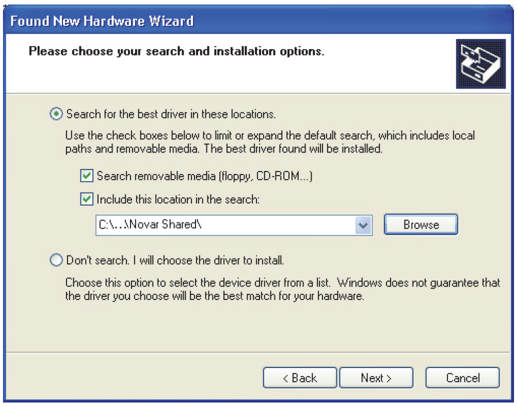
○ Install the software automatically (Recommended)
● Install from a list or specific location (Advanced)

Click Next to continue.

If the wizard requests you to search the driver files, enter the following path:

C:\Honeywell\Novar Shared\USBDriver

Installation drive of the program (C:)



Found New Hardware Wizard

Please choose your search and installation options.

● Search for the best driver in these locations.

Use the check boxes below to limit or expand the default search, which includes local paths and removable media. The best driver found will be installed.

☑ Search removable media (floppy, CD-ROM...)

☑ Include this location in the search:

C:\...\Novar Shared\

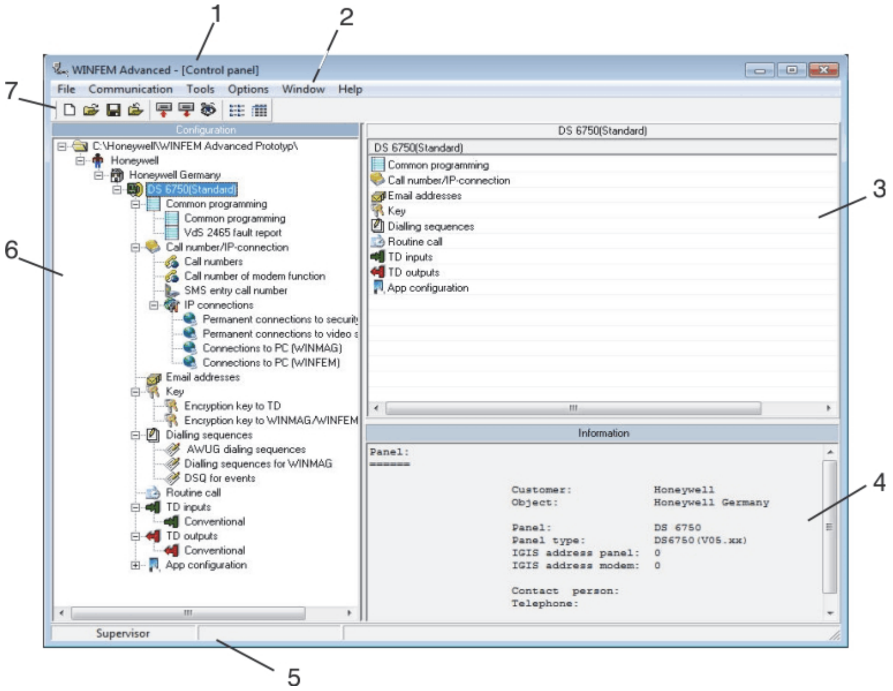
○ Don't search. I will choose the driver to install.

Choose this option to select the device driver from a list. Windows does not guarantee that the driver you choose will be the best match for your hardware.

4. The WINFEM Advanced screen

4.1 General information concerning the WINFEM Advanced screen

The WINFEM Advanced screen has the following structure:



```
Panel:
======

          Customer:            Honeywell
          Object:              Honeywell Germany

          Panel:               DS 6750
          Panel type:          DS6750 (V05.xx)
          IGIS address panel:  0
          IGIS address modem:  0

          Contact  person:
          Telephone:
```

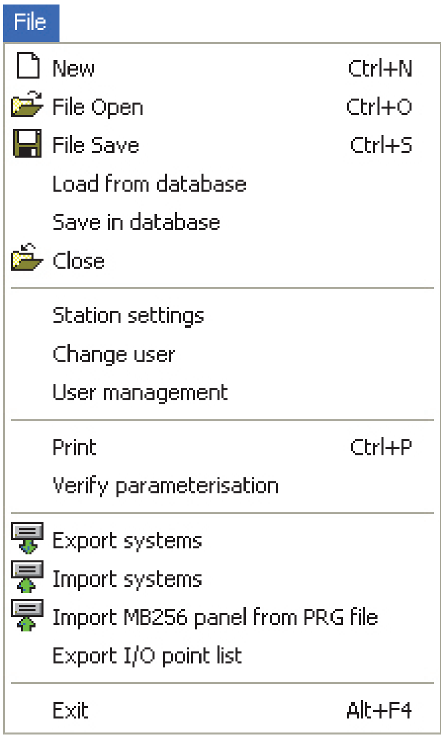
1 - Title bar	2 - Menu bar
3 - Component/status window	4 - Information window
5 - WINFEM status line	6 - Configuration window
7 - Toolbar	

4.2 Title bar

The title bar shows the name of the program.

4.3 Menu bar

4.3.1 Drop-down menu "File"



4.3.1.1 The "New" command
A new program file with the standard parameters is created.

4.3.1.2 The "Open file" command
The "Open file" command loads a saved program file (hard disk, floppy disk, network) into WINFEM Advanced for further processing.
When "Open file" is selected within the programming process for a control panel, you will be asked whether the programming is to be saved.

4.3.1.3 The "Save file" command
Saves the current programming. The file name may comprise 256 characters max. File type ".prx" is added automatically by WINFEM Advanced.

4.3.1.4 The "Load from database" command
This menu item is used for loading data from the internal database for processing. A distinction is made between

- Standard data and
- system specific data.

The standard data correspond to the programming data which are defined during standard programming of the device.

In case of system-specific programming, these data are modified in such a way that they correspond to the actual system configuration. So system data are programming data which have already been created and saved manually. The name of the loaded programming data is shown next to the system name.

4.3.1.5 The "Save in database" command
Saves programming data in the integrated database.

4.3.1.6 The "Close" command
The ongoing programming is closed, but WINFEM Advanced remains open.

4.3.1.7 The "Station settings" command
This command is used to assign a station name and a station number to the WINFEM laptop/PC.
During programming with WINFEM Advanced, the station name and the station number are transmitted to the device. In addition, the user name and the user number are transmitted. The station number and the user number are stored in the event memory.

4.3.1.8 The "Change user" command
This command is used to change to another user for WINFEM Advanced. When a transmission is made to the device, the user number is entered together with the station number in the event memory of the device.

4.3.1.9 The "User management" command
New users as well as the corresponding passwords can be defined here. It is also possible to change passwords, if required.

Changing the password: The supervisor can change the password for each user. Other users can only change their own passwords.
The standard password for the supervisor (winfem) should always be changed to prevent unauthorized access by a third party.

4.3.1.10 The "Print" command
When this command is selected, the print parameter selection window opens. In this window, you can define the print parameters for the printout. It is also possible to select print preview.

4.3.1.11 The "Verify parameterization" command
This command is used to carry out a plausibility check of the output references, text references, detector group references and the detector groups (in preparation).

4.3.1.12 The "Export systems" command
This command is used to export stored systems/device programming. The exported programming can be imported on a second PC/laptop. This function can be used to centrally archive and manage systems/device programming made e.g. on service laptops.
The files have the extension .fdb. Select the desired systems/device programming by activating the corresponding check box(es).

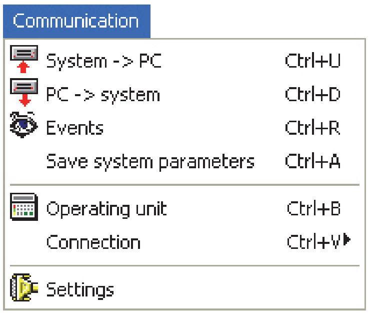
4.3.1.13 The "Import systems" command
This function can be used to import system/device programming created as .fdb files with command "Export files" on a PC/laptop.

4.3.1.14 The “Import MB256 panel from PRG file” command
This command is used to import programming data of a control panel 561-MB256 created with WINFEM-256 directly into WINFEM Advanced. For this purpose, the data must be saved as prg-file in WINFEM-256. When the import is carried out, the customer, the object and the system data are created automatically. In addition, the control panel programming is saved to the database of the control panel.

4.3.1.15 The "I/O point list" command
This command is used to save the programming of a control panel as I/O point list in .txt-format. This file can be imported into the security management software WINMAG.

4.3.1.16 Exit
Program WINFEM Advanced is terminated.

4.3.2 The "Communication" drop-down menu



4.3.2.1 The "Panel -> PC" command
The current configuration data of the system/device is loaded to the PC/laptop for checking or processing.

4.3.2.2 The "PC -> Panel" command
The current configuration data from WINFEM Advanced are loaded into the system/device.

The existing programming in the system/device is overwritten with the data transmitted from the PC! Therefore, check the programming carefully before transmitting it from the PC to the system/device!

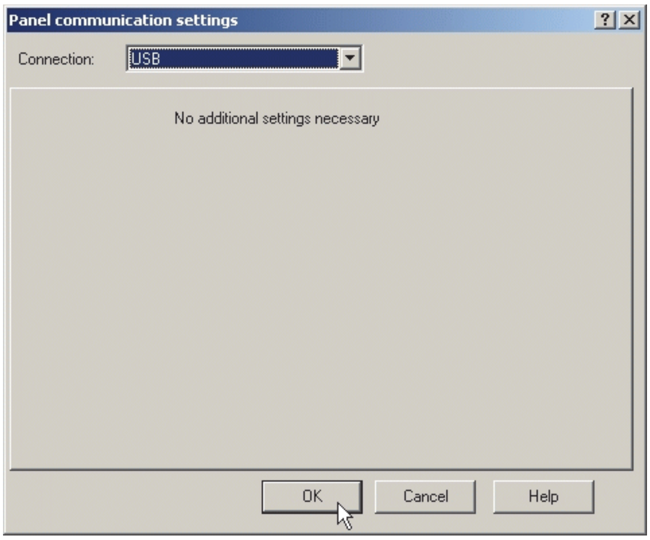
4.3.2.3 The "Events" command
When command "Events" has been selected, you can define in this window which events from the event memory of the device are to be displayed. For detailed information on the "Event memory", please refer to Section "5.3 Event memory".

4.3.2.4 The "Connection" command
When you click on "Connection" another selection menu is opened.

"Establish": A connection is established between the PC/laptop and the system/device according to the connection type selected under "*Communication→Settings*".

"Disconnect": An existing communication connection between PC/laptop and the system/device is disconnected.

4.3.2.5 The "Settings" command
In menu item "Settings", the parameters for connecting PC/laptop and system/device are defined.



Connection: USB

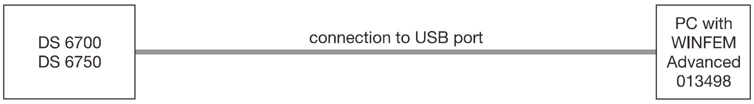
No additional settings necessary

The following connection types are available:

- USB
- TCP/IP
- Modem-DS 14400baud

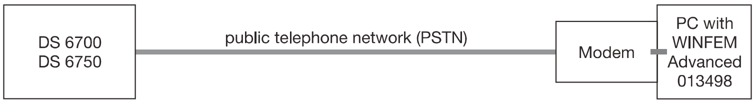
Connection types

<u>- USB</u>
The WINFEM PC is connected to the device via USB.



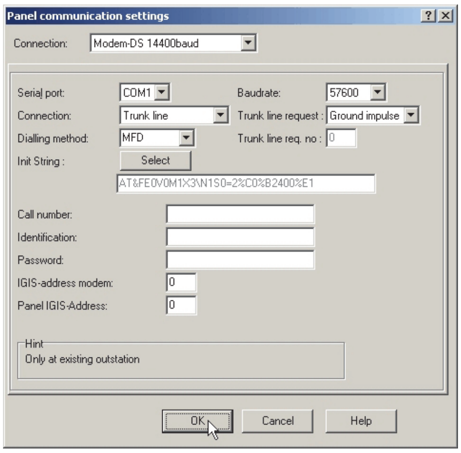
Settings: No further settings are required.

<u>- Modem-DS 14400baud</u>
The WINFEM PC is connected to the control panel via the public telephone network. (PSTN) A Hayes compatible modem (e.g. item no. 058200, external High Speed Modem V.90) is required on the PC side and a DS 6700 or DS 6750 is required on the control panel side. With the transmission device DS 6700 / DS 6750, a connection can be established with 14400 Baud.


DS 6700
DS 6750
public telephone network (PSTN)
Modem
PC with WINFEM Advanced 013498

Settings: "Modem" interfacing → initialization string

The communication parameters of the modem connected to WINFEM have to be set to V32bis. This can be done by setting the AT command: “AT+MS=V32b,1,4800,14400,4800,14400".



Panel communication settings

Connection: Modem-DS 14400baud

Serial port: COM1

Baudrate: 57600

Connection: Trunk line

Trunk line request : Ground impulse

Dialling method: MFD

Trunk line req. no : 0

Init String : Select

AT&FE0V0M1X3\N1S0=2%C0%B2400%E1

Call number:

Identification:

Password:

IGIS-address modem: 0

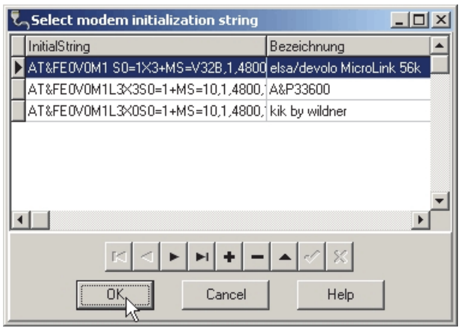
Panel IGIS-Address: 0

Hint: Only at existing outstation

After selecting the right connection and clicking “init String -> select” a initialization string can be select for the modem.
The PC and modem must speak the same language for the PC can send commands to the modem or evaluate feedback from the modem. The AT command set is considered the world wide standard for modem control command syntax. These control commands are summarized under WINFEM in an initialization string.
For several modem types this initialization string is pre-assigned an can be selected directly. Pre-assigned and released modems are:

- Elsa or Devolo MicroLink 56k
- A&P 33600
- kik by wildner

Please observe, that not released modems are not supported by our technical support. Create a modem initialization string with the editor as described below if necessary.



Select modem initialization string

InitialString	Bezeichnung
AT&FE0V0M1 S0=1X3+MS=V32B,1,4800	elsa/devolo MicroLink 56k
AT&FE0V0M1L3X3S0=1+MS=10,1,4800,1	A&P33600
AT&FE0V0M1L3X0S0=1+MS=10,1,4800,1	kik by wildner

Buttons in the selection menu have the following functions:

⏮ Jumps to the first data record in a list.

◀ Jumps to the previous data record in a list.

▶ Jumps to the next data record in a list.

⏭ Jumps to the last data record in a list.

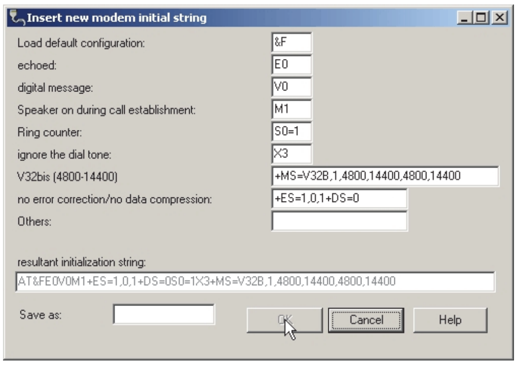
✚ The editor for creating a new data record (new type of modem) is started. If your modem type is not in this list, the appropriate initialization string can be created using this editor.

━ The currently selected data record (modem type) is deleted from the list.

▲ The currently selected data record is opened for editing. For actual processing, click with the cursor in the highlighted line.

✓ Finish editing a data record and confirm changes.

✕ Cancel editing of a data record without accepting changes.



Insert new modem initial string

Load default configuration:	&F
echoed:	E0
digital message:	V0
Speaker on during call establishment:	M1
Ring counter:	S0=1
ignore the dial tone:	X3
V32bis (4800-14400)	+MS=V32B,1,4800,14400,4800,14400
no error correction/no data compression:	+ES=1,0,1+DS=0
Others:	

resultant initialization string:

AT&FE0V0M1+ES=1,0,1+DS=0S0=1X3+MS=V32B,1,4800,14400,4800,14400

Save as:

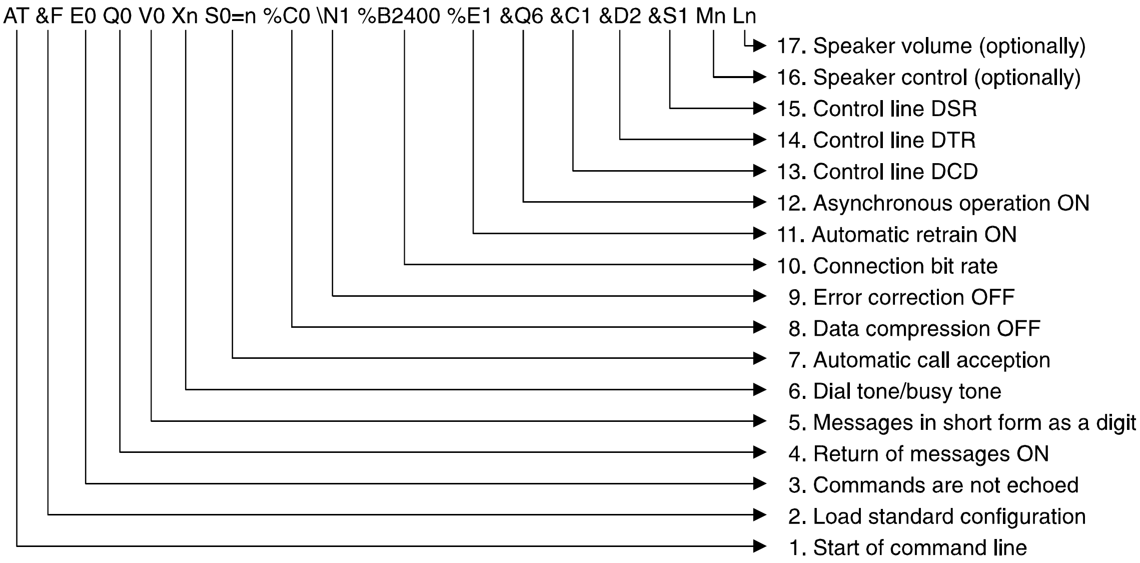
The Editor allows you to create a modem initialization string.

All command fields that are mandatory for operating with WINFEM appear in the editor screen. Some fields already contain commands. These are commands that are used by most modem manufacturers.

There are no set rules for the command syntax of the initialization string, it is structured differently for each modem. Consult the manual of your modem to enter the correct command syntax.

The following commands are required to initialize the modem:

ℹ If any of the commands listed correspond with the default settings of your modem, these commands do not have to be entered.



AT &F E0 Q0 V0 Xn S0=n %C0 \N1 %B2400 %E1 &Q6 &C1 &D2 &S1 Mn Ln

17. Speaker volume (optionally)
16. Speaker control (optionally)
15. Control line DSR
14. Control line DTR
13. Control line DCD
12. Asynchronous operation ON
11. Automatic retrain ON
10. Connection bit rate
9. Error correction OFF
8. Data compression OFF
7. Automatic call acception
6. Dial tone/busy tone
5. Messages in short form as a digit
4. Return of messages ON
3. Commands are not echoed
2. Load standard configuration
1. Start of command line

Initialization string commands

ℹ Due to the numerous different types of modems available, the following command syntax is only to be regarded as an example because they differ from modem to modem.

1. **AT** **AT** is used to initiate all commands that are to be sent to the modem. You can write either "AT" or "at" "At" and "aT" are not permitted.

2. **&F** Loads the modem's standard parameter setting.

3. **E0** Switches off the command echo from the modem.

4. **Q0** Feedback from the modem to the PC is generally active.

5. **V0** Feedback from the modem to the PC is sent in short form as numbers.

6. **X*n*** The dialing behavior is set using this command:

   X0: Ignore dialing tone/engaged tone
   X1: Ignore dialing tone/engaged tone
   X2: Wait on dialing tone / ignore engaged tone
   X3: Ignore dialing tone/evaluate engaged tone
   X4: Evaluate dialing tone/evaluate engaged tone

   The X2 and X4 settings can only be used on a main line or an extension with trunk line simulation.

7. **S0=n** The value **n** indicates the number of rings after which the call is accepted automatically. This is required for "remote parameterization by callback". We recommend setting **S0=2**.

8. **%C0** This command switches data compression off.
   command may also be called **&K0** for some modems.

9. **\N1** When \N1 is entered, the connection is generated without error correction in direct mode.
   On some modems this command is entered as \N0 .
   This command is related to *%Cn*. No data compression is possible with \N0 or \N1.
   On modems initialized using the **&K0** command, error correction is already deactivated by this command.

10. **%B2400** The **%B2400** command sets the transmission speed/baud rate (telephone-side) to 2400 bit/s (V22bis).
    The command syntax for setting the transmission speed differs from that above for some modems. Depending on the modem, other possible entries include **B7** or **&N14** or **+MS=2**.

11. **%E1** (auto retrain) This command resynchronizes the connection parameters if the signal quality is bad.
    The command may also be called ***Q1** for some modems.

12. **&Q6** Asynchronous operation (commands and data). The command syntax may also be **&Q0** or **&M0** or **&M2** depending on the modem.

13. **&C1** The DCD control line indicates the available carrier.

14. **&D2** When this command is set, the modem hangs up when the control line DTR changes from ON to OFF and enters the commend mode.

15. **&S1** The DSR control line is only active in the period between the answer tone and disconnection (in accordance with CCITT).

The following commands are not strictly necessary.

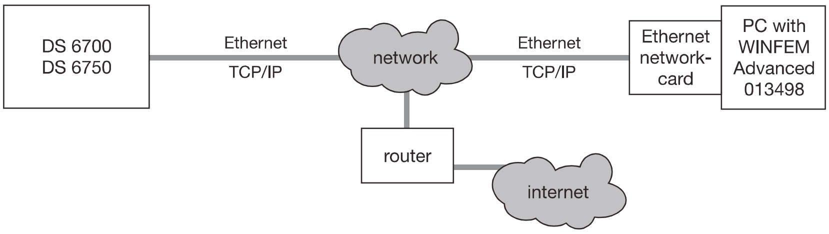
16. **Mn** **n** indicates the operation mode in which the speaker is active.

17. **Ln** **n** sets the volume.

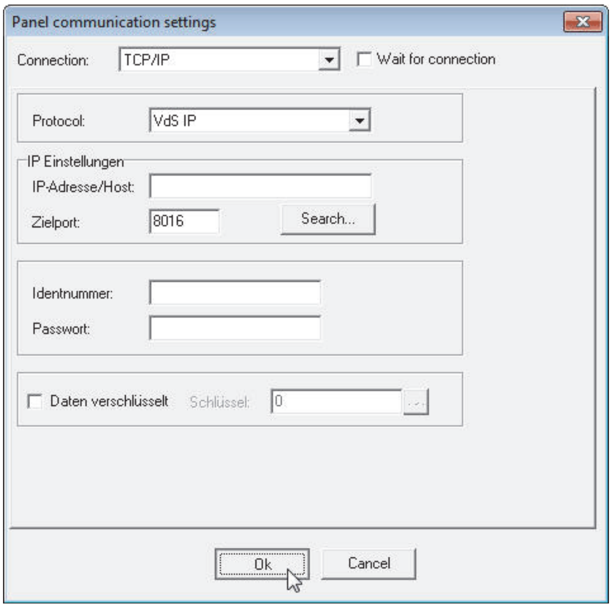
When the initialization string is complete, save the file under an appropriate name.

TCP/IP

WINFEM PC is connected to the device via an Ethernet network. The PC is connected to the Ethernet network via an Ethernet network card.



These same TCP/IP settings are also used in establishing a connection when the function "Establishing a connection with SMS-trigger" (see chapter 8.4.3) is invoked.


Panel communication settings

Connection: TCP/IP □ Wait for connection

Protocol: VdS IP

IP Einstellungen

IP-Adresse/Host:

Zielport: 8016

Identnummer:

Passwort:

□ Daten verschlüsselt Schlüssel: 0

Settings:
IP address or domain name:
Network address at which the control pane or transmission device can be reached within the Ethernet network.

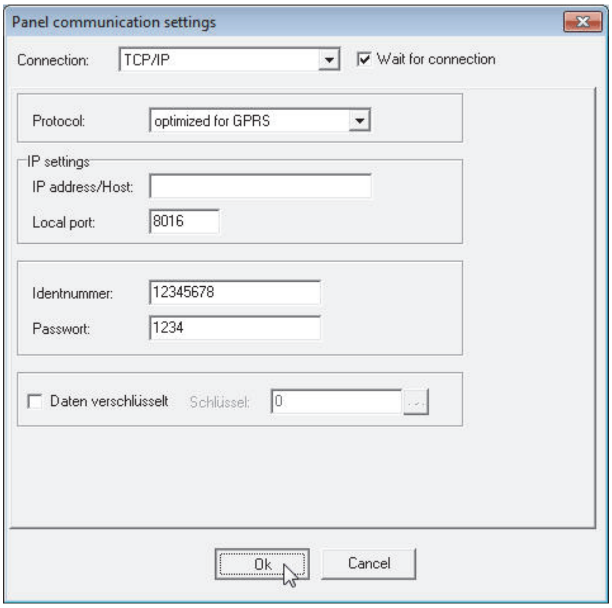
Destination port:
The destination port is the address component within the network protocol. It is necessary to assign the data packets to the right service.

“Search” button:
Opens the dialog for the transmission device search. Transmission devices which are in the same IP network can be located using this search function. Found devices issued with the name, serial no. and IP address.

ID no..:
The device identifies itself to the WINFEM PC with this code. This ID no. is not identical to the ID no. for modem and PSTN. The ID no. can consist of up to 12 digits.

Password:
Like the ID number, the password also serves as additional protection against unauthorized access to the control panel or the transmission device. The PC WINFEM identifies itself with the device with this password. This password is not identical with the password for modem and PSTN. The password can consist of up to 8 digits.

The ID no. and password must be stored within the device programming in one of the WINFEM connections. Otherwise, no connection is made.



Panel communication settings

Connection: TCP/IP ☑ Wait for connection

Protocol: optimized for GPRS

IP settings

IP address/Host:

Local port: 8016

Identnummer: 12345678

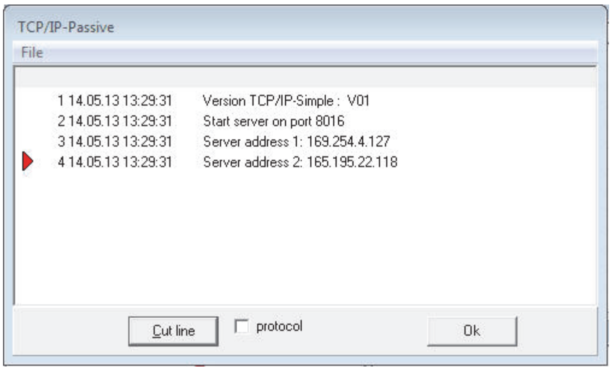
Passwort: 1234

☐ Daten verschlüsselt Schlüssel: 0

Wait for connection:
Only for transmission devices that support the function "Remote Maintenance with SMS-trigger". The default protocol for the WINFEM-PC is "optimized for GPRS" and the default local port is 8016. The following procedure is used to establish a connection with the desired system:

- To allow connections to be set up via SMS-trigger, the transmission device must be programmed in accordance with the specifications in chapter 8.4.3.

- The transmission device to be used for connection setup is selected by entering the ID no. and password. After this information is entered and confirmed via the "ok" button, the connection window showing the server address, namely the address of the WINFEM-PC, is displayed.



TCP/IP-Passive

```
1 14.05.13 13:29:31    Version TCP/IP-Simple :  V01
2 14.05.13 13:29:31    Start server on port 8016
3 14.05.13 13:29:31    Server address 1: 169.254.4.127
4 14.05.13 13:29:31    Server address 2: 165.195.22.118
```

- The connection window remains open till the connection attempt is successful or aborts.

As described in chapter 8.4.3, a connection can now be requested via an SMS-trigger.

Please note: The server address of the WINFEM-PC displayed is in most cases a local IP address, since the PC is located behind a router. If a local IP address is communicated to the transmission device via an SMS-trigger, a connection can be established in the local network only.
A connection to transmission devices outside the local IP network can be established only via the router's public IP address or via a dynamic DNS address or DDNS address with the appropriate port-forwarding configured in the router. After a DDNS address is assigned, the WINFEM-PC continues to be accessible at the same domain name even if the current IP address is unknown. The responsible network administrator can provide more information.

The ID no. and password must be stored in the device programming in one of the WINFEM connections. Otherwise, no connection is made.

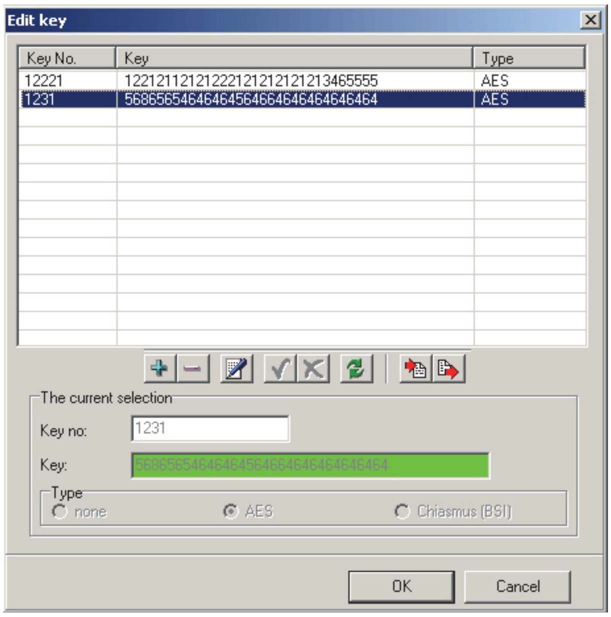
Encrypted data: data transmitted via IP networks is at increased risk of manipulation. The IP connections must therefore be encrypted under certain conditions and with increased security requirements. If manipulation by third parties can not be excluded for the IP network, then data transfer has to be encrypted.
This requires that the installer store the encryption method and key configuration in the control panel or transmission device in advance.

If the "Data encrypted" check box is selected, the button ••• is available for starting the key editor.
This editor can be used to select an existing key for transmission. In addition to this, new keys can be created and stored in the key database.

The keys used here are used for encrypted data transmission between WINFEM/WINMAG and the control panel or transmission device. Programming of these keys is independent of the programming of the keys in Section 10! Keys in Section 10 are only used for encrypted data transmission between the transmission device and the control center (security service).

VdS IP protocol: Default setting: VdS IP protocol

Key editor



Edit key

Key No.	Key	Type
12221	1221211212122212121212121213465555	AES
1231	56865654646464564664646464646464	AES

The current selection

Key no: 1231

Key: 56865654646464564664646464646464

Type ○ none ● AES ○ Chiasmus (BSI)

Buttons in the editor have the following functions:

✚ The fields "Current Selection" for creation of a new data set (key) will be released for use.

− The currently selected data record (key) is deleted from the list.

✎ The currently selected data record (key) is opened for editing. For actual processing, click with the cursor in the highlighted line.

✓ End creation or editing a data record (key) and accept changes.

✗ Cancel creation or editing of a data record without accepting any changes.

⟳ All changes made since starting the key editor are reverted.

⇦ Import a key file (*.key) in WINFEM Advanced.

⇨ Export the data records in a key file (*.key).

"Current Selection" field ✚ - Create or edit key

- Input field key number

The key number is the defined name of the key. This key number is communicated to the receiving device during or before exchange of encrypted data so that it can use the correct key for encoding and decoding the data.
It has to be ensured that both communication partners (WINFEM and control panel) have the same key with an identical key number.
Permissible values for the key number: 1 - 65534.
The use of identical key numbers for different keys is not possible.

- Key input field

  The encryption methods AES and Chiasmus (BSI) (only DS 6750) are supported.

  A 128-bit key is used for the AES encryption algorithm. The key therefore consists of 32 characters (16 bytes). The entry must be hexadecimal. Possible characters are 0 - 9 and A - F.

  The Chiasmus encryption algorithm uses a 160-bit key. The key therefore consists of 40 characters (20 bytes). The entry must be hexadecimal. Possible characters are 0 - 9 and A - F.

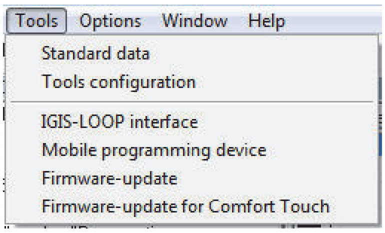
- Generate random key

  WINFEM offers the following option for generating a random key:
  A context menu is displayed by clicking with the right mouse button within the input field. Clicking on the menu item "Create random key" launches an additional program to generate a random key.

- Encryption type selection

  AES or Chiasmus (BSI) (only DS 6750) can be entered as the encryption type.

4.3.3 Drop-down menu "Tools"



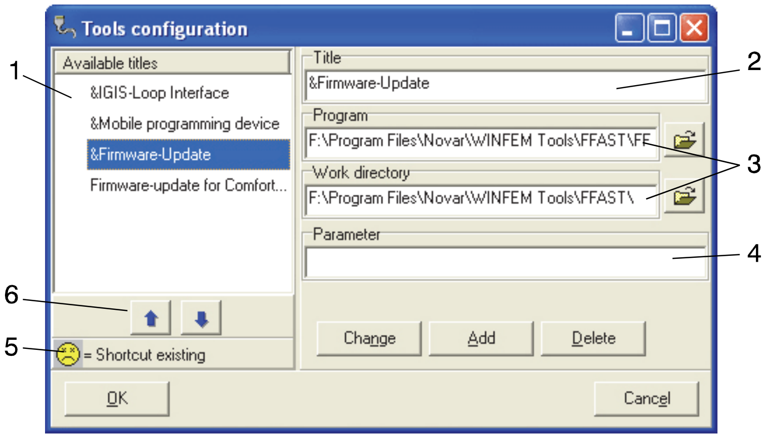
The drop-down menu "Tools" permits direct access to your preferred programs, directly from WINFEM Advanced. When WINFEM Advanced is installed, the programs "Firmware-Update", "IGIS-LOOP Interface", "Mobile Programming Device" and "Firmware-Update for Comfort Touch" are installed by default.

4.3.3.1 Standard data

With this command, you can reset selective areas of the currently loaded programming back to the the factory default programming.

4.3.3.2 Tools configuration

You can use this command to add further programs to the drop-down menu and to edit or delete existing entries of the Tools menu. A maximum of 15 menu entries can be configured.



Title: &Firmware-Update

Program: F:\Program Files\Novar\WINFEM Tools\FFAST\FF

Work directory: F:\Program Files\Novar\WINFEM Tools\FFAST\

Parameter:

1 - Program/title list
2 - Program name/title entry field
3 - Entry fields for path of program file and working directory
4 - Entry field for additional parameters
5 - Symbol for double allocation of shortcut keys
6 - Move buttons

- Program/title list

  This list shows the programs/titles which can be started directly via the drop-down menu. The sequence (from top to bottom) in which the programs are shown in this list is identical with the sequence within the drop-down menu. You can use the move buttons (6) to customize the sequence of the programs.
  The symbol (5) indicates that the same shortcut key is used for 2 or more programs (see program name/title entry field for assigning shortcut keys).

- Program name/title entry field

  The program name/title that appear within the drop-down menu is entered here. The position of the "&"character determines the shortcut key of the program.

Example:	&Portable programmer	>	Portable programmer
	Portable &programmer	>	Portable programmer
	Portable progra&mmer	>	Portable programmer

With this shortcut key, the desired program within the drop-down menu can be started easily when you press the corresponding alphabetic key.

- Entry fields for path of program file and working directory

  - Program: The path and the name of the program file to be started is entered into this field.

  - Working directory: Normally, the directory containing the executable program file is specified here. In some cases, however, programs require files which are stored in other directories. In this case, the directory where these files are located must be entered here so that the program can find them.

- Entry field for additional parameters

  Some programs can be started in different modes by adding additional parameters. These parameters can be entered in this field.

4.3.3.3 Firmware update (FFAST)

Tool for programming the Flash EPROM of transmission devices DS 6600 / DS 7600 / DS 7700 / DS 9500 / DS 9600 and the control panels 561-HB24, 561-MB24, 561-HB48.10, 561-MB100.10 as well as the graphic operating unit 012570. For further information, please see Section "19. Firmware Update".

4.3.3.4 IGIS-LOOP interface

IGIS-LOOP terminal program for the configuration of the IGIS-LOOP Controller 013330.10.
For detailed information on the programming of the IGIS-LOOP Controller, please see the "Instructions for the Installer - Security Network IGIS-LOOP / P03310-02-000-XX".

4.3.3.5 Portable programmer

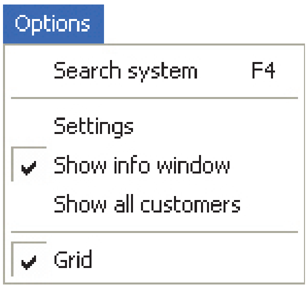
Software emulation of the "Mobile programming device 059998". By means of this emulation, it is possible to program devices which are addressed by the mobile programming device via the terminal mode.
Currently, the following devices can be programmed:

- transmission devices DGA 2400 / DS 8800 / DS 7500-ISDN / DS 7500-ISDN/IGIS
- fire alarm panel BMZ 708

4.3.3.6 Firmware update for Comfort Touch

Tool for programming the flash EPROM of graphic operating unit 012575.
For further information on this subject, please refer to the “Mounting and Connecting Instructions for Operating and Display Panel P00454-10-002-xx”.

4.3.4 Drop-down menu "Options"



4.3.4.1 Search system
The "Search system" command provides a very convenient method for finding certain system programming.
The available search criteria are the name, the place and the street of the desired system.

4.3.4.2 Settings

- Preferences - Sounds
  This menu provides the possibility to activate, deactivate or adjust sounds for the individual events.

- Presettings - Presettings for transmission to the panel
  - Check the configuration for consistency before sending it.
    Before the programming is transmitted definitely from the PC to the control panel, WINFEM identifies the BUS-2 users actually connected to the panel and compares the data with the specifications within the WINFEM programming. If differences are found, they will be displayed.
    If the check box is not activated, the transmission will be made without prior check.

  - Request if the connection is to be cut after transmission.
    If this check box is activated, there will be a request if the connection panel <-> PC is to be cut after a transmission from the panel to the PC or vice versa has been completed. If this function is not activated, the connection is maintained without request.

  - Automatically disconnect RDT connection after a transmission.
    When the transmission via RDT (modem or PSTN) from the panel to the PC or vice versa has been completed, the connection is automatically cut if this check box is activated. If this function is not activated, the RDT connection is maintained.

  - Ignore "command not executed".

- Preferences - Preferences for file management
  This menu provides the option of specifying a certain directory for the program files to be stored (usually a directory on the hard disk of the local computer / laptop). A directory can also be entered for the backup files of the program files (e.g., a directory of the backup server in the network). The button "Start synchronization" is used to save the files in this backup directory.

- Autosave
  Specification of an interval (in minutes), in which the currently loaded program will be automatically saved as a backup. If the "Create backup" check box is not checked, no backup files are created.

- Synchronization
  If the check box is checked and the "Start synchronization" button is clicked on, then the oldest file date is overwritten with the newest file. The direction of synchronization can be influenced by activating different check boxes.

4.3.4.3 Show Info window
This command is used for showing/hiding the information window.

4.3.4.4 Show all customers
With this command, the display of the available system programmings can be limited to <u>a single</u> customer. If this option is activated, all customers stored within the database are shown in the configuration window/tree. If the option is deactivated, only the last customer selected will be shown in the configuration window/tree.

4.3.4.5 Grid
With this command, a chart grid can be shown/hidden in the components/status window.

4.3.5 The "Help" drop-down menu

4.3.6.1 The "Info" command
The WINFEM Advanced version, the driver versions and information about the working memory are displayed in the Information window.

4.4 Components/status window

The individual components/parameters of the "component group" or "object group" selected in the configuration field are shown in the components/status window.
When an individual component has been selected with the left mouse button, the corresponding context menu is opened with the right mouse button. Information about individual customers, objects and systems within the system database are also shown here.

4.5 Information window

The corresponding parameters for the object selected (configuration window or components/status window) are displayed here.

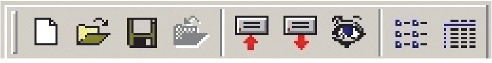
4.6 WINFEM Advanced status line

Shows the current settings of WINFEM Advanced as well as the current programming status (e.g. programming changed but not yet saved).

4.7 Configuration window

The basic hardware/software structure of the system/device are shown in the configuration window. The customers, objects and systems within the systems database are also displayed here. If a programming set-up has already been loaded for a particular system, the name/date of the programming set-up is indicated.

4.8 Toolbar



New
A new program file with the standard parameters is created.

Open file
Command "Open file" loads a file that is stored (hard disk, floppy disk, network) into WINFEM Advanced for further processing.
When "Open file" is selected within the programming process for a system/device, you will be asked whether the programming is to be saved.

Save file
Saves the current programming. The file name may comprise 256 characters max. File type ".prg" is added automatically by WINFEM Advanced.

Close
The ongoing programming is closed, but WINFEM Advanced remains open.

Transfer parameterization data "Panel -> PC"
The current configuration data of the system/device are loaded into the PC for verification or processing.

Transfer parameterization data "PC -> system"
The current configuration data of WINFEM are transferred from the PC to the system/device.

Events
By means of this button, you can open the "Events memory " submenu. See Section 5.3 Events Memory.

Details
Depending on the selection on the configuration window, all defined details, e.g. the BUS users with the corresponding parameters, are shown in the components/status window.

List
A short summary, e.g. of the BUS users or the detector groups is shown in the components/status window.

4.9 Using the mouse

Left mouse button: In WINFEM Advanced, the left mouse button is generally used for selecting or highlighting a component.

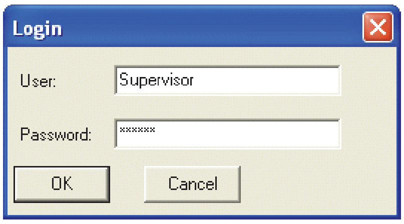
Right mouse button: When an individual component has been selected with the left mouse button, the corresponding context menu is opened with the right mouse button.

5. Programming with WINFEM Advanced

5.1 Basic parameters for customers, object and system

When WINFEM Advanced is started for the first time after a new installation, a message will be output that there is no database available. It is now possible to import existing system databases directly into WINFEM Advanced. When you confirm with "Yes", a window will open where you can select the database directory. Once the desired directory has been selected and confirmed with OK, the user login starts.
A database import can also be carried out at a later point of time with command "File → Load from database". See Section 4.3.1.4.

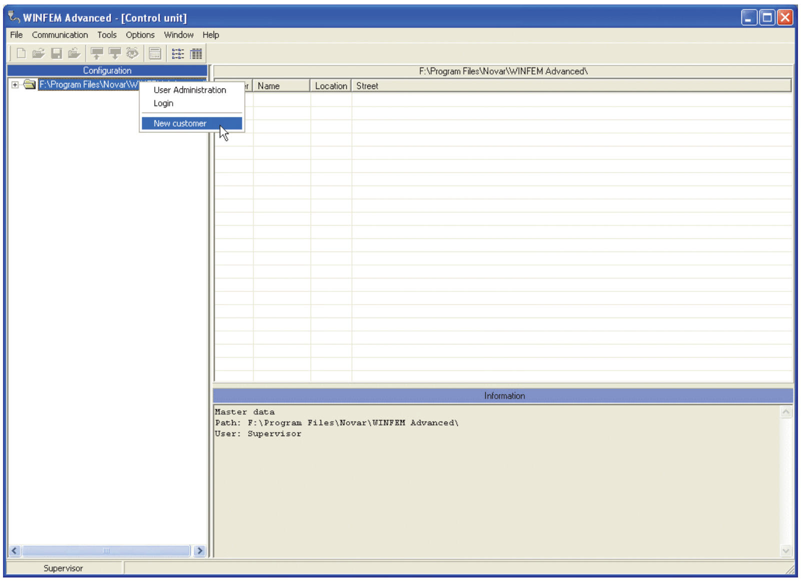
WINFEM can only be operated after a valid user name and the corresponding password have been entered. The default setting is one user: "**Supervisor**". For this user, the password "**winfem**" is set in the factory.



User: Supervisor

Password: ******

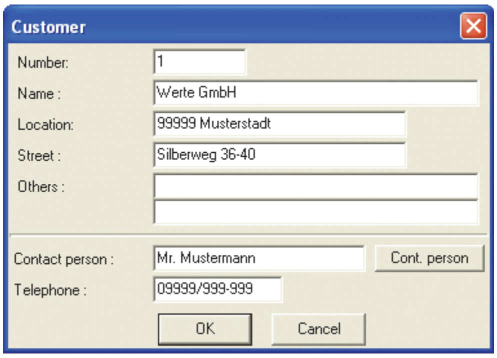
When a valid password has been entered, the actual WINFEM Advanced screen is displayed.
In the configuration window, the installation drive and the installation path of WINFEM Advanced are shown.


WINFEM Advanced - [Control unit]
File Communication Tools Options Window Help
Configuration
F:\Program Files\Novar\W
User Administration
Login
New customer
F:\Program Files\Novar\WINFEM Advanced\
Name
Location
Street
Information
Supervisor

```
Master data
Path: F:\Program Files\Novar\WINFEM Advanced\
User: Supervisor
```

If customers have already been defined, the database path can be opened further with a click on the "+"-symbol beside the folder icon.

For defining a new customer, select the "WINFEM" installation path with the left mouse button and then open the context menu with the right mouse button.

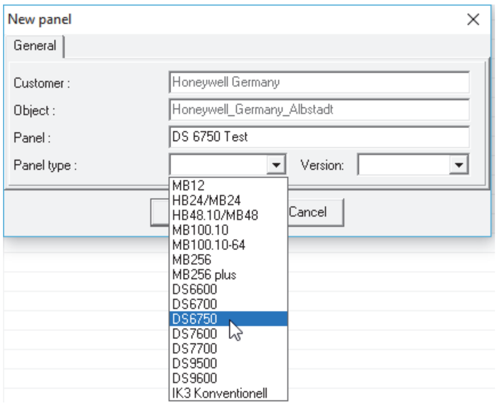


Number:	1
Name :	Werte GmbH
Location:	99999 Musterstadt
Street :	Silberweg 36-40
Others :	
Contact person :	Mr. Mustermann
Telephone :	09999/999-999

When a customer is defined, the parameters (Customer) Number and (Customer) Name are **mandatory** entry fields. The entry of the other parameters is optional.
The contact person is entered in a separate list field, which can be opened via the "Cont. person" button.

When all customer-specific data have been entered and the customer definition window has been closed, you can further open the database path by clicking on the "+"-symbol beside the folder icon. The new customer name is now displayed.
The next step is to define an object. Objects are defined in the same way as customers. When the entry of object data has been completed, proceed with the system definition.

The WINFEM Advanced programming software permits the programming of different control panel or device types. In the framework of the different device programming processes, the menu items within WINFEM Advanced are adjusted to the specific requirements of the device to be programmed. That means that only the menu items which are possible or necessary with the device type selected are shown in WINFEM Advanced.
For this reason, a selection window opens first when menu item "New system" is selected, where the relevant device type and the software version must be selected. A "name" for the system must also be specified here.



New panel

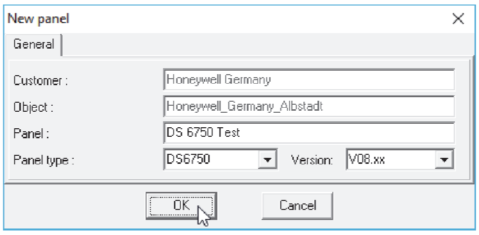
General

Customer : Honeywell Germany

Object : Honeywell_Germany_Albstadt

Panel : DS 6750 Test

Panel type : Version:



New panel

General

Customer : Honeywell Germany

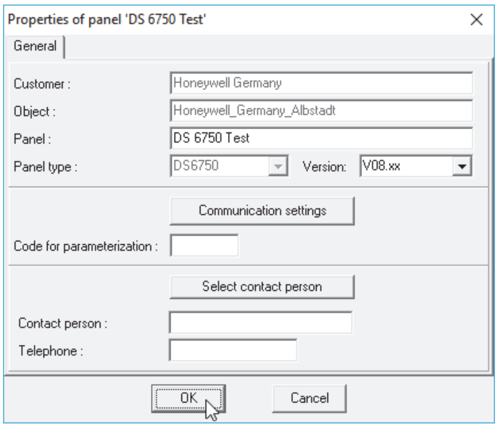
Object : Honeywell_Germany_Albstadt

Panel : DS 6750 Test

Panel type : DS6750 Version: V08.xx

When the device type and the software version have been selected and the system name has been entered, exit the entry window with by clicking on "OK". The "new" system is now displayed in the configuration tree.

Now select the system in the configuration tree with the left mouse button and open the context menu with the right mouse button. Then click on menu item "Properties".
The window for entering the system-relevant basic parameters opens now.



Properties of panel 'DS 6750 Test'

General

Customer : Honeywell Germany

Object : Honeywell_Germany_Albstadt

Panel : DS 6750 Test

Panel type : DS6750 Version: V08.xx

Code for parameterization :

Contact person :

Telephone :

System: In this field, the system name entered in the "New system" window is shown. If necessary, the name can be changed here.

System type: The device type is displayed for information only.

Version: You can select the software version of the system to be programmed directly by clicking it in the drop-down list field.

Communication settings:

This button is used for opening the menu for setting the communication data of the system.

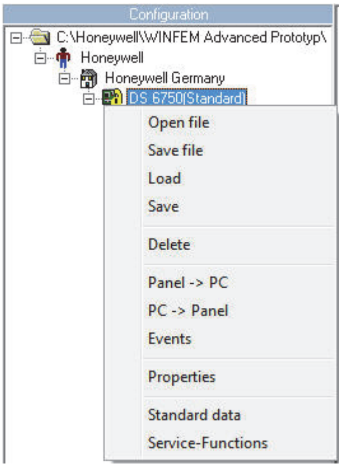
Code for remote parameterization:

This code has to be entered for transmission device programming if stored in the transmission device. This code can be imprinted on the transmission device during programming using the "Service functions" context menu (see Section 20.1.1).
When connecting the transmission device to hazard detection systems via the V.24 interface of the hazard detection system and the serial S1 (RS-232) of the transmission device (transmission device as an integration module in the IACP RS-232 mode), the same code is to be stored for the control panel and the transmission device if possible in order to be able to fully complete programming.

When a connection between PC and control panel is being established, this code is checked. If a difference is found during the verification of the code by the control panel, the connection to the PC will be interrupted.

5.2 "System" context menu

Open the tree structure by clicking the "+"-symbol, as already described above. Select the required system with the left mouse button and then open the context menu with the right mouse button.



- Open file With "Open file", a system programming can be loaded directly from a file. This function is used e.g. when a programming archived on another data medium is required again.

- Save file Save a system programming as a file on a data medium (e.g. for archiving).

- Load This menu item is used for loading data from the internal database for processing. A distinction is made between
  * Standard data and
  * System specific data.

The standard data correspond to the programming data which are defined during standard programming of the device.
In case of system-specific programming, these data are modified in such a way that they correspond to the actual system configuration. So system data are programming data which have already been created and saved manually. The name of the programming data currently loaded is shown next to the system name.

- Save Saves programming data in the integrated database.

- Delete This command is used to delete the currently selected system from the system database.

- Panel → PC* Transfer the system programming and configuration from the system to the PC.

- PC → Panel* Transfer system programming from the PC to the system.

- Events Clicking on "Events" displays the sub-menu "AWUG events".
  Further information on this submenu, see Section5.3.

- Properties The Properties window of the system is opened using this menu item.

- Standard data With this command, you can reset selective areas of the currently loaded programming back to the the factory default programming. (Examples are the VdS 2465 fault report or the programming of the smartphone app).

- Service-Functions * The menu item opens the dialog box for setting the date and time, the dialog box for the debug mode, recording of AWUG texts and the dialog box for collecting keys for encrypted data transmission. For further information on this submenu, see Section 20.

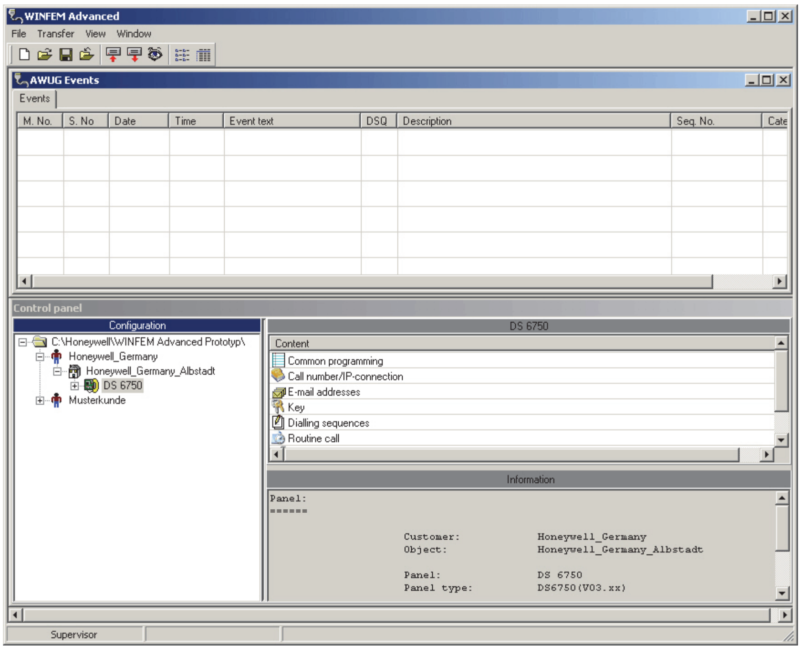
ℹ The processes marked with "*"require a direct connection from the system to the PC/laptop.
The connection type must be defined in menu item "Communication/Settings/Connection".

5.3 Event memory

The event memory is located in the flash memory of the transmission device, which also stores the firmware and the programmed parameters of the device.
It has a storage capacity for at least 1000 events and up to 2000 events. The events are subdivided into main events and secondary events.
A secondary event is an activity initiated by the occurrence of a main event.

Example:
Main event: Activation detector group —> resulting secondary event: user x reached.

Command "Events" is available in the context menu of the system. With this command, the "Events" submenu is opened. The menu for the event memory can also be opened by a direct click on the "eye" icon in the toolbar.

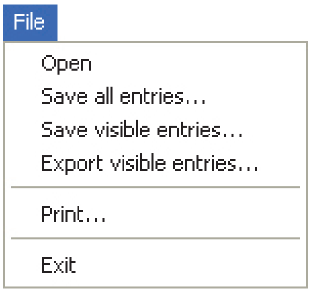


```
Panel:
======

                    Customer:          Honeywell_Germany
                    Object:            Honeywell_Germany_Albstadt

                    Panel:             DS 6750
                    Panel type:        DS6750(V03.xx)
```

5.3.1 The "File" pull-down menu



5.3.1.1 The "Open" command
With this command, you can load a saved event log into the event window for viewing.

5.3.1.2 The "Save all entries" command
The loaded event memory data of a system can be saved in a log file for archiving.

5.3.1.3 The "Save visible entries" command
The event memory data of a system that have been loaded and filtered can be saved in a log file for archiving.

5.3.1.4 The "Export visible entries" command
The event memory data of a system that have been loaded and filtered can be exported into a log file in csv file format.

5.3.1.5 The "Print" command
When this command is selected, the print parameter selection window opens. Here you can define which printer is used as well as the font size and the number of copies.

5.3.2 The "Transfer" pull-down menu

5.3.2.1 The "Whole event memory" command

This command is used for loading the event memory of the system selected into the PC/laptop.

When this command is activated, the selection window for selecting the communication connection type opens first. If the connection type has already been defined, the loading process of the event memory will start immediately.

For setting the connection type, see section "4.3.3.5 Communication - Settings".

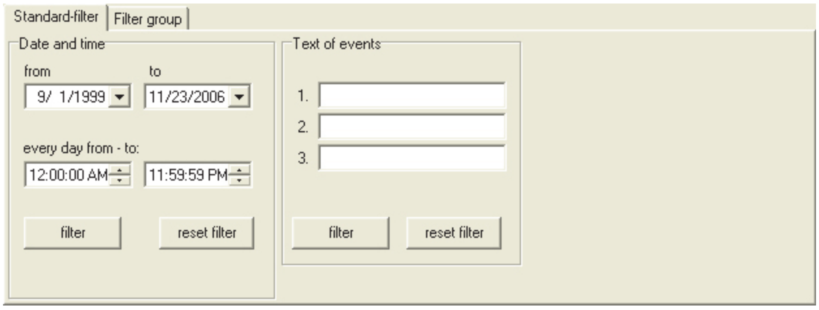
5.3.3 The "View" pull-down menu

5.3.3.1 The "Show all events" command

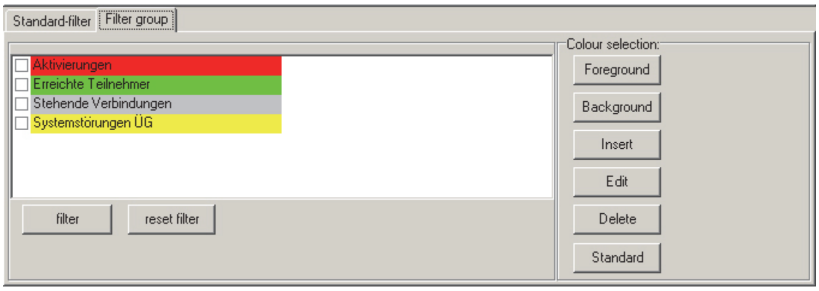
Any filters that might have been set are reset by this command and all system events are displayed in the event window.

5.3.3.2 The "Filter" command

This command activates the display of the filter options. The filters permit the selection of individual event groups for viewing. So it is e.g. possible to display only alarms or the events within a certain period of time.



from: 9/ 1/1999
to: 11/23/2006
every day from - to: 12:00:00 AM 11:59:59 PM
1.
2.
3.



□ Aktivierungen
□ Erreichte Teilnehmer
□ Stehende Verbindungen
□ Systemstörungen ÜG

The “Standard filter” tab includes the filter for date and time as well as the filter for making a selection by the text of events. The desired filter function is set by entering the relevant values.

The filter process is then started with the "filter" button. The desired results are displayed in the event window.

You can use the color selection buttons "Foreground" and "Background" to differentiate the events displayed by different colors.

Tab “Filter category” provides the possibility to select own filters (depending on the possibilities of the individual system/device) by activation of the relevant check box(es).

When you click on the "Insert" button, the selection window for setting a group filter opens. With the “Delete” button, group filters that have been selected can be deleted. Start the filter process for the events with the “Filter” button. The desired results are displayed in the event window.

- Name

  Short designation of the category filter

- Description

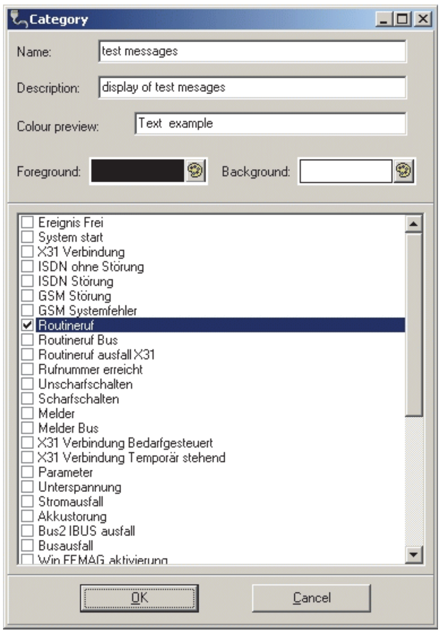
  The category filter can be described/documented here

- Color preview

  Text example for the display of events. The color selection for the foreground color (font) is made via the drop-down list field Foreground, the background color is selected via the drop-down list field Background.

- Category selection window

  Shows all possible categories for the individual device/system. By clicking the relevant check box, you include the category into the filter. It is possible to select several categories within one category filter defined.


Category

Name: test messages

Description: display of test mesages

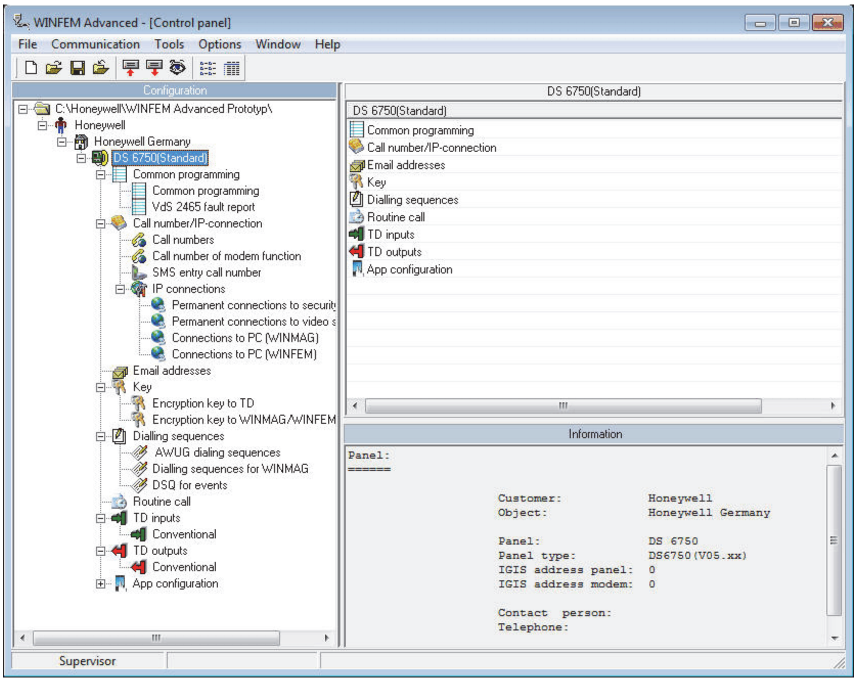
Colour preview: Text example

Foreground: ■ Background: □

- □ Ereignis Frei
- □ System start
- □ X31 Verbindung
- □ ISDN ohne Störung
- □ ISDN Störung
- □ GSM Störung
- □ GSM Systemfehler
- ☑ Routineruf
- □ Routineruf Bus
- □ Routineruf ausfall X31
- □ Rufnummer erreicht
- □ Unscharfschalten
- □ Scharfschalten
- □ Melder
- □ Melder Bus
- □ X31 Verbindung Bedarfgesteuert
- □ X31 Verbindung Temporär stehend
- □ Parameter
- □ Unterspannung
- □ Stromausfall
- □ Akkustorung
- □ Bus2 IBUS ausfall
- □ Busausfall
- □ Win FEMAG aktivierung

6. Programming the system parameters

In the "Configuration“ window, a tree diagram containing the individual parameter groups opens when you click on the [+]-symbol in front of the object "transmission device".



```
C:\Honeywell\WINFEM Advanced Prototyp\
  Honeywell
    Honeywell Germany
      DS 6750(Standard)
        Common programming
          Common programming
          VdS 2465 fault report
        Call number/IP-connection
          Call numbers
          Call number of modem function
          SMS entry call number
          IP connections
            Permanent connections to securit
            Permanent connections to video s
            Connections to PC (WINMAG)
            Connections to PC (WINFEM)
        Email addresses
        Key
          Encryption key to TD
          Encryption key to WINMAG/WINFEM
        Dialling sequences
          AWUG dialing sequences
          Dialling sequences for WINMAG
          DSQ for events
        Routine call
        TD inputs
          Conventional
        TD outputs
          Conventional
        App configuration
```

DS 6750(Standard)

- Common programming
- Call number/IP-connection
- Email addresses
- Key
- Dialling sequences
- Routine call
- TD inputs
- TD outputs
- App configuration

```
Panel:
======

                        Customer:           Honeywell
                        Object:             Honeywell Germany

                        Panel:              DS 6750
                        Panel type:         DS6750(V05.xx)
                        IGIS address panel: 0
                        IGIS address modem: 0

                        Contact  person:
                        Telephone:
```

There are the following groups:

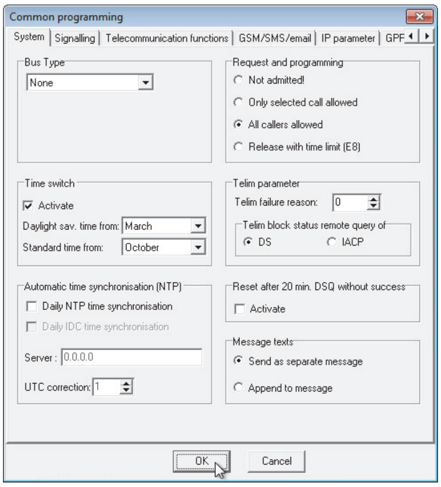
- Common programming
- Call numbers / IP connections
- E-mail addresses
- Keys
- Dialing sequences
- Routine call
- TD inputs
- TD outputs
- BUS-2 (only for BUS-2 master programming)
- App programming (Communication with the smartphone app)

Some parameter groups are subdivided into further subgroups; when you click on the [+]-symbols assigned to these groups, the individual structures are displayed.
Double clicking on the individual group or subgroup opens a corresponding configuration menu or displays the individual parameters in the components/status window. A double-click on the individual parameters in the components/status window opens the corresponding configuration menu.

6.1 System tab

6.1.1 Bus type

The transmission device is equipped with a serial interface which supports different operating modes. The physical connection point is determined by the interface type selected (e.g. I-BUS, BUS-2).



Bus Type: None

Request and programming
○ Not admitted!
○ Only selected call allowed
● All callers allowed
○ Release with time limit (E8)

Time switch
☑ Activate
Daylight sav. time from: March
Standard time from: October

Telim parameter
Telim failure reason: 0
Telim block status remote query of
● DS ○ IACP

Automatic time synchronisation (NTP)
□ Daily NTP time synchronisation
□ Daily IDC time synchronisation
Server : 0.0.0.0
UTC correction: 1

Reset after 20 min. DSQ without success
□ Activate

Message texts
● Send as separate message
○ Append to message

The BUS type can only be changed if the transmission device has been defined as an "independent system" (see also Section 5.1 and Section 5.2).

Standard factory setting for the operating type: IACP RS-232.

6.1.1.1 None
If the serial interface is not used, "none" must be set here.
If anything else is selected although the serial interface is not used, a fault is indicated on the transmission device and, where appropriate, a fault message
is sent (transmitted) to the target call numbers stored.

6.1.1.2 I-BUS
Programming for use of the device as I-BUS user (e.g. IACP 561MB-256).

Please observe the following points when commissioning the device:
When the transmission device is integrated into the I-BUS, the device address is assigned automatically after a reset has been initiated on the intruder alarm control panel. The individual I-Bus users are informed about the Bus addresses one after the other.
For this purpose, the bus users are first set to a defined initial state (address allocation) via a RESET signal by the communication master (intruder alarm control panel).
If now one of the bus users is set to the address allocation mode, e.g. caused by a watchdog reset or something similar, this might result in conflict or even fault situations which might impair the function of the I-BUS system.

Therefore, the following procedure must be complied with when commissioning the device and the I-BUS address must be safely stored:

1. - For initial commissioning, jumper J1 is to be connected (I-BUS learn mode).
2. - Carry out commissioning and parameterization of the intruder alarm control panel.
   The device address assigned during the I-Bus initialization is adopted by the transmission device.
3. - When the parameterization is completed, remove jumper J1 again.
   The I-BUS address is stored.

If the I-BUS learn mode has not been completed correctly and jumper J1 is removed prematurely, the interface of the transmission device is automatically changed to BUS-2.

When jumper J1 is connected, the LED indicator "Fault" is activated statically.
If the I-BUS configuration is to be changed, e.g. when an extension of the intruder alarm system is made, the I-Bus address can be newly parameterized by activating the I-BUS learn mode (connect jumper J1).

- Telephone number extension of conventional systems (extended compatibility mode only DS 6750)
  see 6.1.1.4.

6.1.1.3 Fire I/O-BUS

For integration in the fire detection computer 1024-F this connection is used. Use the I-BUS adapter board (item no. 070780.02) to integrate the DS 6700 / DS 6750 (in compatibility mode!) directly as I-BUS member to FDC 1024-F. Wiring and electrical connection of the DS 6700 / DS 6750 is carried out as with FDC 1024-F. In addition, the IO-BUS address has to be programmed. For more information, please see the FDC 1024-F installation manual.

- Telephone number extension of conventional systems (extended compatibility mode only DS 6750)
  see 6.1.1.4.

6.1.1.4 BUS-2

For use in intruder alarm control panels where the integration of the transmission device is made via BUS-2, the BUS address must be set according to the configuration of the control panel

- Telephone number extension of conventional systems (extended compatibility mode only DS 6750)
  If this check box is checked, MB control panels connected via BUS 2 and I-BUS can transmit alarms via IP connections. Email and AWAG functionalities can also be used. This functionality is implemented using a conversion table in the transmission device DS 6750. Refer to the section 18 for information on programming and the conversion table

6.1.1.5 VdS S1 operating mode

This operating mode of the serial interface (RS232 connection) differs fundamentally from the IPC RS-232 operating mode (Section 6.1.1.8)! The connection of the S1 Interface is used here to connect to hazard detection systems, which are also equipped with a VdS S1 interface in accordance with VdS 2463 and VdS 2465. According to the guidelines, this interface is designed as RS232. When using this operating mode no addressing allocation is performed, but the number of connected users ("slaves") has to be set. Background: When using the serial interface according to VdS, the transmission device basically assumes the role of the communications master. The connected hazard detection system is assigned the "slave" function. Up to 4 hazard detection systems can be operated on serial S1. Therefore the number of "slaves" has to be communicated to the transmission device.

If multiple hazard detection systems have to be connected via the serial S1, an additional RS232 hub is required. The direct connection of multiple hazard detection systems to a transmission device is not allowed.

6.1.1.6 BUS-2 Master

In "stand alone" mode, i.e. the transmission device is not connected via I-BUS, BUS-2 or serial S1 to a hazard detection system, the BUS-2 interface can also be operated in master mode. The interface is then used for the connection of BUS-2 components.

BUS 2 user	Item no.	Max.
5 input module	1313010	16 units total
5 output module	1313110	

Thus the number of activation criteria of the transmission device can be increased from 8 inputs to up to 88 inputs. Mixed use (e.g. 9 input modules and 7 output modules) is possible. For example, up to 40 additional inputs (8 x 5 input modules) and 40 additional outputs (8 x 5 output modules) can be implemented.

6.1.1.7 GPS mouse

For "stand alone" use of the transmission device when the BUS-2 Master mode is not used, a GPS wireless mouse can be connected to the S1 interface (RS232).
It is therefore also possible to use the system in mobile security systems (cash transport, truck container transport, construction vehicles, etc.)

The transmission of messages and the GPS coordinates of mobile systems, can be carried out via GSM networks in conjunction with the redundant radio path (RFW-4000 / RFW-3000). Transmission via PSTN or IP networks is also possible.

Follow the instructions in the installation instructions for connecting the GPS mouse to the transmission device.

Requirements for the GPS mouse:

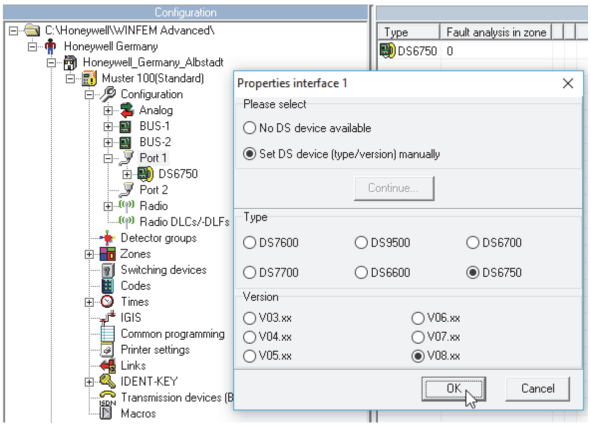
Interface/design:	Serial 9-pin Sub-D
Pin assignment:	acc. V.24
Used interface lines:	TXD, RXD, GND
Physical properties:	acc. V.28
Protocol:	NMEA-0183 Standard (National Marine Electronics Association)

GGA strings are evaluated and transmitted. (GP GGA strings contain all the necessary information on position and accuracy).

6.1.1.8 IACP RS-232 Modus

This mode permits the connection of control panels providing an RS-232 interface with VdS protocol 2465. The connection control panel - transmission device is made via the 9-pole connection cable supplied with the transmission device (see DS 6700 / DS 6750 installation instructions).

The interface must be set accordingly in the configuration menu of the control panel (in the example: 561-MB100 with art.-no. Index .10)
To this end, select menu item "Serial port“ in the configuration window and press the right mouse button. Now the button "Properties" is shown. When you click this button with the left mouse button, the menu "Serial port settings" opens.
Double clicking on menu item “Serial Port” in the configuration window opens the corresponding configuration menu.
The control panel recognizes the transmission device that is connected via an automatic adaptation mechanism.



Properties interface 1

Please select

○ No DS device available
● Set DS device (type/version) manually

Continue...

Type

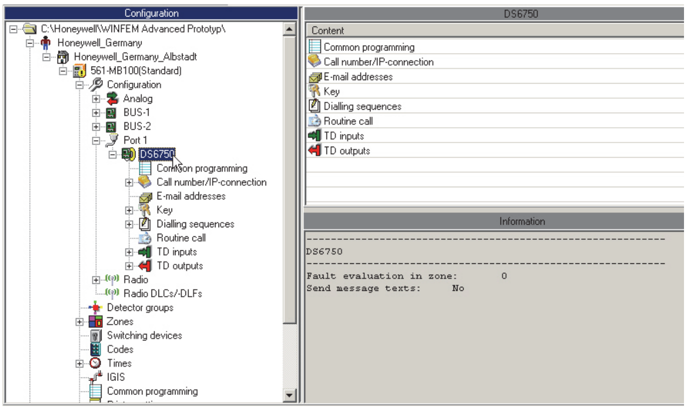
○ DS7600 ○ DS9500 ○ DS6700
○ DS7700 ○ DS6600 ● DS6750

Version

○ V03.xx ○ V06.xx
○ V04.xx ○ V07.xx
○ V05.xx ● V08.xx

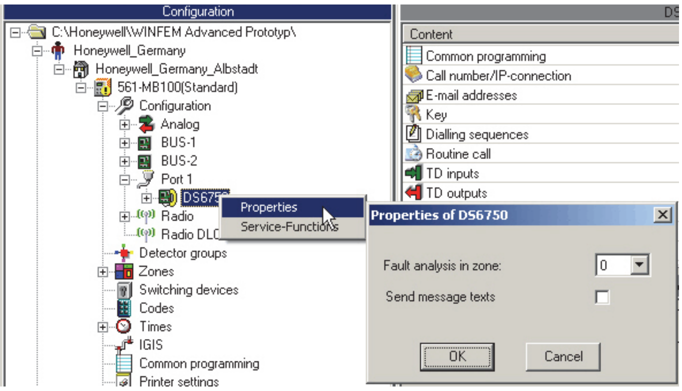
OK Cancel

This configuration can be used to program the entire hazard detection system including the release criterion for the transmission device via the programming device connection of the transmission device. The rest of the programming for conventional detector group inputs (E1- E8) of the transmission device is carried out as for “stand-alone” configuration.



```
-------------------------------------------------------
DS6750
-------------------------------------------------------
Fault evaluation in zone:       0
Send message texts:     No
```

For further programming, the main zone must be defined to which the transmission device is assigned for fault analysis, i.e. in which zone an alarm is triggered when there is a failure of the serial connection (control panel - transmission device).
For this purpose, select object "DS 6700” or “DS 6750" in the configuration window and press the right mouse button. Use the left mouse button in the context menu to open the "Properties" menu.



Properties of DS6750

Fault analysis in zone: 0

Send message texts □

OK Cancel

The main zone for fault analysis is specified via the drop-down list field.

If the range entry is set to "0 = none", no fault evaluation is carried out.

- Send message texts (only possible with VdS 2465 protocol and e-mail)

  If the check box is activated, the message texts of the control panel are transmitted to the transmission device. This message text consists of up to 80 characters made up of zone text, user text (e.g. operating unit IK3), name (e.g. ID data medium). By means of this assignment and programming, you can e.g. implement documentation and person identification for arming/disarming operations for the alarm receiving facility.

6.1.2 Time switch/synchronization

The transmission device is equipped with a clock component, which has a 48 hour power reserve. The following options are available for setting date and time:

- Set using WINFEM Advanced when sending programming.
- When used as an integration module in the hazard detection control panel and connection via I-BUS, BUS-2 or IO-bus, the clock is set using the hazard detection system's operating units.

Relevant only for transmission device DS 6750: Automatic time synchronization via NTP.
For testing purposes, the command "time s" can be used in diagnostic mode (see Section 22) to send a time request to the NTP server.

The current universal time (UTC = Coordinated Universal Time) can be requested from an NTP server. NTP (Network Time Protocol) is used to synchronize clocks, which are interconnected via packet-based communication networks.

The IP address of NTP server must be entered as a numerical xxx.xxx.xxx.xxx IP address or domain name. If no NTP servers are available in the local Intranet, the public time servers of the Physikalisch Technische Bundesanstalt (www.ptb.de), free pool of NTP servers or various universities can be used.
Furthermore, the deviation of the UTC time from local time is to be entered.
The following correction applies to Germany:

Winter time (Standard time)	UTC+1	(CET Central European time without daylight saving time correction)
Daylight saving time	UTC+2	(CEST Central European Summer Time)

For Germany, the UTC value “CET without daylight saving time correction” is to be entered (UTC+1).

6.1.2.1 Time of synchronization

- Daily NTP time synchronization (only DS 6750).

  In the case of a dedicated GPRS or Ethernet IP connection, the clock is synchronized daily at 3:30 a.m. After startup/reset of the DS 6750, a connection is established with the NTP server and the time is transferred.
  If the connection is a demand-actuated connection, the time is queried from the NTP server starting at 3:30 a.m. with the following regular transmission (message or routine call) when the next PPP PSTN, GPRS or Ethernet IP connection is established. The time is only corrected in the transmission device if the difference between time on the device and the determined time is greater than 30 sec.

- Daily IACP time synchronization (only DS 6750).

  "Daily IACP time synchronization" can be enabled for transmission devices which are installed as an integration module in IACP and connected via the "IAPC RS232" interface. The time is passed on to the IACP once a day at 4 a.m.
  Note: A daily event memory entry is made on a daily basis in the IACP event memory.

6.1.3 Automatic switching to daylight saving time

The automatic time change can also be deactivated for stand alone use of the device or when connecting the hazard detection system via serial S1. This can be necessary in the event that a control center works with GMT. The change to daylight saving time is made on the last Sunday in March in Germany. The clock is advanced by one hour between 2:00 and 3:00 h. The clock is changed to winter time (Standard time) on the last Sunday in October. The clock is set back by one hour at 3:00 h. It is possible to shift the times for changing between daylight saving time and winter time and between winter and daylight saving time.

In the factory setting, the daylight saving time / winter time change is activated,
change to daylight saving time as of March, change to winter time as of October.

6.1.4 Interrogation and programming

The configuration of the transmission device can be carried out

- locally, via the USB port or
- remotely via PSTN or
- via Ethernet (TCP/IP).

The transmission device allows remote maintenance and remote parameterization of compatible hazard detection panels to be implemented via PSTN or Ethernet. For a PSTN connection, an analog modem is required on the PC side in addition to the WINFEM Advanced software (see also Section 4.3.2) and the transmission speed is 14400 Baud max.

Note for remote parameterization: If a remote access to the device uses wrong ID numbers and passwords, after the 3rd failed attempt, a disable of the remote service function will be put in place for a period of 30 minutes.
For factory-delivered devices, remote parameterization is possible via the analog telephone network (commissioning). Please note that in this case the identification number used must be 10 times 0 (“0000000000”) and the password 8 times 0 (“000000”). For remote access, the following configuration options are possible:

- Not admitted
Remote access is not possible at any time

- For all callers
In this programming, each call is accepted by the transmission device. The appertaining ID number and the password are used for identification. If no call number is displayed on the landline connection of the transmission device (clip function not active or caller does not send the call number), the caller will only be identified on the basis of the password and the ID number.

This setting does not meet the VdS guidelines.

- For selected call number
If this setting is made, calls are only received from parties for which the number is stored in the "Modem functions call numbers" programming. Calls from other users (subscribers), or calls from users which have suppressed their Caller ID will not be accepted.

The password used by the calling WINFEM Advanced and the identification number must match the password and identification number, which was assigned to the respective number.

- Temporary release (E8)
It is possible allow remote access on a case-by-case basis. The "temporary release (E8)" function is to be activated for this purpose.
In this case, time limited release for the remote service function can be performed by activating detector group 8 (e8). A key switch or release button is connected or an output signal can be connected from an HAS to the detector group input (e8) of the transmission device for this purpose.

Occasional release is limited to a period of about 60 minutes. No number check is carried out. Important! The password used by the calling WINFEM and the identification number must however match the password and identification number, which was assigned to number 1 in the "modem functions number".

6.1.5 Reset after 20 min. DSQ without success

Enabled check box activates an automatic reset of the transmission device under the condition that a DSQ could not successfully be handled. This function takes place after 20 minutes. The activation of this function returned the transmission device in a defined state if a transmission path is disturbed and the DSQ was not completed after 20 minutes. Note that in such cases after the reset a fail message and re-registration transmitted to the control center and there will be a corresponding event memory entry.

6.1.6 Telim failure reason

Entry of the channel for the transmission of system failures in the Telim protocol. The following events activate a transmission on this channel: Telephone line fault/o.k, undervoltage detected/ok, 230 V failure/ok.

6.1.7 Telim block status remote query of

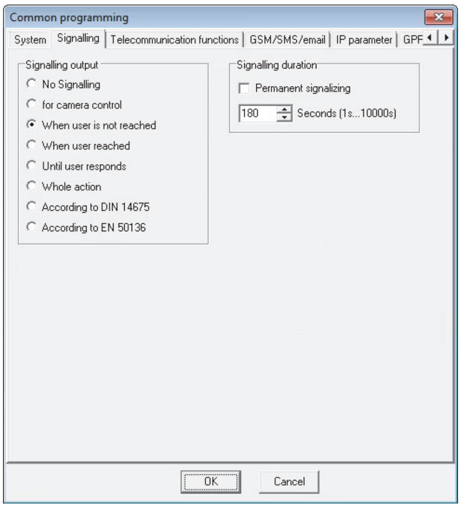
Selection, whether the state of the Telim block (Telim block status of the 8 inputs) is transmitted from the transmission device or from the panel coupled by RS-232 interface (only Telim Protocol).

6.1.8 Message texts

The ASCII clear texts within the VdS2465 protocol are transmitted as separate messages or attached directly to the message. This setting depends on the receiving control unit of the alarm receiving center and must be made known by provider of the alarm receiving center.

6.2 Signaling tab

6.2.1 Configuration of the signaling output



Signalling output
○ No Signalling
○ for camera control
● When user is not reached
○ When user reached
○ Until user responds
○ Whole action
○ According to DIN 14675
○ According to EN 50136

Signalling duration
□ Permanent signalizing
180 Seconds (1s...10000s)

The signaling output of the transmission device consists of a potential-free, programmable relay contact (change-over contact). This relay contact is used in conventional actuation of the transmission device via the parallel S1 to communicate confirmation of successful or failed transmission of a hazard report to a hazard detection system. Thus activation of local alarm signaling can be made dependent on the success or failure of "silent alarm signaling" (see VdS 2311).

Programming of the signal output refers only to the relay contact "signaling" of the transmission device. The output is activated only if "Signal DG" has been activated in detector group programming. The activation time is calculated either from the selected function (e.g. until user reached) or it can be set as a time-related or continuous signal.

When programming as a continuous signal, the signaling output is actuated until another relevant activation criterion occurs or the transmission device is "disarmed" and "armed" again via the arm/disarm input.

The following activation options are available for programming the signal output:

- No signaling
  no function

- For camera control
  The output is actuated if an activation criterion of the detector groups occurs, in which the check box "signal DG" has been checked. (programmable time period for a time signal (from 1-10000 seconds) and a continuous signal. From the application perspective, programming as a continuous signal does not make sense here.

When using the transmission device as a hold-up alarm system, this programming of the signaling output can be used to actuate and activate the camera or the recording system. Activation of these components must be selective, i.e. by individual detector groups (hold-up detector groups).

- If user not reached
  The signal output is activated if no user (subscriber) can be reached if the activation criteria relevant to this function occur. The signaling output can be actuated as a temporary signal (1-10000 sec) or a continuous signal. Actuation is carried out if the message is not issued by 120 sec. after the onset of the activation criterion at the latest and acknowledge by the receiving device (control center).

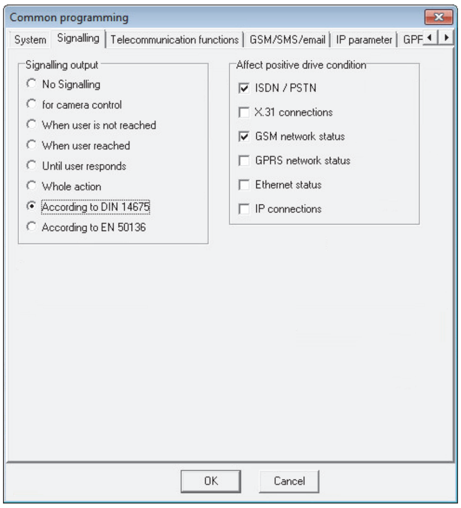
- If user reached
  Output is activated if a user (subscriber) has received the alarm or fault signal. The signaling output can be actuated as a temporary signal (1-10000 sec) or a continuous signal.

- Until user reached
  The signaling output is activated when the activation criterion occurs and remains active until the message is successfully sent to the first user reached.

- Overall action
  The signaling output remains switched on throughout the entire activation phase of the transmission device. The output is actuated in this case on occurrence of the activation criterion and ends once the dialing sequence has been processed.

- According to DIN 14675
  This programming is required when using the fire alarm system connection pcb for transmission devices to extend the DS 6700 and DS 6750 transmission devices. This is for use in fire alarm systems according to EN 54-21. The fire alarm system connection pcb is a fire alarm interface according to DIN 14675, Annex B, and VdS 2463 and allows for the transmission of fire and trouble alarms from fire alarm systems.
  The signaling output is switched on when a user is reached and remains active until the activation criterion is returned to its projected state.

  This dialog allows the selection of faults that affect the positive drive condition (relay output positive drive on pcb). A non-existent positive drive condition will be displayed at the fire detection control unit as a fault in the transmission unit (UEE fault). Parameters must be set based on the connection and network access selected. Factory settings are: ISDN/PSTN fixed network (= fault in the telephone line connection) and GSM network status (= GSM fault).



Signalling output
○ No Signalling
○ for camera control
○ When user is not reached
○ When user reached
○ Until user responds
○ Whole action
● According to DIN 14675
○ According to EN 50136

Affect positive drive condition
☑ ISDN / PSTN
□ X.31 connections
☑ GSM network status
□ GPRS network status
□ Ethernet status
□ IP connections

For more information on installation and connection, see Mounting and Connection Instructions for the fire alarm system connection pcb (item no. 057655) for transmission devices.

- According to EN 50136

EN This programming is necessary when the transmission unit is used according to European standards (EN) 50136.

Functionality: If one of the "stand alone" inputs 1 to 8 of the transmission unit is activated, a timer will be started with the time parameterized here. The activation of the signal output can be parametrized as a time-limited signal as the maximum transmission time (1-10000 sec.). If the selection sequence is not completed successfully within this parameterized time (message time), the signaling relay is activated for 3 seconds.

The following events are entered and documented in the event memory:

- Fault status ATS 1
- Fault resolved status ATS 1
- Fault status ATS 2
- Fault resolved status ATS 2

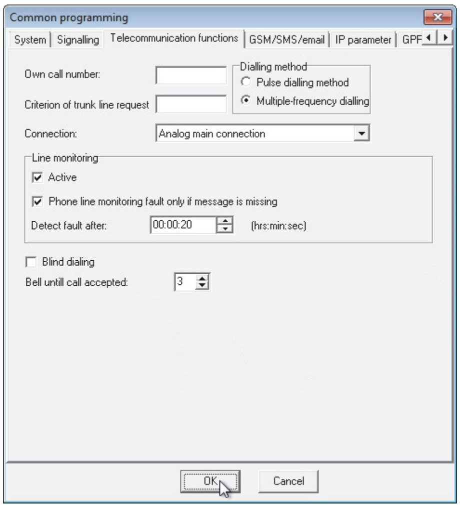
Events are also entered in the event memory when IP connections 1 and 2 or 3 and 4 are faulty or restored. This requires that the events should be entered in the event memory:

- "Dedicated IP connection to the security company" 2 must be parameterized redundantly to 1, while connection 4 must be parametrized redundantly to 3.
- Signaling must be parameterized "according to EN 50136"

6.3 Telecommunications tab

6.3.1 Own call number

Enter own call number.



Own call number:

Criterion of trunk line request

Dialling method
○ Pulse dialling method
● Multiple-frequency dialling

Connection: Analog main connection

Line monitoring
☑ Active
☑ Phone line monitoring fault only if message is missing
Detect fault after: 00:00:20 (hrs:min:sec)

☐ Blind dialing
Bell untill call accepted: 3

The max. length for the entry is 8 digits.

6.3.2 Criterion of trunk line

A trunk line number must be programmed if the transmission device is used within a private branch exchange system (PBX system). Only digits may be entered here.

VdS Using a transmission device within a PBX system does not correspond to the VdS guidelines.

The number stored here is the number that is used when connections are to be established within the PBX system via the public telephone network. The device can call numbers within the PBX system and outside the PBX system (trunk line numbers). The indexing whether a number is a PBX number or a trunk line number is made in the framework of call number programming.

6.3.3 Dialing method

Enter the dialing method used for the transmission device: pulse dialing or multiple-frequency dialing. If possible, multiple frequency dialing should be used to make the dialing process faster.

6.3.4 Connection

If the transmission device is used directly at an analogue trunk line connection, "analogue main connection" must be programmed. When the device is used within a PBX system, the programming must be made accordingly (analogue PBX extension).

6.3.5 Line monitoring

The line monitoring is activated by means of the check box. When line monitoring is programmed, the transmission device, at regular intervals, carries out a check for the no-load voltage of the telephone line. If the minimum requirements are no longer fulfilled, the LED "RDT fault" lights up and the hazard detection control panel receives a message that there is a telephone line fault. A temporal influence on this fault message can be done by entering a time in the input window ➜ **detect fault after**.

VdS In case of older PBX systems or with telephone lines where the no-load voltage is below 20 V, it is recommended to make the programming without line monitoring. Programming in accordance with the VdS-guidelines includes line monitoring.

6.3.5.1 Phone line monitoring fault only if message is missing

A phone line fault does not have to be transmitted necessarily to the emergency call control center if there was no activation of the transmission device during the time of the failure (alarm, fault). But a message about a telephone line failure should be output if an activation criterion relevant for being transmitted occurred during the line failure.

Example 1: The telephone connection is interrupted due to maintenance works carried out in the telephone exchange. During the time of the failure, there is no activation of the transmission device. When the telephone connection works again, the control center does not receive a message.

Example 2: The telephone connection is interrupted and, during the time of the interruption, an alarm is triggered which must be transmitted to the emergency call control center. Since the transmission path is not available and not other transmission path has been connected, the message cannot be transmitted.
When the telephone line fault has been eliminated, the alarm is transmitted to the control center and, in addition, a message about the telephone line fault followed by a subsequent "OK" message is transmitted.
Due to the messages it received one after the other (alarm, fault message, OK message), the emergency call center can clearly track that the alarm message was received with delay because of a telephone line failure.

ℹ The standard factory setting is "phone line monitoring fault only if message is missing”.

If faults are to be reported generally to the control center or to other users, you can remove the tick from the check box. In this case, a transmission (telephone line fault, fault eliminated) always takes place after telephone line fault.

6.3.5.2 Detect fault after

Entering a time here ensures that brief PSTN line faults do not lead to a signal (fault signal) (entry range 20 seconds to 18 hours).
If a time value is entered here (default setting 20 seconds), a fault will only be detected after this time has elapsed. This delay time only applies to the trigger message (the fault is only signaled after the time entered), so that any "good reports" are not delayed. Likewise, an event memory entry is only made after the time entered.

VdS The programming of a delay time greater than 20 seconds is not VdS-compliant.

6.3.6 Blind dialing

It is possible to permit blind dialing (i.e. no dialing tone recognition). In case of blind dialing, the transmission device does not wait for a dialing tone of the telephone network but dials the programmed call number including the trunk line request number, if this has been programmed as well, and transmits the message.

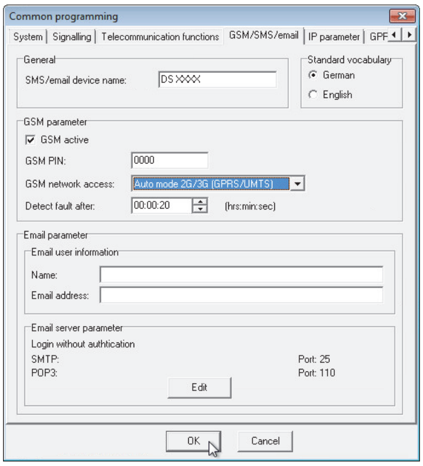
6.3.7 Bell until call accepted

The number of rings until the transmission device receives a call can be specified with this parameter.

6.4 GSM/SMS/e-mail tab

6.4.1 SMS/E-mail device name

Here you can define the text which is to be used as a user ID for SMS or e-mail transmission. Admissible text length: 15 characters. Depending on the position of the radio button in the field "Standard vocabulary" the text transmitted by SMS or e-mail is in English or German.



General
SMS/email device name: DS XXXX

Standard vocabulary
● German
○ English

GSM parameter
☑ GSM active
GSM PIN: 0000
GSM network access: Auto mode 2G/3G (GPRS/UMTS)
Detect fault after: 00:00:20 (hrs:min:sec)

Email parameter
Email user information
Name:
Email address:

Email server parameter
Login without authtication
SMTP: Port: 25
POP3: Port: 110

6.4.1.1 Output format of the transmitted text as SMS

- 1. No SMS/E-mail text has been configured in the transmission device:

[SMS / E-Mail Gerätename]. DS-Kanal: [Kanal] ein ID: [ID-Nummer] [Datum] [Uhrzeit] (Transmission German)
[SMS / E-Mail Gerätename] Dialer-Line: [Kanal] on ID: [ID-Nummer] [Datum] [Uhrzeit] (Transmission English)

[SMS / E-Mail Gerätename]. EMZ-Kanal: [Kanal] ein ID: [ID-Nummer] [Datum] [Uhrzeit] (Transmission German)
[SMS / E-Mail Gerätename] Panel-Line: [Kanal] on ID: [ID-Nummer] [Datum] [Uhrzeit] (Transmission English)

- 2. SMS/E-mail texts configured in the transmission device:

[SMS/E-mail device name]. [SMS / E-mail text] ID: [ID number] [Date] [Time]

6.4.1.2 Output format of the transmitted text as e-mail

When transmitting text as an e-mail via IP networks (PSTN PPP, GPRS PPP or Ethernet) to an appropriate recipient, there are three different ways in which the transmitted text is displayed on the receiver. Sample output of the e-mail:

- 1. SMS/E-mail texts configured in the transmission device:

Transmission German:
SMS/E-Mail Gerätename
Identnummer: XXXXXXXXXXXX
".... 40-stelliger DS Meldertext ..."

Honeywell Security Deutschland
Novar GmbH
Übertragungsgerät: DS6700 / DS6750
Software Version: ADIST.10.0V0x.xx

Transmission English:
SMS/E-Mail Gerätename
ID-Number: XXXXXXXXXXXX
".... 40-stelliger DS Meldertext ..."

Honeywell Security Deutschland
Novar GmbH
Dialer type: DS7700 / DS7600
Software Version: ADIST.10.0V0x.xx

- 2. Detector text transmission has been programmed in the IACP (operating unit texts):

Transmission German:
SMS/E-Mail Gerätename
Identnummer: XXXXXXXXXXXX
".... 80-stelliger EMZ Meldertext ..."

Honeywell Security Deutschland
Novar GmbH
Übertragungsgerät: DS6700 / DS6750
Software Version: ADIST.10.0V0x.xx

Transmission English:
SMS/E-Mail Gerätename
ID-Number: XXXXXXXXXXXX
".... 80-stelliger EMZ Meldertext ..."

Honeywell Security Deutschland
Novar GmbH
Dialer type: DS6700 / DS6750
Software Version: ADIST.10.0V0x.xx

- 3. No detector texts have been stored or activated:

Transmission German:
SMS/E-Mail Gerätename
Identnummer: XXXXXXXXXXXX
Meldung:
Gerät: DS / EMZ
Adresse: 1...99
Zustand: ein / aus

Honeywell Security Deutschland
Novar GmbH
Übertragungsgerät: DS7700 / DS7600
Software Version: ADIST.10.0V0x.xx

Transmission English:
SMS/E-Mail Gerätename
ID-Number: XXXXXXXXXXXX
Message:
System: Dialer / Panel
Address: 1...99
State: on / off

Honeywell Security Deutschland
Novar GmbH
Dialer type: DS7700 / DS7600
Software Version: ADIST.10.0V0x.xx

6.4.2 GSM active

When using and commissioning a redundant radio path (RFW-4000 / RFW-3000), the GSM modem is activated with this entry.

6.4.3 GSM PIN

Entry of the PIN number (up to 8 digits), which is allocated to the SIM card in use.

Please only connect the GSM modem (RFW-4000 / RFW-3000) to the transmission device once the correct PIN has been stored. If no GSM modem is connected, the GSM functionality should not be activated.

6.4.4 GSM network access

Only possible with RFW-4000.10 or RFW-3000.10. If RFW-4000 or RFW-3000 is used, then 2G programming is mandatory here.
Auto mode: The RFW uses the field strength to determine whether it logs into the 2G or 3G network.

CSD connections are not possible in the 3G network. Hence, the following connections are not possible with the "3G only (UMTS)" setting.
- GSM to GSM
- GSM to ISDN V.110
- Telim via GSM (possible with some exceptions)
- Contact ID via GSM (possible with some exceptions)
In "Auto Mode 2G/3G (GPRS/UMTS)" setting, an automatic changeover to GPRS takes place for a short period for these connections.

6.4.5 GSM detect fault after

Entering a time here ensures that brief faults in GSM network access do not lead to a signal (fault signal) (entry range 20 seconds to 18 hours).
If a time value is entered here (default setting 20 seconds), a GSM fault will only be detected after this time has elapsed.
This delay time only applies to the trigger message (the fault is only signaled after the time entered), so that any "good reports" for the relevant criterion are not delayed. Likewise, an event memory entry is only made after the time entered.

VdS The programming of a delay time greater than 20 seconds is not VdS-compliant.

6.4.6 E-mail parameters

E-mail parameters can be entered for both transmission devices. For the transmission device DS 6700, e-mail transmission is performed via Ethernet. The DS 6750 sends e-mail via all IP networks (GPRS, Ethernet or PSTN PPP).

The user name of the e-mail account as well as the own e-mail address (assigned to the transmission device) are to be stored as e-mail parameters. The user name is displayed to the e-mail recipient as the sender's name, the e-mail address is displayed to the e-mail recipient as the sender's e-mail address.
The e-mail server parameters are entered by clicking on the "Change" button.

6.4.7 E-mail server parameters

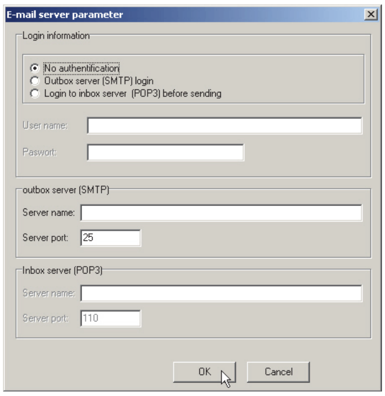
The login information is to be entered in this tab, which is provided by the Internet service provider (e-mail provider) or administrator. Depending on the e-mail account the Internet service provider may require secure password authentication prior to sending for the incoming mail server (POP3) or outgoing mail server (SMTP) and this has to be included in the login information.

- User name: Login name for the e-mail server

- Password: Password to log into the e-mail server

- Server name: Address of the incoming and outgoing mail servers, can only be entered as a numeric xxx.xxx.xxx.xxx IP address or domain name.

- Server port: Port of outgoing or incoming mail server.



Login information
● No authentification
○ Outbox server (SMTP) login
○ Login to inbox server (POP3) before sending
User name:
Paswort:

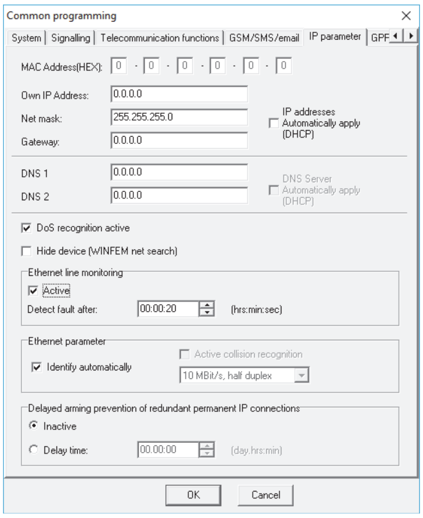
outbox server (SMTP)
Server name:
Server port: 25

Inbox server (POP3)
Server name:
Server port: 110

6.5 "IP parameters" tab

To configure the IP functions of the transmission device, you need some information and parameters that may be provided by your network administrator.

Please note the following for DSL access:
Direct connection to a DSL modem is not possible. Network access has to be made via a router as a general rule. This can in turn be connected directly to the DSL modem. Modem and router are usually integrated in a single device.



MAC Address(HEX): 0 - 0 - 0 - 0 - 0 - 0
Own IP Address: 0.0.0.0
Net mask: 255.255.255.0
Gateway: 0.0.0.0
□ IP addresses Automatically apply (DHCP)
DNS 1 0.0.0.0
DNS 2 0.0.0.0
□ DNS Server Automatically apply (DHCP)
☑ DoS recognition active
□ Hide device (WINFEM net search)

Ethernet line monitoring
☑ Active
Detect fault after: 00:00:20 (hrs:min:sec)

Ethernet parameter
☑ Identify automatically
□ Active collision recognition
10 MBit/s, half duplex

Delayed arming prevention of redundant permanent IP connections
● Inactive
○ Delay time: 00.00:00 (day.hrs:min)

6.5.1 MAC address

The MAC address is printed at the factory and can not be changed, but only controlled. The MAC address is a unique, individual number assigned for each device and serves to clearly identify terminal devices or network cards within a network.

6.5.2 Own IP address

The IP address to be used by the device is to be entered here.

6.5.3 The subnet mask

The IP address contains the address of the network, in which the network user is located and the local address reserved for the terminal device. The first part of the IP address is the network address and the last part is the user address (host address). Separation of the two address parts is not bound to a fixed location but can in theory be placed at any point in the 32-bit IP address.
The length of the network address results from the address class, which in turn depends on the size of the local network (number of network users).
A terminal device has to be able to decide whether a target IP address is in the local network or if the data packets have to be "routed out" of the network through the gateway. The subnet mask is used for this purpose.
A common value for the subnet mask is 255.255.255.0 (class C networks) for example. Other values are possible however. You can obtain detailed information from the responsible system administrator.

6.5.4 Gateway

A gateway is used for connections to users in an external network. The IP address of the gateway has to be communicated to the terminal device (the transmission device here) for connection with users in external networks.

6.5.5 Automatic IP address allocation (DHCP)

If the "IP addresses Automatically apply (DHCP)" check box is checked, the device is automatically assigned the IP parameters (address, subnet mask and gateway) by a DHCP server in the network. In many standard DSL connections, the functionality of a DHCP server is carried out by the existing DSL router.

ℹ As a result the IP address of the device can change dynamically, and thus access for remote maintenance via IP may no longer be possible.

6.5.6 Entry for DNS 1 / DNS 2

The DNS IP address is used by the transmission device for domain address name resolution into an IP address. For example, a request of the address "mailto.t-online.de" returns the IP address "194.25.134.89". The returned IP address does not always have to be the same, because the request may be redirected to a different IP address depending on availability. In the case of dial-up via PSTN PPP, DNS addresses are assigned automatically.
If the "DNS Server Automatically apply (DHCP)" check box is checked, then the IP addresses of available DNS servers are automatically assigned to the device by an existing DHCP server.

6.5.7 Ethernet line monitoring

VdS Line monitoring has to be activated as a general rule (default setting) for VdS-compliant use. Permanent layer-1 monitoring of the Ethernet interface is carried out from the transmission device. If layer-1 of the Ethernet interface has been down, Ethernet access is evaluated as "in trouble".
Entering a time here ensures that brief faults do not lead to a signal (fault signal) (the fault is only reported after the time entered - entry range 20 seconds to 1 hour). The programming of a delay time greater than 20 seconds is not VdS-compliant. Likewise, an event memory entry is only made after the time entered. **Exception: In the case of a DP4 connection to security companies, this line monitoring is not to be programmed because the line monitoring is programmed in the dialog tab for the individual connections.**

6.5.8 DoS recognition

If the transmission device receives numerous illegal or improper data packets for several seconds, then the network connection is disabled for a few seconds to ensure the remaining functions of the device and to prevent further interference. Whether the impingement persists and the device has to be disconnected again is then checked at frequent intervals. Such a sabotage attempt is signaled in the same way as line monitoring.

6.5.9 Hide device

If this check box is checked, then the device will not be visible in a network via the WINFEM internal device search. All other devices are listed in the respective WINFEM search dialog, which allows for accessing devices via IP even in networks with automatic address assignment (DHCP).

6.5.10 Ethernet parameters

If the "Identify automatically" check box is checked, the device automatically detects the Ethernet parameters to be used. In some applications, this is not desirable or possible. In such cases, the parameters are then adjusted manually according to the network requirements.

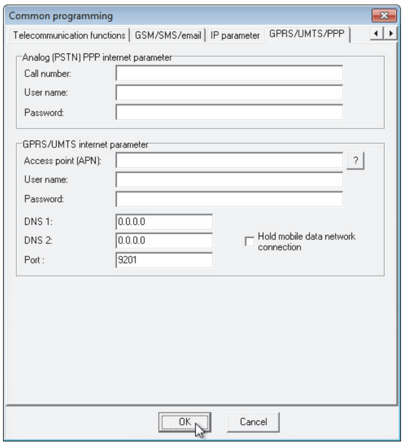
6.6 "GPRS/PPP" tab

6.6.1 Analog (PSTN) PPP Internet parameter

The parameters for the (PSTN) PPP Internet access can only be entered with the DS 6750. These parameters are used for e-mail delivery and message transmission over VdS 2456.

For this configuration, you need some information and parameters that have to be made provided to allow for dial-in via an analog (PSTN) connection to the Internet (e.g. Internet by Call).

- Call number:	Dial-in number of Internet provider
- User name:	Login for Internet access
- Password:	Password to log in for Internet access



Analog (PSTN) PPP internet parameter
Call number:
User name:
Password:

GPRS/UMTS internet parameter
Access point (APN):
User name:
Password:
DNS 1: 0.0.0.0
DNS 2: 0.0.0.0
Port : 9201
□ Hold mobile data network connection

6.6.2 GPRS Internet parameter

In conjunction with the RFW-4000 / RFW-3000, the transmission devices allow for message transmission via GPRS and also UMTS (3G) for:

- Dedicated IP connections (encrypted and unencrypted),
- Demand-actuated IP connections (encrypted and unencrypted),
- E-mail sending (only DS 6750).
- NTP (only DS 6750).

Using the "?" button, the menu for predefined selection of several providers is opened. The selection is accepted by clicking and the data is entered in the parameter fields.
Activation of the GPRS / UMTS connection requires GSM activation in the "GSM / SMS" tab.

The GPRS/ UMTS connection is disconnected during GSM csd dial-up connection.

- Hold mobile data network connection
  If the transmission device is to remain logged on in GPRS/UMTS, the check box is to be checked.

The login information provided by the service provider (GPRS provider) or administrator is to be entered in the tab.

- Access point (APN):	(access point name), name of an access point in a GPRS network
- User name:	User name
- Password:	Password for the GPRS Internet connection
- DNS 1:	first DNS IP address
- DNS 2:	second DNS IP address
- Port:	Account number

Examples for current access data in Germany (as of April 2016, no responsibility taken for correctness). Current access data is to be verified with the mobile operators.

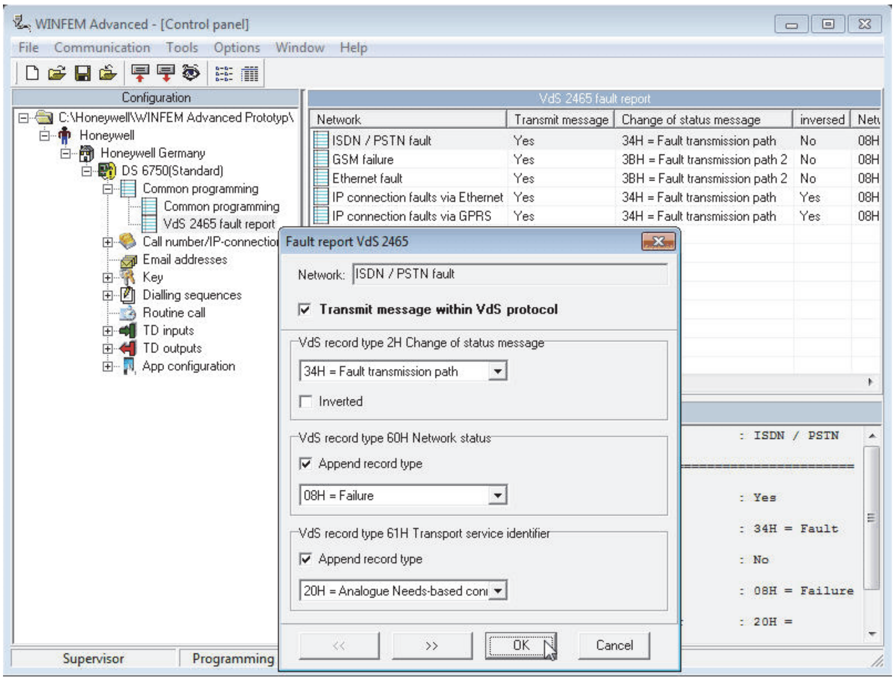
Provider	**T-D1**	**Vodafone**	**E-Plus**	**O2**
Access point (APN)	internet.t-mobile	web.vodafone.de	internet.eplus.de	surfo2 *or* internet *(depending on the contract)*
User name	any1)	—*	eplus	—*
password	any1)	—*	gprs	—*
DNS 1	193.254.160.1	139.007.30.125	212.23.97.2	62.134.11.4
DNS 2	—*	139.007.30.126	212.23.97.3	195.182.110.132
Port	9201	9201	9201	9201

any1) Entry required, field can not remain empty. *— no entry required

Note on cost control: A GPRS "flat rate" is to be selected for dedicated line connections because GPRS fees are usually billed according to the transferred data volume.
No precise statements can be made pertaining to the amount of data of demand-actuated IP connections via GPRS, and therefore we recommend a GPRS "flat rate" here as well.

6.7 "Fault report VdS 2465" tab

The tab "Fault report VdS 2465" is opened by double clicking on the corresponding network access entry in the component/status window.



Network	Transmit message	Change of status message	inversed	Netı
ISDN / PSTN fault	Yes	34H = Fault transmission path	No	08H
GSM failure	Yes	3BH = Fault transmission path 2	No	08H
Ethernet fault	Yes	3BH = Fault transmission path 2	No	08H
IP connection faults via Ethernet	Yes	34H = Fault transmission path	Yes	08H
IP connection faults via GPRS	Yes	34H = Fault transmission path	Yes	08H

Fault report VdS 2465

Network: ISDN / PSTN fault

☑ **Transmit message within VdS protocol**

VdS record type 2H Change of status message

34H = Fault transmission path

☐ Inverted

VdS record type 60H Network status

☑ Append record type

08H = Failure

VdS record type 61H Transport service identifier

☑ Append record type

20H = Analogue Needs-based coni

```
: ISDN / PSTN
========================
: Yes
: 34H = Fault
: No
: 08H = Failure
: 20H =
```

For each network access entry, the transmit message within the VdS protocol can be individually specified for the record type or can be reprogrammed on the basis of control center specifications.

To restore these parameters to the default factory programming, use the command "Standard data" in the "Tools" menu to selectively restore this area of programming.

7. Programming of call numbers / IP connections

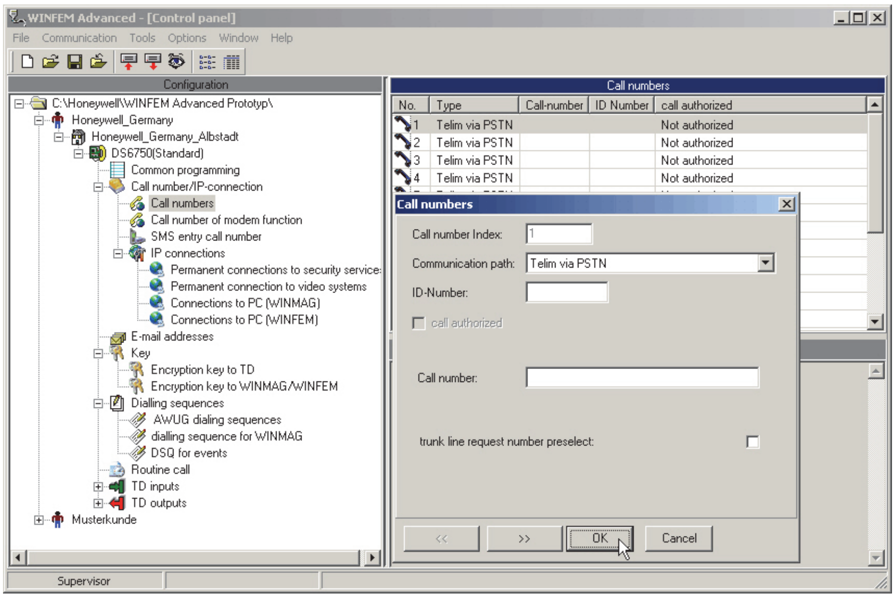
Programming of the call numbers and IP connection data is divided into the respective type of call number or IP connection. When you click the +-symbol in the configuration window, the tree structure will expand and show the individual call number type.

These are in detail:

- Call numbers
- Call numbers modem function
- SMS entry call number
- IP connections:
  (Dedicated line connections as well as connections to WINMAG, video control panels and WINFEM).

When you click on the individual call number type in the configuration window, the individual parameters (call numbers and their configuration) are displayed in the components/status window.
Double clicking directly on the call number or user address in the components/status window opens the individual configuration menu.

7.1 Call numbers


WINFEM Advanced - [Control panel]
File Communication Tools Options Window Help
Configuration
C:\Honeywell\WINFEM Advanced Prototyp\
Honeywell_Germany
Honeywell_Germany_Albstadt
DS6750(Standard)
Common programming
Call number/IP-connection
Call numbers
Call number of modem function
SMS entry call number
IP connections
Permanent connections to security service:
Permanent connection to video systems
Connections to PC (WINMAG)
Connections to PC (WINFEM)
E-mail addresses
Key
Encryption key to TD
Encryption key to WINMAG/WINFEM
Dialling sequences
AWUG dialing sequences
dialling sequence for WINMAG
DSQ for events
Routine call
TD inputs
TD outputs
Musterkunde
Supervisor
<<
>>
OK
Cancel

Call numbers

No.	Type	Call-number	ID Number	call authorized
1	Telim via PSTN			Not authorized
2	Telim via PSTN			Not authorized
3	Telim via PSTN			Not authorized
4	Telim via PSTN			Not authorized

Call numbers

Call number Index: 1

Communication path: Telim via PSTN

ID-Number:

□ call authorized

Call number:

trunk line request number preselect: □

The device has a user memory in which up to 20 different call numbers, or other destination addresses (e.g. IP addresses) can be entered. In a special configuration menu, the target addresses stored in this memory can be assigned to the different "dialing sequences" (see "AWUG dialing sequences", "Dialing sequences for WINMAG" and "DSQ for events").

Basic explanations concerning the configuration menu:

- Call number "Index“

shows the position of the current call number in the call number memory - this number is the internal call number name/address of the device.

- Check box "Authorized to call“

Here you can define whether a call from the number stored at this position is to be accepted.

For some call number/user types, it does not make sense to activate the call authorization, e.g. an e*Cityruf number cannot be authorized to call.

- ID Number

The ID number belonging to the individual user is entered here. By means of this number, the transmission device identifies itself at the remote station (e.g. emergency call control center).

The length of the identification number is limited to 12 digits max .
In case of a Telim transmission, the ID number must always have 6 digits.
In case of contact ID transmissions, only 4 digits may be entered.

- Call number

The call number of the user is stored here. For some user types (IP connections, e-mail), the configuration menu is different here since other or additional information or parameters must be stored. (Please observe the notes concerning the individual call number types).

- Call number protocol

The user type and the transmission protocol used are specified here.

- Trunk line request number preselect

The users to be addressed can be within the same private branch exchange system as the transmission device. In this case, no trunk line request number must be dialed for contacting the user.

Explanations concerning the individual call number/address types and relevant notes for the configuration.

7.1.1 Telim via PSTN / GSM (GSM only with RFW-4000)

This connection is only possible with some restrictions when a GSM modem is used in "3G network" setting.

Telim is an analogue transmission protocol. According to the receiving device in the control center (demand-driven connection), this protocol must be used.

7.1.2 Contact ID via PSTN / GSM (GSM only with RFW-4000)

This connection is only possible with some restrictions when a GSM modem is used in "3G network" setting.

Contact ID is an analogue transmission protocol. According to the receiving device in the control center (demand-driven connection), this protocol must be used.

VdS The transmission of alarm criteria with Contact ID protocol is **not** performed according to VdS regulations.

7.1.3 VdS2465 analogue

This call number protocol is suitable for demand-driven connections via analogue telephone connections. The connection between the transmission device and the receiving control panel takes place via V.22 and a transfer rate of 1200 bit/s.

7.1.4 e* Cityruf tone-only

The transmission functionality is similar to SMS but the transmission is not made to mobile phones but to pagers (network: e*message , successor of Cityruf).

7.1.5 Voice over PSTN / GSM (GSM only with RFW-4000)

In addition to emergency service centers, DS 6700 / DS 6750 transmission devices can also be used to call private individuals (telephone / mobile phone). Messages are transmitted as plain text announcements. To this end, the device is equipped with a standard vocabulary from which the particular message is generated depending on the application and functionally. In addition to this, it is possible to enter (record) individual text passages.

Please refer to Section 20.6 for further information on programming the voice function.

- The "Announcement acknowledgment" check box

  When checked, the voice message has to be acknowledged by the called party. Acknowledgment is performed using the telephone keypad with the ID number assigned to the user.

- The "Authorized to call" check box

  Here you can define whether a call from the number stored at this position is to be accepted to perform interrogations and remote control functions (DS 6750 only).

7.1.6 SMS transmission and protocols

Explanations concerning the individual SMS transmission types and relevant notes for the configuration are included in Section 7.3.

7.1.7 GSM to PSTN (V.110)

Only possible if an RFW-4000 is connected. Messages are transmitted via GSM (in the 2G mobile network) to a receiving device, control centre (ARC = Alarm Receiving Centre).

This connection is not possible when a GSM modem is used in "3G network" setting!

If a alternative path is required with continuous routing, GSM transmission has to be used throughout. This requires that the receiving device is equipped with a GSM receiver. Nevertheless, in certain aspects GSM to PSTN can be sensible.

7.1.8 GSM to GSM

Only possible if an RFW-4000 / RFW-3000 is connected. The transmission of the message is sent via GSM in the 2G mobile network) to a GSM receiving device. This transmission setting is used if an alternative path is required with continuous routing.

This connection is not possible when a GSM modem is used in "3G network" setting!

7.1.9 Demand-actuated Ethernet IP

Not only dedicated but also demand-actuated line connections can be implemented via IP networks. Unlike "conventional network addresses" (call numbers), the IP address of the recipient have to be stored for these types of connections.

In addition to this, the following parameters have to be entered:

The local port number used by the transmission device on connection to the remote site. 0 is to be entered here as a general rule and the transmission device then automatically determines an available port. If necessary, consult the network administrator.

The destination port used by the receiving device. For more information, the control center operator is to be asked.

- DSCP/ToS: If required by the network administrator, prioritization can be set in local networks using this input field.

- VdS service request activated:
  In the VdS2465 protocol, a message can only be issued if the receiving control unit first polls the transmission unit. This is normally happens every 8 seconds from the receiving control unit. In order to reduce the volume of data, some control rooms can increase the polling interval. The disadvantage here is that messages will also be transmitted with a delay. The VdS2465 protocol "service request" feature allows the transmission unit actively to request a poll from the receiving control unit in order to transmit the message promptly.

It is essential to check with the alarm receiving centre whether this performance feature is supported.
In addition, the "Fault detection after" time must not be less than the maximum polling time of the control room, as otherwise a line fault will be detected. A reserve of at least 10 seconds is recommended.
The "Detect fault after" time is set for the **Ethernet connection** (Ethernet line monitoring) in the ➜ **IP Parameter** tab in the ➜ **Common programming** parameter group.

7.1.10 Demand-actuated encrypted Ethernet IP

This call number protocol is applied if a demand-actuated connection is to be implemented via IP networks and secure transmission is also required. Up to 5 keys can be stored for the transmission devices, one of which must be assigned.

- The "Previously transfer ID number“ check box
  Depending on the control center, the ID number can be transmitted without encryption during connection set-up if this check box is checked.

- VdS service request activated:

  In the VdS2465 protocol, a message can only be issued if the receiving control unit first polls the transmission unit. This is normally happens every 8 seconds from the receiving control unit. In order to reduce the volume of data, some control rooms can increase the polling interval. The disadvantage here is that messages will also be transmitted with a delay. The VdS2465 protocol "service request" feature allows the transmission unit actively to request a poll from the receiving control unit in order to transmit the message promptly.

It is essential to check with the alarm receiving centre whether this performance feature is supported.
In addition, the "Fault detection after" time must not be less than the maximum polling time of the control room, as otherwise a line fault will be detected. A reserve of at least 10 seconds is recommended.
The "Detect fault after" time is set for the **Ethernet connection** (Ethernet line monitoring) in the ➜ **IP Parameter** tab in the ➜ **Common programming** parameter group.

7.1.11 Demand-actuated GPRS IP

The IP address of the recipient has to be stored for this type of connection. In addition to this, the following parameters have to be entered:
The local port number used by the transmission device on connection to the remote site. 0 is to be entered here as a general rule and the transmission device then automatically determines an available port. If necessary, consult the network administrator.

The destination port used by the receiving device. For more information, the control center operator is to be asked.

- DSCP/ToS: If required by the network administrator, prioritization can be set in local networks using this input field.

- VdS service request activated:

  In the VdS2465 protocol, a message can only be issued if the receiving control unit first polls the transmission unit. This is normally happens every 8 seconds from the receiving control unit. In order to reduce the volume of data, some control rooms can increase the polling interval. The disadvantage here is that messages will also be transmitted with a delay. The VdS2465 protocol "service request" feature allows the transmission unit actively to request a poll from the receiving control unit in order to transmit the message promptly.

It is essential to check with the alarm receiving centre whether this performance feature is supported.
In addition, the "Fault detection after" time must not be less than the maximum polling time of the control room, as otherwise a line fault will be detected. A reserve of at least 10 seconds is recommended.
The "Detect fault after" time is set for the **GPRS connection** (GPRS monitoring) in the ➜ **GSM/SMS/E-Mail** tab in the ➜ **Common programming** parameter group.

7.1.12 Demand-actuated encrypted GPRS IP

This call number protocol is applied if a demand-actuated connection is to be implemented via GPRS IP networks and secure transmission is also required. Up to 5 keys can be stored for the transmission devices, one of which must be assigned.

- The "Previously transfer ID number“ check box

  Depending on the control center, the ID number can be transmitted without encryption during connection set-up if this check box is checked.

- VdS service request activated:

  In the VdS2465 protocol, a message can only be issued if the receiving control unit first polls the transmission unit. This is normally happens every 8 seconds from the receiving control unit. In order to reduce the volume of data, some control rooms can increase the polling interval. The disadvantage here is that messages will also be transmitted with a delay. The VdS2465 protocol "service request" feature allows the transmission unit actively to request a poll from the receiving control unit in order to transmit the message promptly.

It is essential to check with the alarm receiving centre whether this performance feature is supported.
In addition, the "Fault detection after" time must not be less than the maximum polling time of the control

room, as otherwise a line fault will be detected. A reserve of at least 10 seconds is recommended.
The "Detect fault after" time is set for the **GPRS connection** (GPRS monitoring) in the ➜ **GSM/SMS/E-Mail** tab in the ➜ **Common programming** parameter group.

7.1.13 Demand-actuated PSTN PPP IP (only DS 6750)

This protocol is used to connect to an IP network. The connection is established via dial-up over the analog telephone network (PSTN) to the Internet. The IP address of the recipient has to be stored in this case. In addition to this, the following parameters have to be entered:
The local port number used by the transmission device on connection to the remote site. 0 is to be entered here as a general rule and the transmission device then automatically determines an available port. If necessary, consult the network administrator.

The destination port used by the receiving device. For more information, the control center operator is to be asked.
The dial-up parameters for the Internet are entered in the "GPRS / PPP" tab (see Section 6.5).

- DSCP/ToS: If required by the network administrator, prioritization can be set in local networks using this input field.

7.1.14 Demand-actuated encrypted PSTN PPP IP

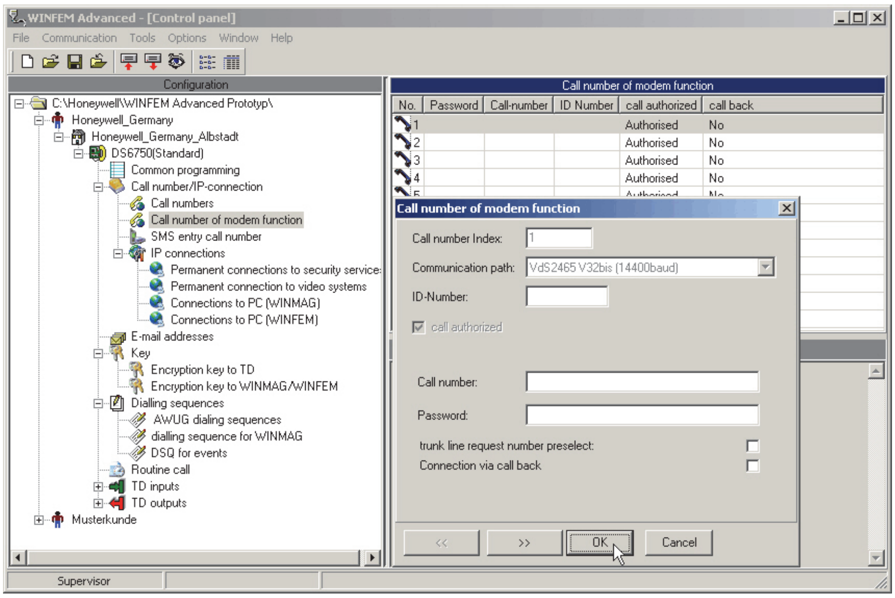
This call number protocol is applied if a demand-actuated connection is to be implemented via PSTN and secure transmission is also required. Up to 5 keys can be stored for the transmission devices, one of which must be assigned. The ID number can optionally be transmitted without encryption during connection set-up (depending on the control center).

7.1.15 E-mail via Ethernet / PSTN PPP / GPRS

E-mail transmission for the DS 6700 transmission device is carried out via Ethernet Internet access. For the DS 6750 transmission device , e-mail can be sen via PSTN PPP Internet access, GPRS or Ethernet Internet access.

One of 10 addresses that can be entered using the configuration menu "E-mail addresses" can be used as the e-mail address.

7.2 Call numbers modem function


WINFEM Advanced - [Control panel]
File Communication Tools Options Window Help
Configuration
C:\Honeywell\WINFEM Advanced Prototyp\
Honeywell_Germany
Honeywell_Germany_Albstadt
DS6750(Standard)
Common programming
Call number/IP-connection
Call numbers
Call number of modem function
SMS entry call number
IP connections
Permanent connections to security service:
Permanent connection to video systems
Connections to PC (WINMAG)
Connections to PC (WINFEM)
E-mail addresses
Key
Encryption key to TD
Encryption key to WINMAG/WINFEM
Dialling sequences
AWUG dialing sequences
dialling sequence for WINMAG
DSQ for events
Routine call
TD inputs
TD outputs
Musterkunde
Supervisor
<<
>>
OK
Cancel

Call number of modem function

No.	Password	Call-number	ID Number	call authorized	call back
1				Authorised	No
2				Authorised	No
3				Authorised	No
4				Authorised	No
5				Authorised	No

Call number of modem function

Call number Index: 1

Communication path: VdS2465 V32bis (14400baud)

ID-Number:

☑ call authorized

Call number:

Password:

trunk line request number preselect: □

Connection via call back □

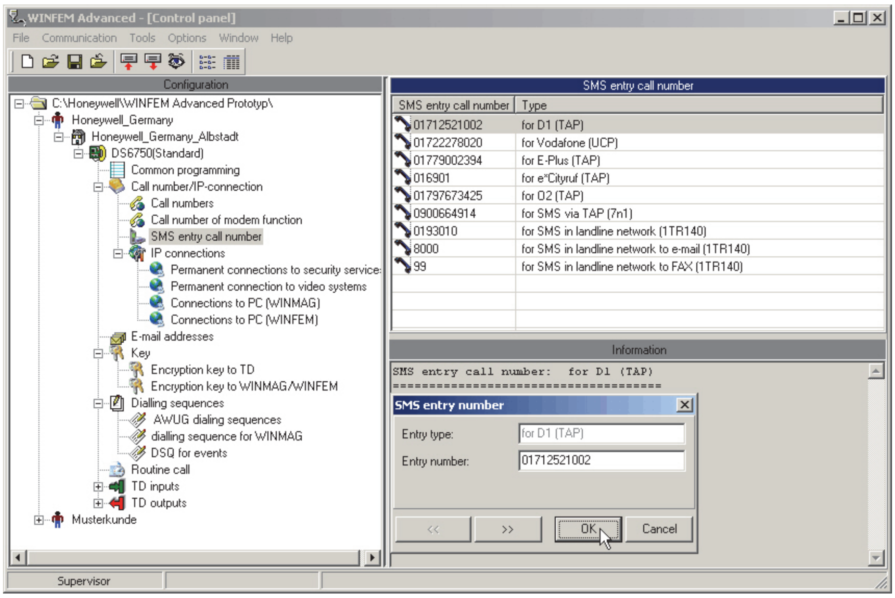
The call numbers of the users admitted for remote service are stored here. The data stored here (identification number, password, call number) must match the data stored in the WINFEM station or WINMAG control center used to access the device via the analog telephone network (PSTN) by modem.

- The “Connection via call back” check box

When calling a WINFEM or WINMAG station at the transmission device, the "caller" transmits the respective password. The transmission device checks whether the password is stored and assigned to a call number. Then the transmission device sends call back acknowledgment to the caller and the telephone connection is disconnected. The transmission device dials the number allocated to the password and transmits the corresponding identification number to the WINFEM or WINMAG station for identification. Now access is possible from this station.

Remote interrogation via call back is the safest way to prevent abuse.
A separate telephone connection is to be set up for the transmission device or the ring tone until call acceptance (see Section 6.3.8) is to be configured appropriately because the transmission device immediately occupies the telephone line when a call is received.

7.3 SMS access call numbers / SMS transmission and protocols


WINFEM Advanced - [Control panel]
File
Communication
Tools
Options
Window
Help
Configuration
C:\Honeywell\WINFEM Advanced Prototyp\
Honeywell_Germany
Honeywell_Germany_Albstadt
DS6750(Standard)
Common programming
Call number/IP-connection
Call numbers
Call number of modem function
SMS entry call number
IP connections
Permanent connections to security service:
Permanent connection to video systems
Connections to PC (WINMAG)
Connections to PC (WINFEM)
E-mail addresses
Key
Encryption key to TD
Encryption key to WINMAG/WINFEM
Dialling sequences
AWUG dialing sequences
dialling sequence for WINMAG
DSQ for events
Routine call
TD inputs
TD outputs
Musterkunde
Supervisor

SMS entry call number

SMS entry call number	Type
01712521002	for D1 (TAP)
01722278020	for Vodafone (UCP)
01779002394	for E-Plus (TAP)
016901	for e*Cityruf (TAP)
01797673425	for O2 (TAP)
0900664914	for SMS via TAP (7n1)
0193010	for SMS in landline network (1TR140)
8000	for SMS in landline network to e-mail (1TR140)
99	for SMS in landline network to FAX (1TR140)

Information

```
SMS entry call number:  for D1 (TAP)
======================================
```

SMS entry number

Entry type: for D1 (TAP)

Entry number: 01712521002

The entry numbers for the SMSC (Short Message Service Center) are stored here.
The call numbers are factory-set and can not be changed . They may only be changed if the access number of an SMSC has changed.

7.3.1 General information on sending an SMS

SMS can be sent by landline using two different methods. Either via a landline SMS provider (1TR140 protocol) such as Deutsche Telekom or Materna (AnnyWay). Or else via a cellular gateway (TAP / UCP protocol) usually offered by the corresponding cellular network operators.

7.3.2 SMS structure

An SMS has the following structure:

SMS device name	Message	ID Number	Date / Time

SMS device name
15 characters freely programmable in the “General Programming”, SMS device name tab.

Message
40 characters can be transmitted per channel for projected and non-projected states. This text is freely programmable in the “DS Inputs” programming in the “Outputs of IACP - SMS text” or permanently stored as standard text in the transmission device for each event. The standard text is provided only if no SMS text has been defined.

ID number
Programmed identification number of the call number.

Date Time
Date and time when an event takes place.

SMS transmission examples:
Including freely programmable message text:
Reich Company. Intrusion alarm at main entrance ID:4711 01.01.2008 at 22.10h

Including standard text message:
Reich Company. IACP line:23 state ON ID:4711 02.01.2008 22.10h

7.3.3 SMS sending via landline over a cellular gateway (TAP and UCP protocol only DS 6750)

Each cellular network operator provides its own gateway for its network. The current entry call number of the cellular gateway can be found in WINFEM under the programming menu “SMS entry call numbers”.
These call numbers are cellular call numbers and are charged according to the duration of the call.
Compared with “SMS by landline” these entries are relatively expensive and unreliable.

Cellular gateways

T-D1	TAP	01712521001	
Vodafone (D2)	UCP	01722278000	
E-Plus	TAP	01779002394	
O2	TAP	01797673425	
SMS via TAP(7n1)	TAP 7n1	0900664914	(Mobilkom Austria)

When using the transmission device in Switzerland, the D2 network access (network operator) must be used calling the following SMSC service call number: 0794998990

7.3.4 SMS via landline (1TR140 protocol only DS 6750)

In Germany there are two providers who offer a gateway (FSMSC) for this type of sending an SMS:
- Deutsche Telekom (on Telekom connections only)
- AnnyWay (also possible on other telephone connections, see www.sms-im-festnetz.de).

One entry allows access to each compatible landline and cellular network. Messages can also be transmitted to landline and cellular networks abroad.

An SMS can be transmitted to a landline number by two methods:
- As voice message (message is being read).
- As SMS (transmission to terminal devices compatible with SMS in landline network)

Normally a received SMS is read in the landline by means of a voice call. The emphasis of the voice output can be affected by punctuation marks. For example, by inserting a comma or period between words and digits, a small pause is added in the voice output.
To receive an SMS as a written message, you must log on once to the corresponding gateway. This must be done once for each landline connection that is to receive the SMS as message. In addition, an SMS-capable landline network telephone is required.

An SMS from the network is **not** accepted by the transmission device. This allows a downstream SMS-capable telephone to continue receiving SMS messages. Accordingly, error messages or reception confirmations from the network will also be sent to the downstream telephone.

ATTENTION: Please note that time restrictions are in place for delivering an SMS as voice message, which cannot be influenced by the transmission device. For information on the current performance characteristics, please contact your provider.
e.g. Deutsche Telekom, times during which an SMS is delivered as a voice message:
Mon. to Fri.: 07:00 a.m. to 11:00 p.m.
Sat. Sun. and public holidays: 08:00 a.m. to 11:00 p.m.

The log-on procedure for receiving an SMS as text message differs from provider to provider.
Deutsche Telekom: Text “ANMELD” by SMS to the call number 8000
AnnyWay: Send one SMS

Gateway parameters: SMS to landline and mobile phone

	Deutsche Telekom	AnnyWay
SMS by landline	193010	9003266900

7.3.5 E-mail and fax recipients (only DS 6750)

The DS 6750 can also send e-mails and faxes via the SMS by landline service. However, this must have been implemented in the corresponding gateway.

In WINFEM and in the DS 6750 the Telekom Gateway has been pre-programmed. To change to the AnnyWay Gateway, for the required parameters, please refer to the following table:

Gateway parameters: e-mail and fax recipients

	Deutsche Telekom	AnnyWay
SMS to Email	Separator “ ” (space) Call number 8000	Separator “:” Call number 6245
SMS to fax recipient	Call number area code 99	Not possible

7.3.6 SMS transmission* via PSTN (to D1, Vodafone, O2, E-Plus) only DS 6750

For SMS messages to cell phones.
Each of the four cellular network operator maintains its own Short Message Service Center (SMSC). Each of the SMSCs have different numbers and the transmission protocols used in each case are different. Therefore it is necessary to distinguish this type of user by operator.

*SMS is a service of the network operator. The transmission device has no influence on the functionality and security of this service. If the SMS user is not reached, 2 more attempts are made to send an SMS via PSTN.

7.3.7 SMS* via PSTN to e* Cityruf

The transmission functionality is similar to SMS but the transmission is not made to mobile phones but to pagers (network: e*message , successor of Cityruf).

*SMS is a service of the network operator. The transmission device has no influence on the functionality and security of this service.

7.3.8 SMS via GSM

Only possible when using the RFW-4000 / RFW-3000. SMS messages are not sent via the SMSC (SMS Service Center) used in "SMS via PSTN", but directly via the GSM modem of the RFW-4000 / RFW-3000.

This type of SMS transmission allows in part SMS transmission to landline users, (please refer to the terms and conditions as well as the specifications the respective carrier).

7.3.9 SMS via GSM Modem to e-mail address (D1, Vodafone, O2, E-Plus)

Only possible if an RFW-4000 / RFW-3000 is connected. One of 10 addresses that can be entered using the configuration menu "E-mail addresses" can be used as the e-mail address.

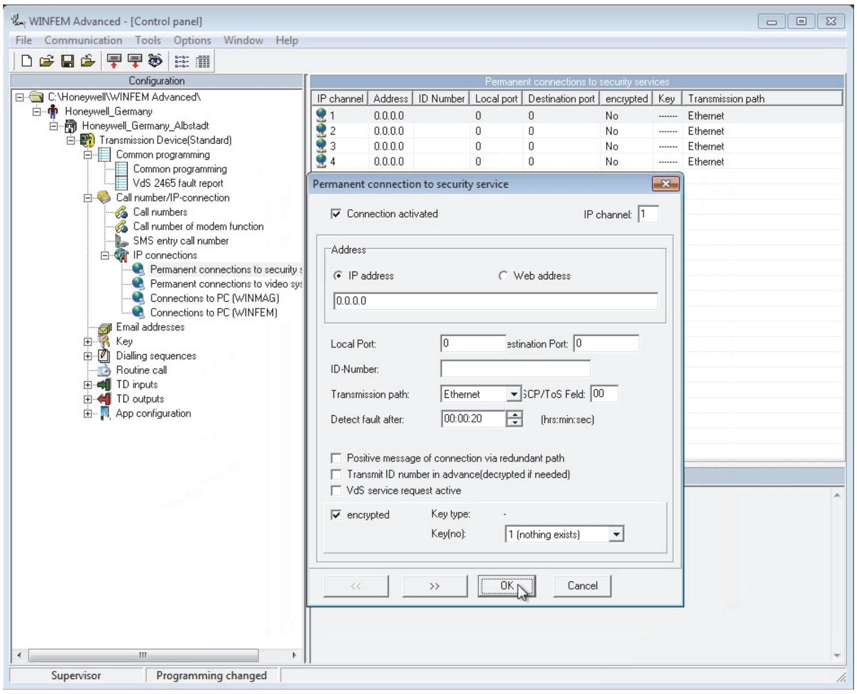
8. IP connections

Programming of the IP connection data is divided into the respective type of IP user. When you click the +-symbol in the configuration window, the tree structure will expand and show the respective IP user type.

These are in detail: Dedicated line connections to security service
Dedicated line connections to video control panels (DS 6750 only)
WINMAG connections (DS 6750 only)
WINFEM connections

By clicking on the appropriate IP user type in the configuration window, the individual parameters (IP addresses and their configuration) are displayed in the component/status window.
Double clicking directly on the IP channel in the components/status window opens the individual configuration menu.

8.1 Dedicated line connections to security service


WINFEM Advanced - [Control panel]
File Communication Tools Options Window Help
Configuration
C:\Honeywell\WINFEM Advanced\
Honeywell_Germany
Honeywell_Germany_Albstadt
Transmission Device(Standard)
Common programming
Common programming
VdS 2465 fault report
Call number/IP-connection
Call numbers
Call number of modem function
SMS entry call number
IP connections
Permanent connections to security s
Permanent connections to video sys
Connections to PC (WINMAG)
Connections to PC (WINFEM)
Email addresses
Key
Dialling sequences
Routine call
TD inputs
TD outputs
App configuration
Supervisor
Programming changed
<<
>>
OK
Cancel

Permanent connections to security services

IP channel	Address	ID Number	Local port	Destination port	encrypted	Key	Transmission path
1	0.0.0.0		0	0	No	-------	Ethernet
2	0.0.0.0		0	0	No	-------	Ethernet
3	0.0.0.0		0	0	No	-------	Ethernet
4	0.0.0.0		0	0	No	-------	Ethernet

Permanent connection to security service

☑ Connection activated IP channel: 1

Address
● IP address ○ Web address
0.0.0.0

Local Port: 0 estination Port: 0
ID-Number:
Transmission path: Ethernet SCP/ToS Feld: 00
Detect fault after: 00:00:20 (hrs:min:sec)

☐ Positive message of connection via redundant path
☐ Transmit ID number in advance(decrypted if needed)
☐ VdS service request active
☑ encrypted Key type: -
Key(no): 1 (nothing exists)

The IP address and port number of the remote site, to which a dedicated line connection is to be established, are entered here. Alternatively a Web address (URL) can be entered. To do this click on the entry "Web address" and enter the Web address (E.g. Alarmreceiver.com) in the input field. This data has to be made available by the control center operator. The local port number is the outgoing port number used by the transmission device on connection to the remote site. 0 is to be entered here as a general rule and the transmission device then automatically determines an available port. If necessary, consult the network administrator.

- DSCP/ToS: If required by the network administrator, prioritization can be set in local networks using this input field.

- The "Positive message of connection via redundant path" check box:
The connection status is communicated via the redundant transmission path. When restoring a connection, the positive message is also sent via the redundant transmission path.

- Checkbox „Transmit ID number in advance“
Depending on the control room, the ID number can be transmitted without encryption when this checkbox is enabled during a connection set-up.

-Detect fault after (time):

VdS A permanent layer 1 check of the Ethernet interface is carried out from the transmission unit. If layer 1 of the Ethernet interface has failed, the Ethernet access is evaluated as "faulty". Entering a time here ensures that brief faults do not lead to a signal (fault signal) (the fault is only reported after the time entered - entry range 20 seconds to 18 hours). The programming of a delay time greater than 20 seconds is not VdS-compliant. Likewise, an event memory entry is only made after the time entered.

- VdS service request activated:

In the VdS2465 protocol, a message can only be issued if the receiving control unit first polls the transmission unit. This is normally happens every 8 seconds from the receiving control unit. In order to reduce the volume of data, some control rooms can increase the polling interval. The disadvantage here is that messages will also be transmitted with a delay. The VdS2465 protocol "service request" feature allows the transmission unit actively to request a poll from the receiving control unit in order to transmit the message promptly.

It is essential to check with the control room whether this performance feature is supported.
In addition, the "Fault detection after" time programmed here must not be less than the maximum polling time of the control room, as otherwise a line fault will be detected. A reserve of at least 10 seconds is recommended.

- The “Redundant to IP connection x” check box

If required, the 4 programmable IP connections can be designed to be redundant to each other. The following fixed assignment applies: IP connection 2 can be programmed as redundant to IP connection 1. IP connection 3 can be programmed as redundant to IP connection 2. IP connection 4 can be programmed as redundant to IP connection 3. It can be set up a DP4 connection to the Receiving Centre Tranceiver (RCT) with 2 primary and 2 secondary connections.

The redundant connections must be parametrized within the dialing sequence using an "or" logic operation.

Connection	permanent connection	redundant to
SP (Single Path) Single Path Alarm transmission		
Single Path	1	-
Single Path	2	1 (off)
Single Path	3	2 (off)
Single Path	4	3 (off)
DP (Dual Path) simple Dual Path Alarm transmission		
Dual Path - Primary Transmission path	1	
Dual Path - Secondary Transmission path	2	1 (on)
DP (Dual Path) Dual Path Alarm transmission		
Dual Path - Primary Transmission path	1	-
Dual Path - redundant alternative Primary Transmission path	2	1 (on)
Dual Path - Secondary Transmission path	3	2 (on)
Dual Path - redundant alternative Secondary Transmission path	4	3 (on)
The Dual Paths Secondary Transmission path must be monitored by routine calls!		

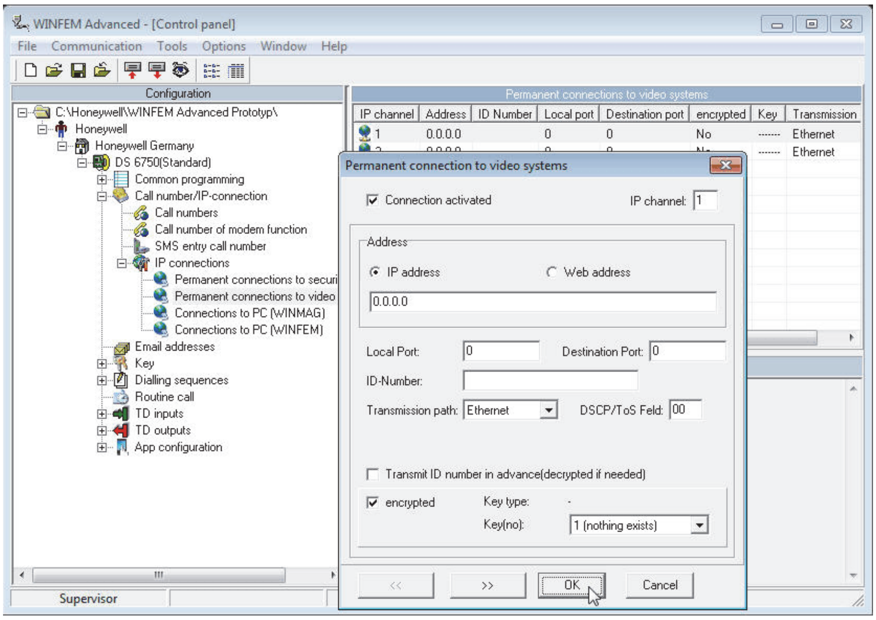
For this programming point observe the chapter “IP transmission of messages”.

- The "encrypted" check box:

data transmitted via IP networks is at increased risk of manipulation. The IP connections must therefore be encrypted under certain conditions and with increased security requirements. If manipulation by third parties can not be excluded for the IP network, then data transfer has to be encrypted.
In this case, the encryption method and key configuration has to be agreed on in advance with the operator of the receiving device. The ID number can optionally be transmitted without encryption during connection set-up (depending on the control center).
If the "encrypted" check box is checked, then an additional window is displayed for selection of the valid key for this connection. The keys are configured in the "key" menu in Section 10.1. (Key to transmission control unit).

BSI To minimize the possibility of error and sabotage in secure (encrypted) connections, it should always be ensured that the same key (number or value) is not used for multiple connections.

8.2 Dedicated line connections to video control panels (DS 6750 only)


WINFEM Advanced - [Control panel]
File Communication Tools Options Window Help
Configuration
Supervisor
<< >> OK Cancel

C:\Honeywell\WINFEM Advanced Prototyp\
- Honeywell
  - Honeywell Germany
    - DS 6750(Standard)
      - Common programming
      - Call number/IP-connection
        - Call numbers
        - Call number of modem function
        - SMS entry call number
        - IP connections
          - Permanent connections to securi
          - Permanent connections to video
          - Connections to PC (WINMAG)
          - Connections to PC (WINFEM)
      - Email addresses
      - Key
      - Dialling sequences
      - Routine call
      - TD inputs
      - TD outputs
      - App configuration

Permanent connections to video systems

IP channel	Address	ID Number	Local port	Destination port	encrypted	Key	Transmission
1	0.0.0.0		0	0	No	-------	Ethernet
						-------	Ethernet

Permanent connection to video systems

☑ Connection activated IP channel: 1

Address

● IP address ○ Web address

0.0.0.0

Local Port: 0 Destination Port: 0

ID-Number:

Transmission path: Ethernet DSCP/ToS Feld: 00

□ Transmit ID number in advance(decrypted if needed)

☑ encrypted Key type: -

Key(no): 1 (nothing exists)

Video panels can be connected to the DS 6750 via TCP/IP (Ethernet). Communication takes place by means of the VdS 2465-S2 protocol via a dedicated TCP/IP connection. The video panel behaves like a transmission control unit in connection with the DS 6750 in accordance with VdS 2471 and 2465-S2. The connection is always established via the DS 6750 The basic requirements of the interface are stipulated in guidelines VdS 2465 VdS 2465-S2. It is possible to couple two video panels with the DS 6750 with dedicated line connections
Changes in state or controls of the intruder alarm control panel are communicated by the DS 6750 to the video panel with the intrusion control panel outputs. The video panel can also communicate changes in state or controls to the intruder alarm control panel using the intrusion control panel inputs and corresponding programmed macros. The connection of the intruder alarm control panel and the video panel permits functional integration of both systems and realization of cross-system interactions such as:

- Illustration of the functionality of both systems
- Integration of the system state of the video panel in the forced actuation of the intruder alarm control panel
- Transmission of system faults to the control center / security service
- Control of the video panel by operating conditions of the intruder alarm control panel
- Control the intruder alarm control panel by operating conditions of the video panel
- Overlaying of names in the video image for access control and switching operations
- Dedicated TCP/IP - connection with ongoing function monitoring

The IP address and port number of the remote site, to which a dedicated connection is to be established, are entered in the input window. Alternatively a Web address (URL) can be entered. To do this click on the entry "Web address" and enter the Web address (E.g. Videocheck.com) in the input field. This data has to be provided by the owner of the video panel or the network administrator.

The local port number is the outgoing port number used by the transmission device on connection to the remote site. 0 is to be entered here as a general rule and the transmission device then automatically determines an available port. If necessary, consult the network administrator.

- DSCP/ToS: If required by the network administrator, prioritization can be set in local networks using this input field.

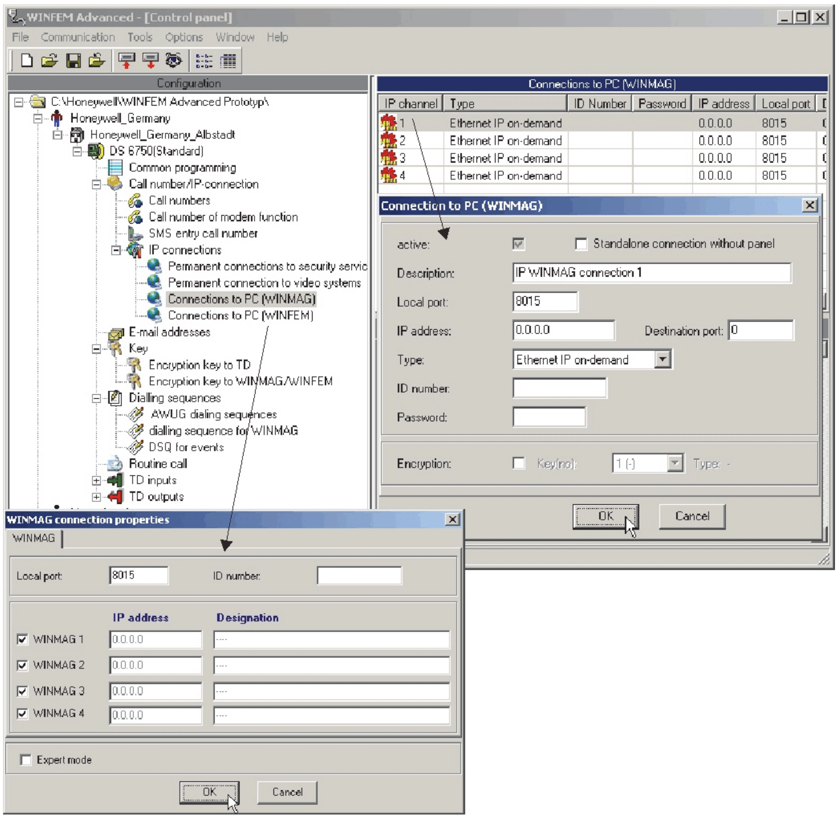
- The "encrypted" check box:

data transmitted via IP networks is at increased risk of manipulation. The IP connections can therefore be encrypted and then meet increased security requirements. If manipulation by third parties can not be excluded for the IP network, then data transfer has to be encrypted.
In this case, the encryption method and key configuration has to be agreed on in advance with the operator of the video panel.

If the "encrypted" check box is checked, then an additional window is displayed for selection of the valid key for this connection. The keys are configured in the "key" menu in Section 10.1.
(Key to transmission control unit).

BSI To minimize the possibility of error and sabotage in secure (encrypted) connections, it should always be ensured that the same key (number or value) is not used for multiple connections.

8.3 WINMAG connections (DS 6750 only)


WINFEM Advanced - [Control panel]
File Communication Tools Options Window Help
Configuration
C:\Honeywell\WINFEM Advanced Prototyp\
Honeywell_Germany
Honeywell_Germany_Albstadt
DS 6750(Standard)
Common programming
Call number/IP-connection
Call numbers
Call number of modem function
SMS entry call number
IP connections
Permanent connections to security servic
Permanent connection to video systems
Connections to PC (WINMAG)
Connections to PC (WINFEM)
E-mail addresses
Key
Encryption key to TD
Encryption key to WINMAG/WINFEM
Dialling sequences
AWUG dialing sequences
dialling sequence for WINMAG
DSQ for events
Routine call
TD inputs
TD outputs

Connections to PC (WINMAG)

IP channel	Type	ID Number	Password	IP address	Local port
1	Ethernet IP on-demand			0.0.0.0	8015
2	Ethernet IP on-demand			0.0.0.0	8015
3	Ethernet IP on-demand			0.0.0.0	8015
4	Ethernet IP on-demand			0.0.0.0	8015

Connection to PC (WINMAG)

active: ☑ ☐ Standalone connection without panel
Description: IP WINMAG connection 1
Local port: 8015
IP address: 0.0.0.0 Destination port: 0
Type: Ethernet IP on-demand
ID number:
Password:
Encryption: ☐ Key(no): 1 (-) Type: -
OK Cancel

WINMAG connection properties

WINMAG

Local port: 8015 ID number:

	IP address	Designation
☑ WINMAG 1	0.0.0.0	----
☑ WINMAG 2	0.0.0.0	----
☑ WINMAG 3	0.0.0.0	----
☑ WINMAG 4	0.0.0.0	----

☐ Expert mode

OK Cancel

8.3.1 WINMAG input window

The IP address and port number of the remote site (destination port), to which a dedicated or demand-actuated line connection is to be established, are entered here. This data has to be made available by the WINMAG system administrator.

The local port number is the outgoing port number used by the transmission device on connection to the remote site. 0 is to be entered here as a general rule and the transmission device then automatically determines an available port. If necessary, consult the network administrator.

- The “Stand alone connection without panel” check box

If the transmission device is operated without downstream intruder alarm control panel and WINMAG connection is to be realized, then this check box is to be checked. This performance feature can be used to connect (external) WINMAG units. Up to 4 IP connections, which is selected in this dialog, and a PSTN dial-up connection, which is selected in the "Dialing sequence for WINMAG" dialog, are used as a means of transmission.

In a system configuration with a downstream intruder alarm control panel, it is possible to transmit the system configuration on one WINMAG connection and the states of the 8 detector group inputs (E1 - E8) on another WINMAG connection of the transmission device.

Up to 88 input states can be transmitted using the BUS-2 master functionality of the DS 6750. Up to 82 outputs are used for switching operations. It is also possible to transmit system information from the DS 6750 to WINMAG.

- Description

A custom text for the connection can be entered in this field. The text can be up to 40 characters long and also appears as an event log entry.

- Password

The WINMAG PC uses the password to authenticate itself with the transmission device. This password is not identical with the password for PSTN connections. The password can consist of up to 8 digits.

The same password can not be used for the WINMAG PC and the WINFEM PC (see Section 8.3.1)!

- The "encrypted" check box

If the "encrypted" check box is checked, the valid key for this connection can be selected in the selection window. The keys are configured in the "key" menu in Section 10.2 (key to WINMAG/WINFEM)

BSI

To minimize the possibility of error and sabotage in secure (encrypted) connections, it should always be ensured that the same key (number or value) is not used for multiple connections.

- Connection type

List of the possible routeways to WINMAG. The corresponding connection type is to be set in the dialog. When connecting to WINMAG via Ethernet, the "demand-actuated Ethernet IP" setting is recommended because the WINMAG PC usually initializes the connection.
The "demand-actuated GPRS IP" connection type can only be implemented using the service of a GSM provider, which allows incoming connections to the GPRS IP address.

8.3.2 WINMAG connections properties input window

- ID number

This parameter appears only when the expert mode is not activated. If the “export mode” parameter is activated, then an individual ID number can be assigned for each individual connection. If the "expert mode" parameter is not active, then the ID number applies to all connections. The transmission device identifies itself to the WINMAG PC using this ID number. This ID number is not identical to the ID number for PSTN connections. The ID no. can consist of up to 12 digits.

- Activation of WINMAG (connections)

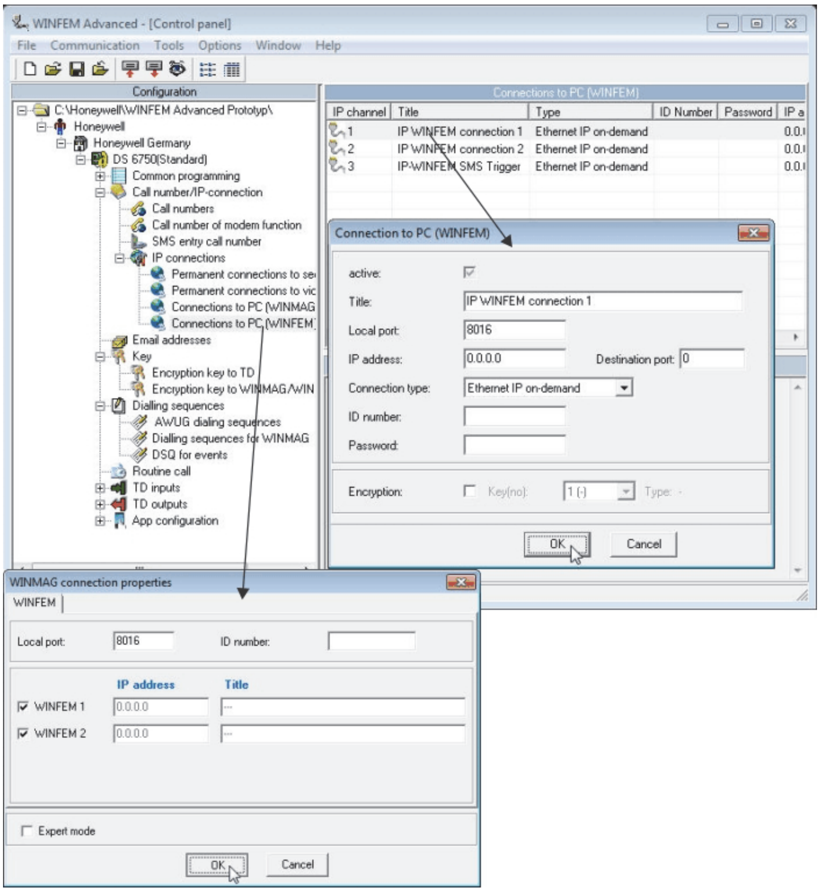
  Required connections can be released or blocked using the respective check box. The connection is released if the check box is checked. This allows for creation of multiple connections and only the required connection is released.

- Expert mode

  If expert mode is activated, then the "Destination port" and "ID number" can be entered separately for each connection. If the expert mode is not activated, then the same ID number is used for every connection. The destination port is set to the same value as the local port.

If the expert mode was activated and different ID numbers were assigned, then the ID number of WINMAG connection 1 is adopted for the other connections when the expert mode is switched off. In the case of different destination port values, all connections are changed to the value of the local port.

8.4 WINFEM connections


WINFEM Advanced - [Control panel]
File Communication Tools Options Window Help
Configuration
C:\Honeywell\WINFEM Advanced Prototyp\
Honeywell
Honeywell Germany
DS 6750(Standard)
Common programming
Call number/IP-connection
Call numbers
Call number of modem function
SMS entry call number
IP connections
Permanent connections to se
Permanent connections to vic
Connections to PC (WINMAG
Connections to PC (WINFEM)
Email addresses
Key
Encryption key to TD
Encryption key to WINMAG/WIN
Dialling sequences
AWUG dialing sequences
Dialling sequences for WINMAG
DSQ for events
Routine call
TD inputs
TD outputs
App configuration

Connections to PC (WINFEM)

IP channel	Title	Type	ID Number	Password	IP a
1	IP WINFEM connection 1	Ethernet IP on-demand			0.0.0
2	IP WINFEM connection 2	Ethernet IP on-demand			0.0.0
3	IP-WINFEM SMS Trigger	Ethernet IP on-demand			0.0.0

Connection to PC (WINFEM)

active: ☑
Title: IP WINFEM connection 1
Local port: 8016
IP address: 0.0.0.0 Destination port: 0
Connection type: Ethernet IP on-demand
ID number:
Password:
Encryption: ☐ Key(no): 1 (-) Type: -

OK Cancel

WINMAG connection properties

WINFEM

Local port: 8016 ID number:

	IP address	Title
☑ WINFEM 1	0.0.0.0	---
☑ WINFEM 2	0.0.0.0	---

☐ Expert mode

OK Cancel

8.4.1 WINFEM input window

The IP address and port number of the remote device (destination port) from which demand-actuated connection can be made, are entered here to configure the transmission device and the system. The IP address does not necessarily have to be entered. This is only required if access can only be made from certain IP addresses (fixed IP address). Due to the fact that it can be assumed that it will also be accessed from "dynamic IP addresses", entering the IP address at this point is usually not necessary.
The local port number is the outgoing port number used by the transmission device on connection to the remote site. 0 is to be entered here as a general rule and the transmission device then automatically determines an available port. If necessary, consult the network administrator.

Entry of the ID number and password is required as a general rule.

- Description

A custom text for the connection can be entered in this field. The text can be up to 40 characters long and also appears as an event log entry.

- Type of connection

List of possible connection paths to WINFEM. The appropriate connection type must be set in the dialog. Used when connecting via "demand-actuated Ethernet IP" Ethernet, since it is the WINFEM-PC that generally initializes the connection.
To set up a connection with the function "Remote maintenance via SMS-trigger", the connection type "GPRS IP demand-actuated" must be used.

- Password

The WINFEM PC uses the password to authenticate itself with the transmission device. This password is not identical with the password for PSTN connections. The password can consist of up to 8 digits.

ℹ The same password can not be used for the WINMAG PC and the WINFEM PC (see Section 8.2.1)!

- The "encrypted" check box

If the "encrypted" check box is checked, the valid key for this connection can be selected in the selection window. The keys are configured in the "key" menu in Section 10.2 (key to WINMAG/WINFEM)

BSI To minimize the possibility of error and sabotage in secure (encrypted) connections, it should always be ensured that the same key (number or value) is not used for multiple connections.

EN The remote access for WINFEM must be set up with AES encryption (see chapter 10.2).

8.4.2 WINFEM connections properties input window

- ID number

This parameter appears only when the expert mode is not activated. If the “export mode” parameter is activated, then an individual ID number can be assigned for each individual connection. If the "expert mode" parameter is not active, then the ID number applies to all connections. The transmission device identifies itself to the WINFEM PC using this ID number. This ID number is not identical to the ID number for PSTN connections. The ID no. can consist of up to 12 digits.

- Activation of WINFEM (connections)

Required connections can be released or blocked using the respective check box. The connection is released if the check box is checked. This allows for creation of multiple connections and only the required connection is released.

- Expert mode

If expert mode is activated, then the "Destination port" and "ID number" can be entered separately for each connection.
If the expert mode is not activated, then the same ID number is used for every connection. The destination port is set to the same value as the local port.

ℹ If the expert mode was activated and different ID numbers were assigned, then the ID number of WINFEM connection 1 is adopted for the other connections when the expert mode is switched off. In the case of different destination port values, all connections are changed to the value of the local port.

8.4.3 Remote maintenance with SMS-trigger

Transmission devices TD 6700 and TD 6750 can establish a connection with a WINFEM at a pre-defined IP address ❶ or at an IP address communicated to them ❷. Connection setup is initiated via an SMS-trigger to the transmission device. An SMS-trigger is an SMS to the transmission device that results in a call-back via Ethernet or GPRS. Remote maintenance can be performed via the connection established either over a point-to-point Ethernet connection or over the mobile network using GPRS.

The procedure below should be followed:

● For remote maintenance via SMS-trigger, an RFW-3000 or RFW-4000 must be used.

❶ The pre-programmed IP channel to be used for establishing a connection is selected by sending an SMS with the following content:

Trigger IPx [Passwort]
Passwort -> Passwort of the WINFEM IP connection
x -> WINFEM IP connection1 or 2

Example: Trigger IP1 123456

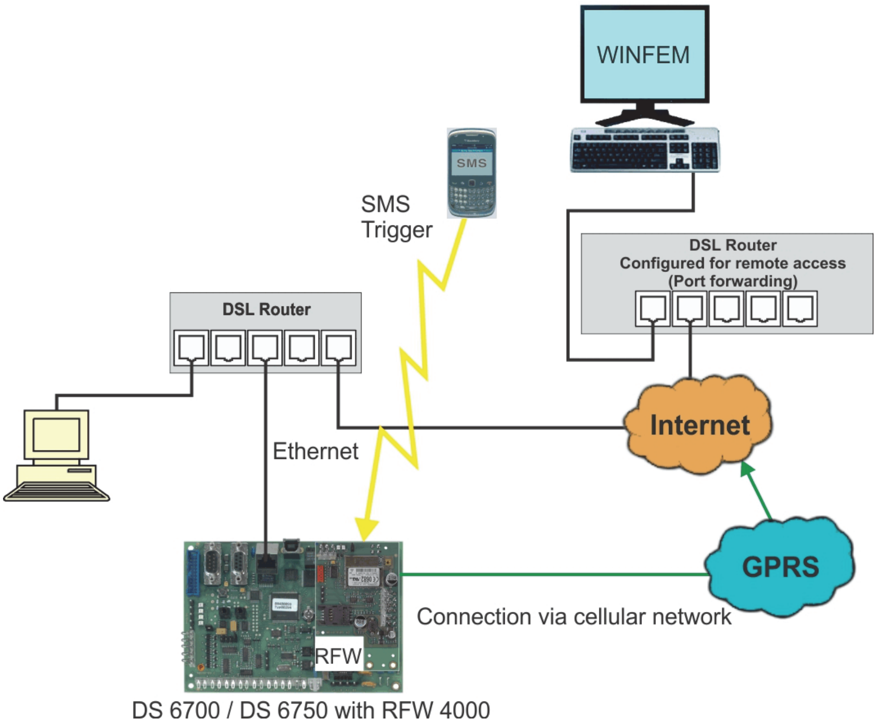
Upon receipt of the SMS, the transmission device checks to see if this password is assigned to the relevant WINFEM IP connection. Next, the transmission device establishes an IP connection using the stored connection data and transmits the corresponding ID no. to the WINFEM station for identification. Access from this station is now enabled.

❷ **An alternate method for establishing a connection** is to send the destination IP address and connection path (Ethernet/GPRS) for the connection setup in the SMS. This procedure is used when the WINFEM IP address for connection setup is not a fixed IP address.
Connection setup is initiated by sending an SMS with the following content:

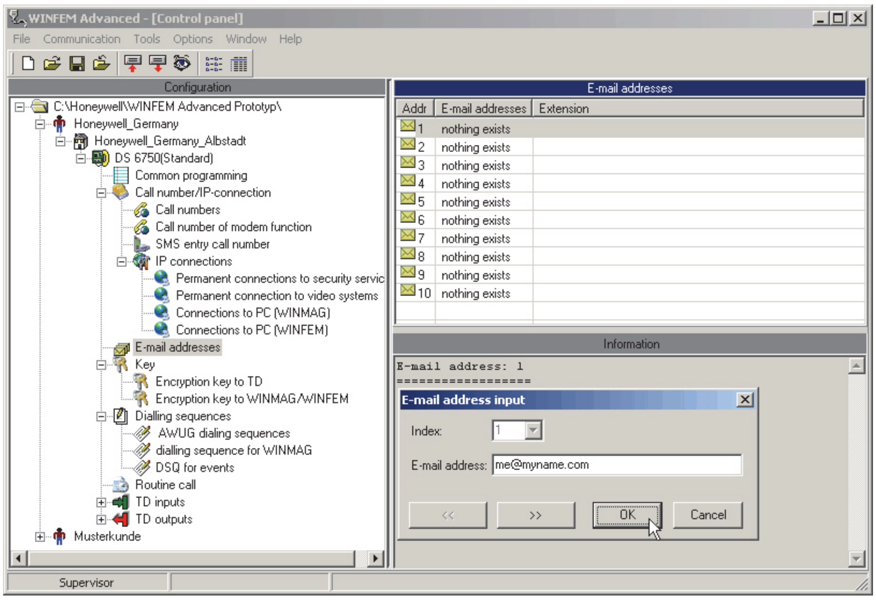
Trigger IP3 [Passwort]/[Path]/[Destination IP]
[Path] -> e Ethernet, g GPRS
[Destination IP] -> IP address of the WINFEM station, numerical or URL

Example: Trigger IP3 123456/e/192.168.188.2

After the SMS is received by the transmission device, the password for WINFEM IP connection 3 is checked. Next, the transmission device establishes an IP connection using the connection data in the SMS, namely [Path] and [Destination IP], and transmits the corresponding Id. no. to the WINFEM station for identification. Access from this station is now enabled.


WINFEM
SMS
SMS
Trigger
DSL Router
Configured for remote access
(Port forwarding)
DSL Router
Ethernet
Internet
GPRS
Connection via cellular network
RFW
DS 6700 / DS 6750 with RFW 4000

9. E-mail addresses


WINFEM Advanced - [Control panel]
File Communication Tools Options Window Help
Configuration
E-mail addresses
Information
Supervisor
<< >> OK Cancel

- C:\Honeywell\WINFEM Advanced Prototyp\
  - Honeywell_Germany
    - Honeywell_Germany_Albstadt
      - DS 6750(Standard)
        - Common programming
        - Call number/IP-connection
          - Call numbers
          - Call number of modem function
          - SMS entry call number
          - IP connections
            - Permanent connections to security servic
            - Permanent connection to video systems
            - Connections to PC (WINMAG)
            - Connections to PC (WINFEM)
        - E-mail addresses
        - Key
          - Encryption key to TD
          - Encryption key to WINMAG/WINFEM
        - Dialling sequences
          - AWUG dialing sequences
          - dialling sequence for WINMAG
          - DSQ for events
        - Routine call
        - TD inputs
        - TD outputs
  - Musterkunde

Addr	E-mail addresses	Extension
1	nothing exists	
2	nothing exists	
3	nothing exists	
4	nothing exists	
5	nothing exists	
6	nothing exists	
7	nothing exists	
8	nothing exists	
9	nothing exists	
10	nothing exists	

```
E-mail address: 1
=================
```

E-mail address input

Index: 1

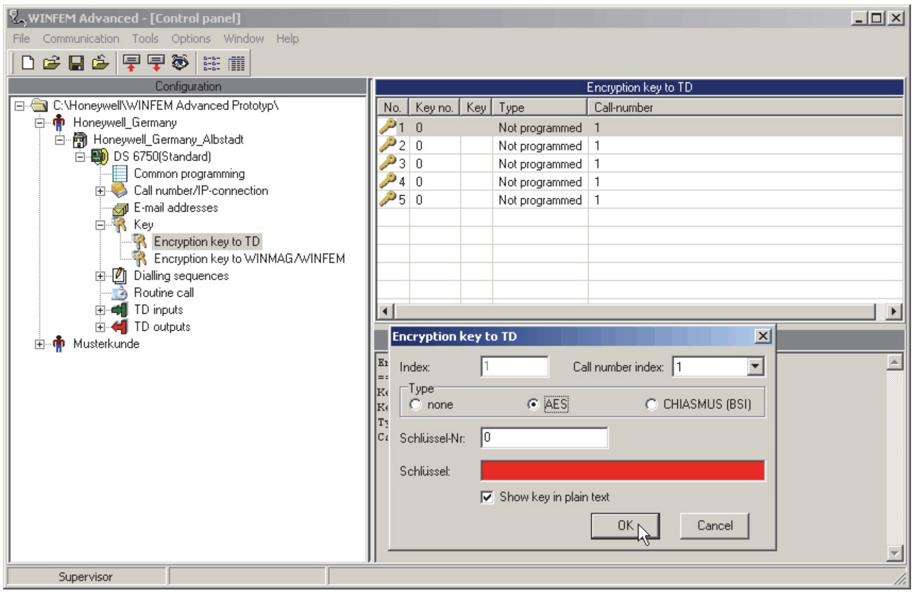
E-mail address: me@myname.com

It is possible to store up to 10 e-mail addresses.

9.1 Overview of e-mail notification

E-mail notification via:	DS 6700	DS 6750
PSTN PPP access	-----	possible
Ethernet	possible	possible
RFW-3000 / RFW-4000 via GPRS	-----	possible
RFW-3000 / RFW-4000 via SMS over GSM Modem to e-mail	possible	possible

10. Key


WINFEM Advanced - [Control panel]
File Communication Tools Options Window Help
Configuration
Encryption key to TD
Supervisor
OK Cancel

- C:\Honeywell\WINFEM Advanced Prototyp\
  - Honeywell_Germany
    - Honeywell_Germany_Albstadt
      - DS 6750(Standard)
        - Common programming
        - Call number/IP-connection
        - E-mail addresses
        - Key
          - Encryption key to TD
          - Encryption key to WINMAG/WINFEM
        - Dialling sequences
        - Routine call
        - TD inputs
        - TD outputs
  - Musterkunde

No.	Key no.	Key	Type	Call-number
1	0		Not programmed	1
2	0		Not programmed	1
3	0		Not programmed	1
4	0		Not programmed	1
5	0		Not programmed	1

Encryption key to TD

Index: 1 Call number index: 1

Type: ○ none ● AES ○ CHIASMUS (BSI)

Schlüssel-Nr: 0

Schlüssel:

☑ Show key in plain text

It is possible to store 5 different keys for encrypted transmission to the transmission control unit (receiving control panel at the security service). Regardless of this, another 5 different keys can be stored for encrypted data transmission between WINFEM / WINMAG and the transmission device.

10.1 Key to transmission control unit

10.1.1 Key number

The key number is the defined name of the key. This key number is communicated to the receiving device during or before exchange of encrypted data so that it can use the correct key for encoding and decoding the data.
It has to be ensured that both communication partners (transmission device and receiving device) have the same key with an identical key number.
The use of identical key numbers for different keys is not allowable.
Permissible values for the key number: 1 - 65534

10.1.2 Key

The transmission devices support different encryption algorithms:

1. CHIASMUS (BSI) (DS 6750 only)
2. AES

Both algorithms consist of a symmetrical process, but with different key lengths. CHIASMUS generally uses a 160 Bit key (40 characters in hexadecimal code), whereas AES works with a 128 Bit key (32 characters in hexadecimal code).

- Generate random key
  WINFEM offers the following option for generating a random key:
  A context menu is displayed by clicking with the right mouse button within the input field. Clicking on the menu item "Create random key" launches an additional program to generate a random key.

- Call number index
  If the alarm receiver supports automatic key assignment, then this is the call number which can be used to request a new key (see Section 10.1.3).

10.1.3 Automatic key assignment

The transmission devices support automatic key assignment by the control center: This method of key assignment is preferred over manual entry because it is less error prone than manual entry.
The following procedure is required for automatic key assignment:

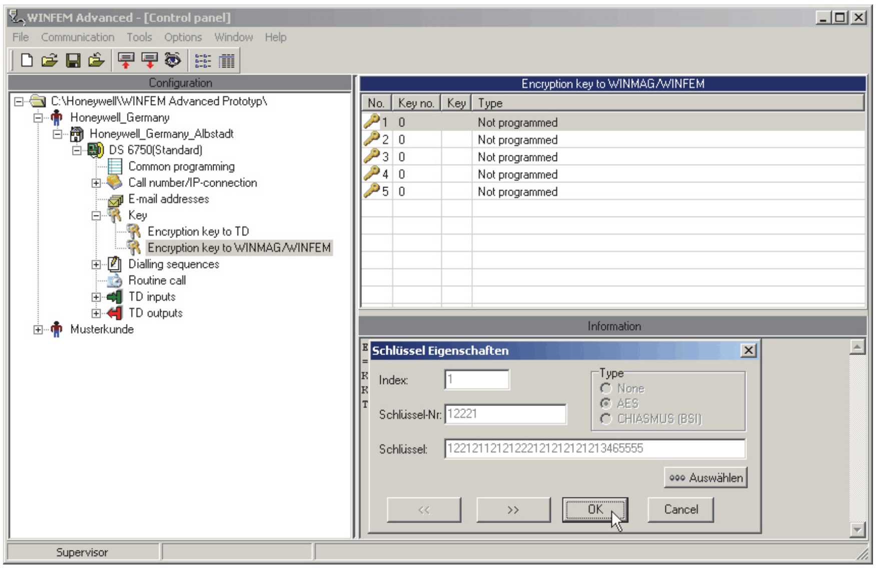
Prerequisite: A second transmission path is available in addition to the IP network.

When entering the connection data (IP address for the dedicated connection or IP address for demand-actuated connection), only one key index is used, for which neither a key number nor a key is programmed.

A key has to be requested once using the service function "pick up transmission control unit key" (in the "System" context menu, see also Section 20.3) for encrypted data transfer with the alarm receiving device (control center).
The transmission device first establishes a connection via the second path to the control center and requests a key. The call number assigned to the index is used as the call number.
All other key requests and key transmissions are then carried out automatically via control command from the transmission control unit.

10.2 Key to WINMAG (DS 6750 only) / WINFEM

The keys used here are used for encrypted data transmission between WINFEM/WINMAG and the control panel or the transmission device Programming of the keys is carried out in the same manner as described in Section 4.3.2 for connecting TCP / IP.



Encryption key to WINMAG/WINFEM

No.	Key no.	Key	Type
1	0		Not programmed
2	0		Not programmed
3	0		Not programmed
4	0		Not programmed
5	0		Not programmed

Schlüssel Eigenschaften

Index: 1

Schlüssel-Nr: 12221

Type: ○ None ● AES ○ CHIASMUS (BSI)

Schlüssel: 1221211212122212121212121213465555

10.2.1 Key number

The key number is the defined name of the key. This key number is communicated to the receiving device during or before exchange of encrypted data so that it can use the correct key for encoding and decoding the data.
It has to be ensured that both communication partners (WINFEM and transmission device) have the same key with an identical key number.
The use of identical key numbers for different keys is not allowable.
Permissible values for the key number: 1 - 65534

10.2.2 Key

CHIASMUS (BSI) (DS 6750 only)
AES

Both algorithms consist of a symmetrical process, but with different key lengths. CHIASMUS generally uses a 160 Bit key (40 characters in hexadecimal code), whereas AES works with a 128 Bit key (32 characters in hexadecimal code).
The entry must be hexadecimal. Possible characters are 0 - 9 and A - F.

- Generate random key

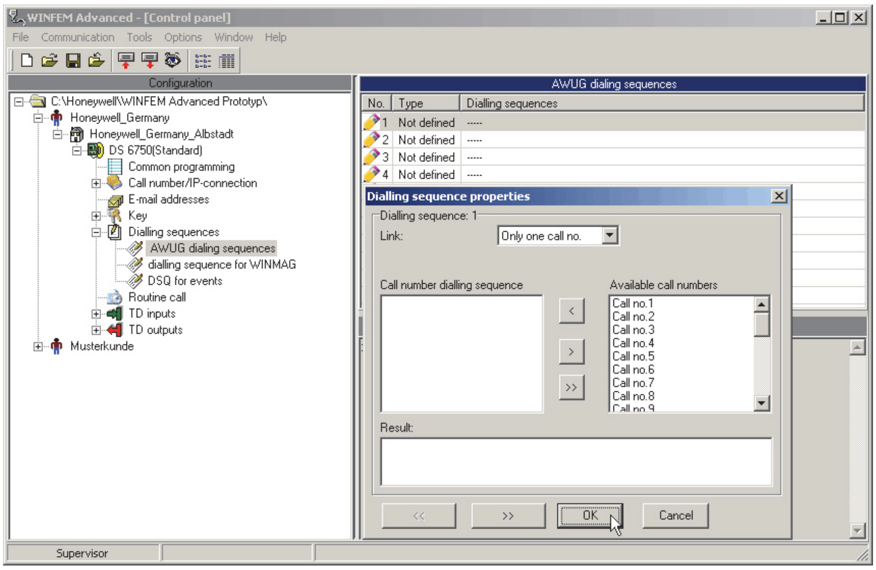
  WINFEM offers the following option for generating a random key:
  A context menu is displayed by clicking with the right mouse button within the input field. Clicking on the menu item "Create random key" launches an additional program to generate a random key.

10.2.3 Key editor

The button ooo is used to start the key editor.
This editor can be used to select an existing key for transmission. In addition to this, new keys can be created and stored in the key database. Further notes on the key editor are described in Section 4.3.2.

EN The remote access for WINFEM must be set up with AES encryption (see chapter 8.4.1).

11. Dialing sequences



No.	Type	Dialling sequences
1	Not defined	-----
2	Not defined	-----
3	Not defined	-----
4	Not defined	-----

Dialling sequence: 1

Link: Only one call no.

Available call numbers: Call no.1, Call no.2, Call no.3, Call no.4, Call no.5, Call no.6, Call no.7, Call no.8, Call no.9

Dialing sequence programming is subdivided into other subgroups. When you click on the +-symbol in the configuration window, the tree structure is expanded and shows the individual subgroups:

- AWUG - dialing sequences
- Dialing sequences for WINMAG
- DSQ for events (device-specific events)

When you click on the individual subgroup, the individual parameters (dialing sequence type, call number assignment) are displayed in the status window.
When you double click on the dialing sequence in the status window, the individual configuration menu opens.

A dialing sequence contains call numbers of users and controls the dialing/transmission behavior. The assignment of the dialing sequence is made during the configuration of the detector groups.

For dialing sequences allocated to dedicated line connections, the dedicated line connection should usually be entered as the first user.

11.1 AWUG - dialing sequences

It is possible to define a max. of 8 different dialling sequences. Up to 10 call numbers (users) can be assigned to each dialling sequence. Assignment of the individual dialing sequences is carried out in the "Message groups" and "Inputs" configuration menu and also in the configuration menu for the detector group configuration menu "IACP outputs" and "IACP functional groups outputs".

The dialing behavior can be specified in the "Link" selection window of the configuration menu “Dialing sequence properties". The following link options are available:

In the case of redundant connections, both numbers must be parametrized within the dialing sequence as an "or" logic operation.

11.1.1 One call number only

Transmission is carried out to one of the users from the assigned call numbers / destination address batch. As soon as the relevant message has been transmitted to one of the assigned users, there will be no other dialing/transmission concerning the current criterion. Dialing is carried out in the same order as the users are stored in the address batch. In case of non availability, the dial-up for each user that is stored is repeated 12 times. The dial-up repetition is as follows:

1st to 3rd dialing with 5 sec. pause
4th and 5th dialing with intervals of 10 sec.
6th and 7th dialing with intervals of 20 sec. each
8th and 9th dialing with intervals of 30 sec. each
10th to 12th dialing with intervals of 60 sec. each
With dialing time, ringing time and intervals, it will take at least 5 minutes before a single cycle is processed.

11.1.2 One per group

This offers the possibility to split a dialling sequence among two separate user groups.
If this option is activated, the transmission is made to one user from the first group and one user from the second group. The dialing cycle is only terminated when a user from each group has been reached or when the max. number of admissible dialing attempts has been exceeded.

Example 1: In connection with the transmission of a message about a technical fault, the responsible control center is to be informed and, in addition, a SMS message is to be output to the responsible service staff.
The dialling sequence configuration could be as follows:
(´X1, call no.1,call no.5) group separation (call no.6, call no.7)

The representation in WINFEM in this case would be:
(X1 or call no.1 or call no.5) and (call no.6 or call no.7)
The first group in this example includes the control center access numbers and this control center is to have a dedicated line connection (X1). If the dedicated line connection to the control center is not available, the transmitter tries to reach it via numbers 1 or 5.
The second group contains the telephone/mobile phone numbers of the service staff . One of the two connections must be reached in any case, irrespective of whether a message can be transmitted to the control center.

Example 2: The transmission device is connected to two control centers via a dedicated line connection. Both control centers are accessible via demand-actuated PSTN connections in the event of failure of the dedicated line connection. Transmission is to be carried out to both control centers.
Possible dialing sequence configuration:
(X1, call no.1,call no.5) group separation (X2, call no.6, call no.7)

11.1.3 All call numbers

All call numbers / addresses must be reached.
Thus, it is possible to inform up to 10 users per event.

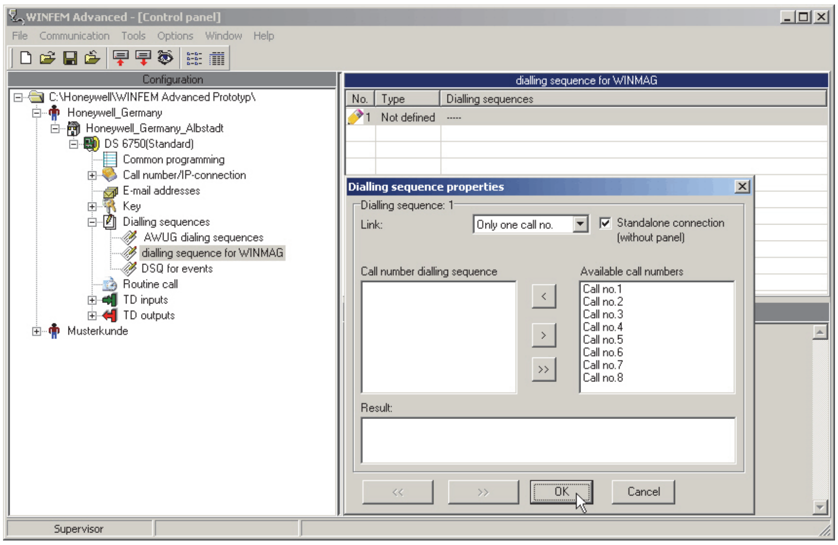
The dialing cycle is only terminated when each user has been reached or when the max. number of admissible dialing attempts for each individual user has been exceeded.

11.1.4 Call number dialing sequence

The assignment of the user to the dialling sequence is displayed in this window.
In the selection window "Available call numbers“, the call numbers / user addresses available for an assignment to a dialling sequence are displayed.

In order to include a call number into the dialing sequence, the number of the user must be selected in the "Available call numbers" window, then the < button must be activated.
It is also possible to select and include a user by double-clicking on the call number in the "Available call numbers" window.
The insertion of a "group separation" (one per group) is made in the same way.
When the >> button is actuated, the entire DSQ is deleted.
By selecting call numbers in the "Call number dialing sequence" window and
pressing the ">" button, individual participants can be removed. Double clicking on the call number in the "Call number dialing sequence" window will also remove the user.

11.2 Dialing sequences for WINMAG (DS 6750 only)



dialling sequence for WINMAG

No.	Type	Dialling sequences
1	Not defined	-----

Dialling sequence properties

Dialling sequence: 1

Link: Only one call no.

☑ Standalone connection (without panel)

Call number dialling sequence

Available call numbers: Call no.1, Call no.2, Call no.3, Call no.4, Call no.5, Call no.6, Call no.7, Call no.8

Result:

It is possible to transmit information in the IGIS alarm point format to decentralized WINMAG stations. Configuration is usually done by means of the operating units or by means of the WINFEM programming directly in the corresponding hazard detection control panel. One dialing sequence is available for this function. The only available configuration option is “One Call Number Only”. Any number of users from the “Call Number Modem Function” stack can be assigned.

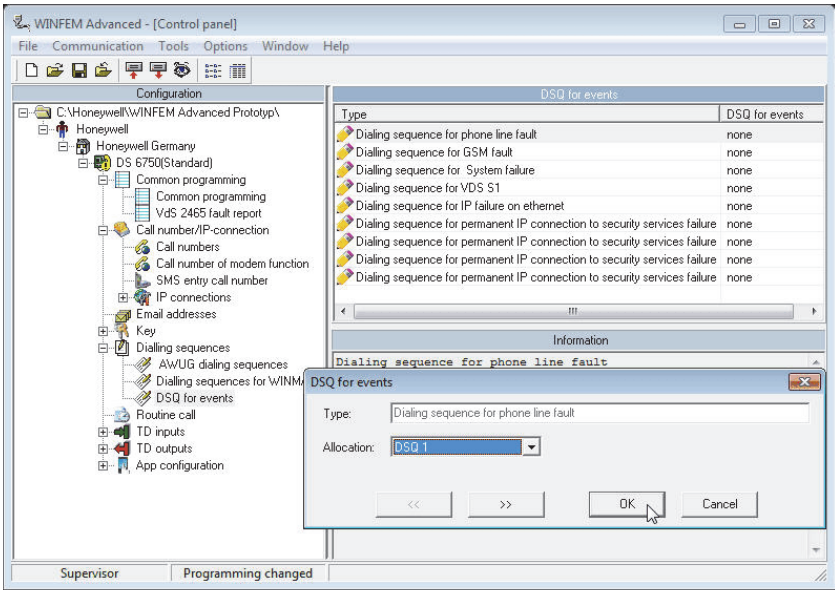
- The "Standalone connection (without panel)" check box

  If the transmission device is operated without downstream intruder alarm control panel and WINMAG connection is to be realized, then this check box is to be checked. This performance feature can be used to connect (external) WINMAG units.

11.2.1 Text routing channel

The text entered here will be stored in the event memory of the intruder alarm control panel upon activating this dialing sequence (Input field only visible when the transmission device is used as integration module with IACP).

11.3 DSQ for events (device-specific events)



DSQ for events

Type	DSQ for events
Dialing sequence for phone line fault	none
Dialling sequence for GSM fault	none
Dialling sequence for System failure	none
Dialing sequence for VDS S1	none
Dialing sequence for IP failure on ethernet	none
Dialing sequence for permanent IP connection to security services failure	none
Dialing sequence for permanent IP connection to security services failure	none
Dialing sequence for permanent IP connection to security services failure	none
Dialing sequence for permanent IP connection to security services failure	none

Information

Dialing sequence for phone line fault

DSQ for events

Type: Dialing sequence for phone line fault

Allocation: DSQ 1

In this window, dialing sequences are assigned to the individual device-specific events or faults. The dialing sequences already defined under "AWUG dialing sequences" are available for this purpose.

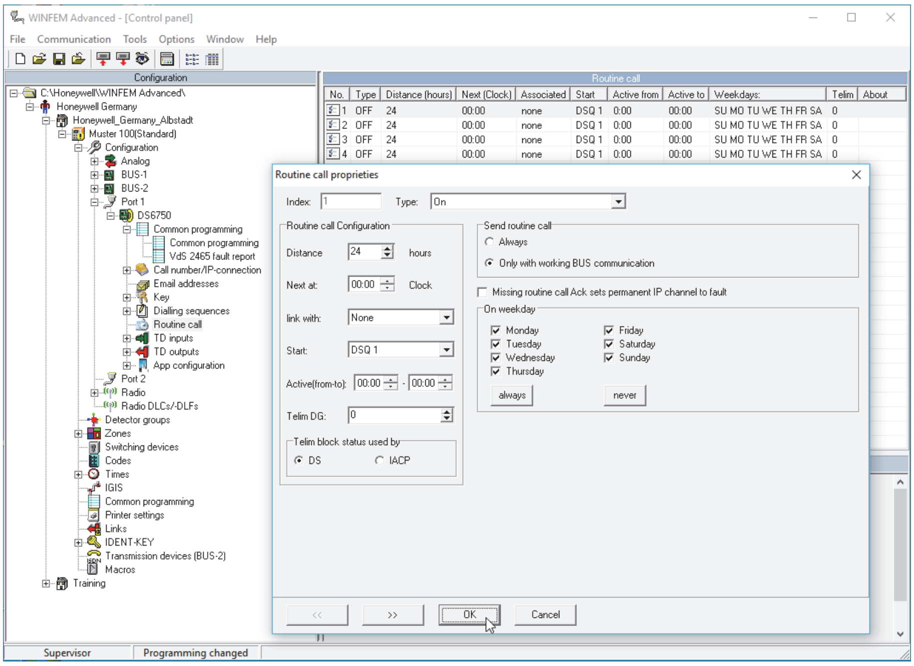
12. Routine call

The transmission device supports up to 4 independent routine call cycles.

VdS In case of configurations according to the VdS-guidelines, a cyclical test call must be transmitted to the individual receiver units. The transmission devices permit connection to several different emergency call centers / receiving devices. In addition to this, the transmission devices can simultaneously establish several dedicated line connections. Therefore, it might be necessary to implement separate independent routine call functions for individual control centers. In most cases, one routine call cycle is sufficient.

Each of the individual routine call groups can be configured individually, according to the relevant requirement profile. When you click on "Routine call" in the configuration window, the available routine call cycles and their configurations are displayed in the status window.

Double clicking on a routine call cycle will open the corresponding configuration menu.



Routine call

No.	Type	Distance (hours)	Next (Clock)	Associated	Start	Active from	Active to	Weekdays:	Telim	About
1	OFF	24	00:00	none	DSQ 1	0:00	00:00	SU MO TU WE TH FR SA	0	
2	OFF	24	00:00	none	DSQ 1	0:00	00:00	SU MO TU WE TH FR SA	0	
3	OFF	24	00:00	none	DSQ 1	0:00	00:00	SU MO TU WE TH FR SA	0	
4	OFF	24	00:00	none	DSQ 1	0:00	00:00	SU MO TU WE TH FR SA	0	

Routine call proprieties

Index: 1 Type: On

Routine call Configuration

Distance 24 hours

Next at: 00:00 Clock

link with: None

Start: DSQ 1

Active(from-to): 00:00 - 00:00

Telim DG: 0

Telim block status used by: ● DS ○ IACP

Send routine call: ○ Always ● Only with working BUS communication

□ Missing routine call Ack sets permanent IP channel to fault

On weekday: ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

always never

12.1 Routine call type

Activation/deactivation of the individual routine call cycle is made via the drop-down list field "Type". Only after routine call type "on" has been selected and switched on it is possible to continue with the configuration of the other parameters.

Default setting: off

- Off

Routine call is not active.

- On

Routine call configuration for demand-actuated connections if no alternative radio path is available or for dedicated line connections if no reduced routine call interval is required between the individual test calls if the dedicated connection fails.

- Alternating routine call GSM <-> no GSM

This setting is only required when using an alternative GSM path (dual path signaling backup with the RFW-4000 / RFW-3000).

In the case of an alternating routine call, the individual test calls are alternately made via GSM and the "non-GSM transmission path". Depending on the programmed dialing sequence, this can be the PSTN transmission path or an on-demand IP connection path, for example. Since, according to VdS standards, the individual transmission paths have to be checked for functionality (by means of a test call) within 24 hours, a time interval of 12 hours should be set between the individual routine calls (see routine call interval).
If "alternating routine call" is programmed, the transmission path to be followed by the next test call must be defined (if necessary, in consultation with the relevant control room operator). This is the purpose of the "Next Transmission starts with" ("non-GSM" <-> "GSM") selection option, which is only available with this operating mode. When designing the selected dialing sequence, it must be ensured that both transmission paths are assigned. The numbers assigned to the respective transmission path to be checked are used to transmit the routine calls.
Another option for VdS-compliant routine call design is to use two routine call cycles. The standard operating mode for routine calls can be used in this case. (Switched on). The interval can be set to 24 hours. However, it must be noted that, in this case, different dialing sequences corresponding to the relevant transmission path must be used.

- Routine calls with TCP/IP failure expansion
It is also useful to generate a cyclic test call at 24-hour intervals for dedicated connections.

In the event of a failure of the dedicated TCP/IP connection, some control rooms require test calls at short intervals using the still functioning alternative path.

If this operation mode is used, an additional configuration menu will be opened. If the "Send routine call immediately after IP failure" checkbox is enabled, the test call cycle is started immediately after a failure is detected in the dedicated connection. If the checkbox is not enabled, the first test call only starts after the time set in the "Interval" field. The intervals between the routine calls in the event of a failure in the dedicated connection can be set here:: Permissible value range: 1 - 254 minutes.
In addition, a dialing sequence for the "extended failure" must be specified. This can be identical to the basic extended failure used for the relevant routine call cycle (configuration point: "Start"). It is also possible to select a different extended failure for this case.

The following allocations apply: Routine call no. 1 on failure of the 1st TCP / IP connection
Routine call no. 2 on failure of the 2nd TCP / IP connection

Example: Standard DSQ1 with the configuration IP1, Rn1, Rn2 for routine call (index) 1
When the dedicated line connection is working properly, test transmission is carried out according to the time specifications (e.g. at 24-hour intervals).
If DSQ 1 is also used on failure of the dedicated connection (IP1), then the failure test messages are sent to Rn1 or Rn2 (depending on reachability of the call numbers).

12.2 Routine call configuration

12.2.1 Routine call interval

This programming defines the number of hours between routine calls. According to the VdS-guidelines, an interval of 24 hours per transmission path is sufficient. It is, however, possible to define the interval between routine calls individually. Possible values: 0 - 255 hours.

If the interval between routine calls is set to 0, this that has the same effect as "routine call off".

12.2.2 Next routine call at at

Is used to define the routine call hours. The next routine call will be made at the time specified here. The following test calls will be made in accordance with the interval (distance) specified above.

When programming the routine call configuration new again, the time for the parameter “next call at” is only reconfigured in the transmission device, when another parameter is changed within the routine call configuration. This measure prevents a failure of the routine call if the parameter of the “next call at” of the routine and the current time are far apart.

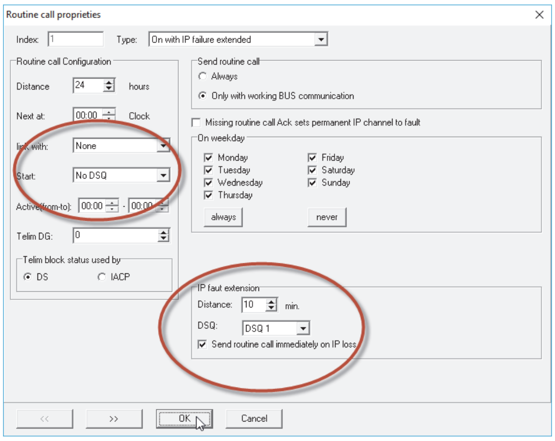
12.2.3 Link with detector groups/inputs

Provides the possibility to make the generation of routine calls dependent on detector group states.
Example: A link is established to detector 2:
A routine call to the set time occurs only if detector group 2 is in triggered condition at this point.

12.2.4 Dialing sequence for the routine call

A DSQ from the available dialing sequence batch can be selected .

The "no DSQ" selection can **only** be rationally **used in combination** with **routine call type "IP failure extended"**. No routine calls are transmitted as long as there is a dedicated TCP/IP connection to the security company.
In the event of a failure of the dedicated TCP/IP connection, test calls will be transmitted at short intervals using a dialing sequence still be defined (dialing sequence for "IP failure extended". For this an additional configuration menu will be opened. This extended failure can be identical to the extended failure used for the respective routine call cycle, but should contain a call number of an analog telephone connection to the security company. The intervals between the routine calls in the event of a failure in the dedicated connection should be set in this configuration menu:
Permissible value range: 1 - 254 minutes.


Routine call proprieties

Index: 1 Type: On with IP failure extended

Routine call Configuration
Distance 24 hours
Next at: 00:00 Clock
link with: None
Start: No DSQ
Active(from-to): 00:00 - 00:00
Telim DG: 0
Telim block status used by
● DS ○ IACP

Send routine call
○ Always
● Only with working BUS communication

☐ Missing routine call Ack sets permanent IP channel to fault

On weekday
☑ Monday ☑ Friday
☑ Tuesday ☑ Saturday
☑ Wednesday ☑ Sunday
☑ Thursday

IP faut extension
Distance: 10 min.
DSQ: DSQ 1
☑ Send routine call immediately on IP loss

12.2.5 Active periods

This field provides the option to specify that test calls are made only at certain times of the day. Example: Test calls are to be made only during the night, from 21:00 h to 06:00 h. During this period, the interval between the individual test calls is to be 3 hours. Possible configuration for this setting:
Routine call distance: 3 hours Active from 21:00 h to 06:00 h.

12.2.6 Telim channel for routine calls

Contains the assigned DSQ call numbers of Telim receiving centers - the corresponding Telim channel "(0 - 16) must be assigned, if necessary in co-ordination with the control center operator. This is performed in the input field "Telim reason" (Telim message reason).

12.2.7 Telim block status used by

Selection, whether the state of the Telim block (Telim block status of the 8 inputs) is transmitted from the transmission device or from the panel coupled by RS-232 interface (only Telim Protocol).

12.2.8 Sending a routine call

Choose whether a routine call is only to be transmitted when the bus communication is working with the downstream intruder control and indicating equipment. Bus communications are monitored on the RS-232 interface with VdS protocol 2465 to the connected intruder control and indicating equipment.

VdS n the case of a VdS-compliant configuration, the sending of routine calls is only to be programmed if bus communications are functioning.

12.2.9 Failure to acknowledge a routine call influences forced actuation

Each routine call is acknowledged by the receiving equipment. If the checkbox "Failure to acknowledge a routine call influences forced actuation" is enabled, the lack of an acknowledgment will be included in the forced actuation of the downstream intruder control and indicating equipment.

If the routine call can not be transmitted because the acknowledgment of the receiving equipment is missing, the transmission device behaves as if the associated dedicated IP connection is disturbed.
Routine call 1 -> dedicated IP connection 1 (e.g. Receiving Centre Transceiver RCT 1)
Routine call 2 -> dedicated IP connection 2 (e.g. Receiving Centre Transceiver RCT 2)
Routine call 3 -> dedicated IP connection 3 (e.g. Receiving Centre Transceiver RCT 3)
Routine call 4 -> dedicated IP connection 4 (e.g. Receiving Centre Transceiver RCT 4)
The non-active (disturbed) IP connection is included in the positive drive condition of the connected intruder alarm panel.

ℹ Observe for this programming point the chapter “IP transmission of messages”.

12.2.10 Week days

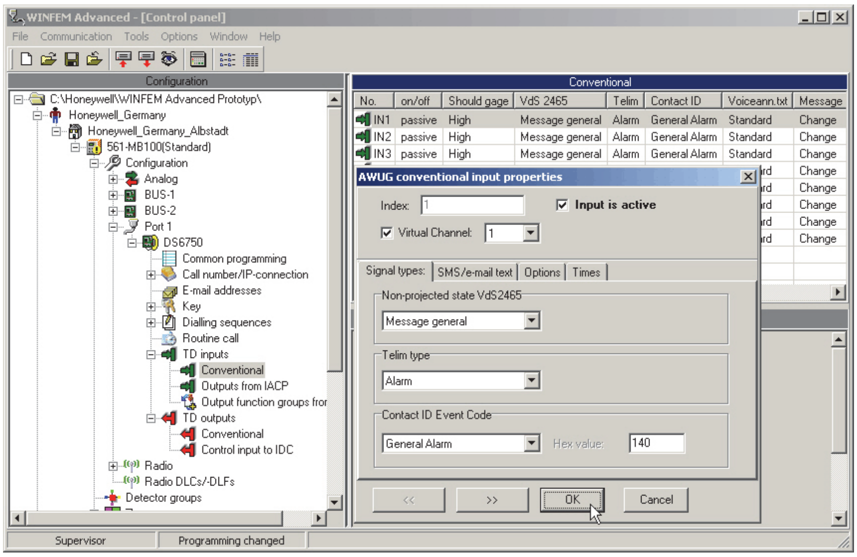
It is possible to specify that test messages are to be transmitted only on certain days of the week.

13. Transmission of messages

If the transmission devices are operated in stand-alone mode, they each have the 8 conventional inputs. When control panels are connected via the RS-232 interface (IACP RS-232 mode), 100 virtual inputs are available for the transmission device, which are designated as "Outputs from IACP". In addition, 100 “Output function groups from IACP" are available.

13.1 Inputs (detector groups)

The device has 8 conventional inputs (E1 - E8). Each input (detector group) can be configured individually, according to the relevant requirement profile.
When clicking on "inputs" in the configuration window, the status window displays the available inputs and the corresponding configuration.
Double clicking on an input will open the corresponding configuration menu.



Conventional

No.	on/off	Should gage	VdS 2465	Telim	Contact ID	Voiceann.txt	Message
IN1	passive	High	Message general	Alarm	General Alarm	Standard	Change
IN2	passive	High	Message general	Alarm	General Alarm	Standard	Change
IN3	passive	High	Message general	Alarm	General Alarm	Standard	Change

AWUG conventional input properties

Index: 1 ☑ Input is active

☑ Virtual Channel: 1

Signal types: | SMS/e-mail text | Options | Times

Non-projected state VdS2465: Message general

Telim type: Alarm

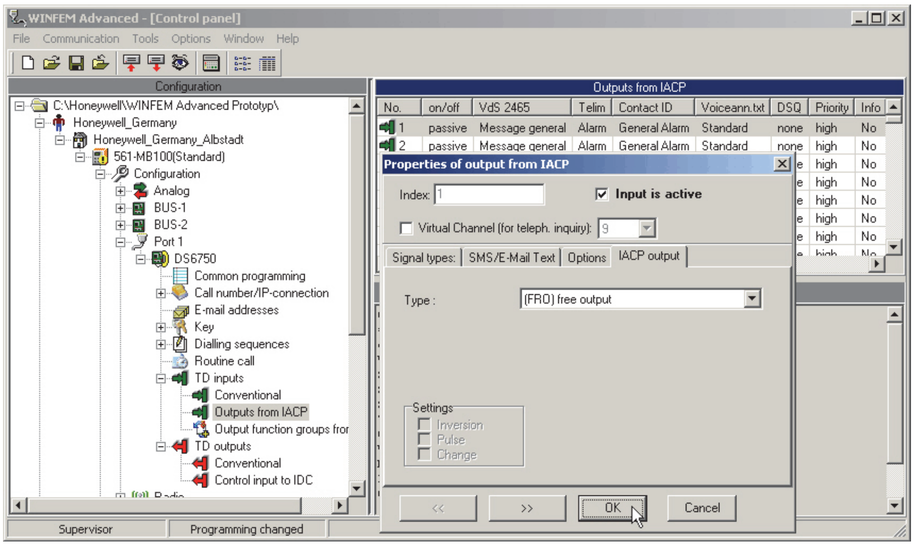
Contact ID Event Code: General Alarm Hex value: 140

<< >> OK Cancel

13.2 Inputs (detector groups) in IACP RS-232 mode

Each of the 100 inputs can be configured individually, according to the object-specific requirements. The same procedure can be used here as in configuration of the conventional inputs of the transmission device. Use of conventional signal inputs is also possible independent of the virtual inputs.
The intruder alarm control panel provides 100 virtual outputs, which are "virtual inputs" for the transmission device. Programming of these "virtual signal inputs" is similar to configuration of the transmission device's conventional inputs.

By default, all IACP outputs are "free" (free outputs), i.e. no output signal has been assigned to them. The corresponding output signal type is defined via the drop-down list field "Type". For further information on programming the output signals, please refer to the programming instructions for the hazard detection panel.



Outputs from IACP

No.	on/off	VdS 2465	Telim	Contact ID	Voiceann.txt	DSQ	Priority	Info
1	passive	Message general	Alarm	General Alarm	Standard	none	high	No
2	passive	Message general	Alarm	General Alarm	Standard	none	high	No

Properties of output from IACP

Index: 1 ☑ Input is active

☐ Virtual Channel (for teleph. inquiry): 9

Signal types: | SMS/E-Mail Text | Options | IACP output

Type : (FRO) free output

Settings
☐ Inversion
☐ Pulse
☐ Change

<< >> OK Cancel

13.2.1 Input is active

Only inputs that are marked as active will be evaluated by the transmission device.

Passive inputs (detector groups) can neither be configured nor evaluated. No event log entries are made for these inputs either.

This will require that inputs that are to result in activation of the transmission device or inputs that are to be used for other functions (such as linking to another input) have to be marked as active.

13.2.2 Virtual channel

In connection with the AWAG function of the transmission device, this programming is used for assigning the voice text which is transmitted when the relevant input is activated. The transmission device has 9 virtual channels which influence the paging device that is integrated in the device (AWAG function).
The number of available detector groups or inputs may be significantly higher (in case of extension with BUS 2 input modules). Therefore it is possible to allocate the individual inputs to a virtual channel (voice channel). A total of 9 different spoken texts (= voice channels) can be assigned. In the corresponding selection window, one of the remaining available virtual channels of the respective input can be assigned. It is not possible to assign a virtual channel to several inputs.

The number corresponding to the virtual channel is used for the announcement if no individual text was entered.

Example:
Detector group 5 is assigned to virtual channel 1. "12345" has been stored as the "own call number". No individual texts have been stored.
In the case of trouble in detector group 5, the following announcement is issued:
"Attention, this is an announcement from information system 12345, input 1 has been triggered. Repeat by pressing the star key"

For more information on the language functions, refer to Section 20.6.

13.3 Signal types tab

13.3.1 Signal type not VdS 2465 projected state

The input can be assigned to the signal type, which is communicated to the receiving device on transmission. (fire, burglary, hold-up, etc).
All signal types defined in VdS 2465 are offered for selection in the selection window. Some manufacturers of receiving stations have defined their own signal types in addition to the VdS definitions.

If a manufacturer-specific signal type is to be used, "HEX value" must be defined as signal (bottom entry in the selection list). Another selection window will then open for assigning the value. Admissible range of values: 1 – 7F.

13.3.2 Telim type

Only relevant if a dialling sequence including a Telim user is assigned to the detector groups. The signal types supported by the Telim protocol are available.

Due to the Telim protocol, only the "Outputs from IACP" 1 to 16 may be programmed for Telim receiving centers. "Outputs from IACP” greater than 16 will always be transmitted as reason 16.

13.3.3 Contact ID Event Code

A desired signal type which is communicated to the receiving center during a transmission via a Contact ID Event Code can be assigned to the output from IACP here.
The frequent signal types defined according to the Contact ID Event Code are offered for selection.

If another signal type is to be used, "HEX value" must be defined as signal type (bottom entry in the selection list). Another selection window will then open for assigning the value. Admissible range of values: 000-FFF (Hex digits B,C,D,E,F are also supported).

13.4 SMS/e-mail text tab

13.4.1 SMS/e-mail text

Here you can define the text which is to be transmitted to mobile phones or pagers as an SMS or e-mail message when the transmission device is activated via the relevant input.
It is possible to specify a text for the two input states that are possible (should/should not resp. projected / non-projected).

The max. length is 40 alphanumeric characters /text.
If no text is assigned to the input and SMS transmission is provided for, a standard text generated by the transmission device will be transmitted. The triggered input is transferred here as address number.
In any case, the text stored here has a higher priority than the detector group text that is transmitted from the control panel to the transmission device according to the programming (Section 6.1.1.9). You can store texts for certain inputs which are then transmitted from case to case.

13.4.1.1 Also send the text to the control center

With transmission protocol VdS 2465, it is possible to send the message texts to the receiving stations as well.

13.5 Options tab

13.5.1 Projected state with

The projected state is the state in which the input is in non-triggered state. Each input can be assigned an individual physical projected state. The following projected states can be assigned:

- High level

  The inputs are connected with a pull-up resistor (12.1 KOhms to 12 V operating voltage). In this configuration, the open input is in non-operative status.
  In the case of short circuit with 0 V (GND) or conclusion of the input with 12.1 KOhms, the input takes on the "triggered" or "trouble" state.

- Low level

  In the case of short circuit with 0V, the input is in non-triggered (undisturbed) state.

- 12.1k termination

  The input works as a resistance monitored differential detector group if programmed in this way. If the input is terminated with a resistance of 12.1 KOhms, then it is in non-operative status (non-triggered status). An change to the terminating resistor of + / - 40% of the projected value results in a malfunction of the input and thus to actuation.

13.5.2 Start dialing sequence

Here you can define the dialing sequence which is to be processed when the transmission device is activated by the relevant input. In the drop-down list field "Start DSQ”, a dialling sequence can be selected from the dialling sequences defined before.

It is also possible to allocate no dialing sequence. In this case, the input is evaluated by the transmission device and the event is entered in the event memory if the input state is changed. This type of configuration makes sense, for example, if the input is used as an input variable for connection to another input or **in conjunction with the programming of the smartphone app for transmitting or display of output signals**.

13.5.3 Priority

The priority class that is transmitted to the receiving station is defined here. Normally, priority "high" is used. Another priority class should only be used if this is requested by the control center operator. This parameter is also considered during evaluation and processing by the transmission device. So it is e.g. possible to assign a lower priority to technical messages than to alarms.

13.5.4 Detector group linking

It is possible to make transmission of an input dependent on the state of another input. The linking functions always refer to the "non-projected state" of the respective input.

If no link is required, the input must be linked with itself (default setting).

The linking function can result in very complex activation behavior of the transmission device. Multiple links can be defined and the active and blocking periods allocated to the input used as an input variable are included in the link. If a link is programmed, transmission takes place on activation of the input only if the input specified under "Linked to" is also in the "triggered" state.

The input used as the input variable does not necessarily have to be associated with a dialing sequence. The associated delay times, blocking periods and active periods are taken into account however.

Example:
Input 1 is programmed with a delay time of 20 seconds and is linked to itself (EG1). No dialing sequence is assigned (Start: "No DSQ").

Input 2 is assigned to DSQ1 and a link with input 1 results.
This results in the following activation behavior:
Input 1 can not be transmitted, input 2 is transmitted only if input 1 has been triggered for the duration of the delay time and the triggered state of input 1 still exists at time of activation of input 2.
If input 2 is triggered before the delay time of input 1 has expired, no transmission is carried out.

13.5.5 Voice announcement text

Either the standard vocabulary or an announcement text 1 -4 can be assigned as the voice announcement text. Further information is provided in Section 20.6.

13.5.6 Signal detector group (detector group related signaling)

Assignment is made here as to whether the detector group has an effect on the potential-free "output signal". See Section 6.2, "Signaling tab“.

Example: The signaling output includes the configuration "for camera control".
Detector group 2 is used to transmit technical messages, e.g. pertaining to air conditioning system failure.
The "Signal detector group" check box should not be checked because a technical fault should not cause camera activation.
For a detector group that serves as a "hold-up detector group", "Signal detector group" has to be activated because camera recording should take place if this detector group is triggered.

13.5.7 Include GPS information in transmission

This can be used to specify whether the GPS coordinates should be included in detector group transmission if a GPS mouse is connected.

13.5.8 Message in the case of status change or fault

If "Message in case of fault" is programmed, transmission is only carried out if the input is actuated. A change of the input from fault to no fault state does not result in activation of the transmission device.

If "Message in case of state change" is set, then transmission is carried out every time the status of the input changes and therefore for both triggering and resetting.

13.6 Times tab

13.6.1 delay

If no delay time is entered (default setting), then transmission for the input is carried out according to the VdS guidelines. A fault is evaluated as an actuation criterion and results in activation (note debounce time of 200 ms).
If the input is assigned a time delay, then activation occurs only when the input is in the fault state for longer than the period of time defined here. The delay time is only relevant to the actuation message, any "no fault message" of the current input is transmitted without delay.

VdS Programming of a delay time is not in accordance with VdS.

13.6.2 Blocking time

This can prevent permanent activation from taking place by criteria that provide no stable output signal.

VdS No blocking time can be set for VdS compliant use.

Transmission of the input is only carried out again once the set blocking time has expired. The blocking time starts when the input is actuated.
Possible no-fault message from the input can take place before the blocking time transpires. However, renewed actuation is only possible once the set time has transpired.

13.6.3 Active from - to

The active time is used to place a limit on the time that messages are sent for individual inputs.
Example: Actuation of input 03 should only result in transmission between 6 p.m. and 6 a.m.

The input behaves passively outside the active periods. If no time restrictions are required "active from 00:00 to 00:00" has to be entered!

13.7 IACP output tab

By default, all IACP outputs are "free" (free outputs), i.e. no output signal has been assigned to them. The corresponding output signal type is defined via the drop-down list field "Type".

The corresponding functionality for the transmission is assigned to this IACP output via the tabs in the same was as programming of conventional inputs. The only differences are in the programming of the Options tab. In total, transmission signal types for 100 IACP outputs can be assigned here.
For further information on programming the output signals, please refer to the programming instructions for the hazard detection panel.

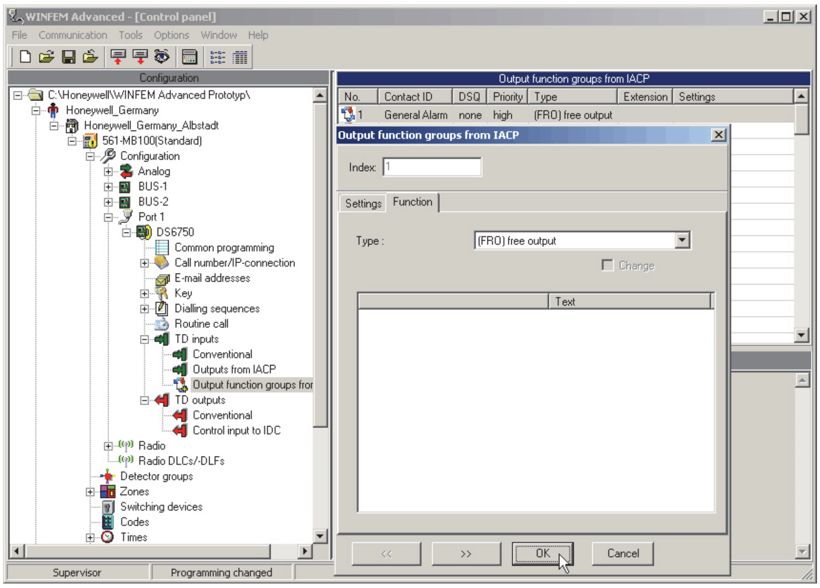
13.7.1 The Options tab

13.7.1.1 Assignment of a dialling sequence
Here you can define the dialling sequence which is to be executed when the transmission device is activated by the relevant output signal. In the drop-down list field "Start DSQ", a dialling sequence can be selected from the dialling sequences defined before.

13.7.1.2 Priority
The priority class that is transmitted to the receiving station is defined here.
Normally, priority "high" is used. Another priority class should only be used if this is requested by the control center operator. This parameter is also considered during evaluation and processing by the transmission device. So it is e.g. possible to assign a lower priority to technical messages than to alarms.

13.7.1.3 Voice announcement text
Either the standard vocabulary or an announcement text 1 -4 can be assigned as the voice announcement text. Further information is provided in Section 20.6.

13.8 Output function groups from IACP in IACP RS-232 mode (only for Contact ID)



No.	Contact ID	DSQ	Priority	Type	Extension	Settings
1	General Alarm	none	high	(FRO) free output		

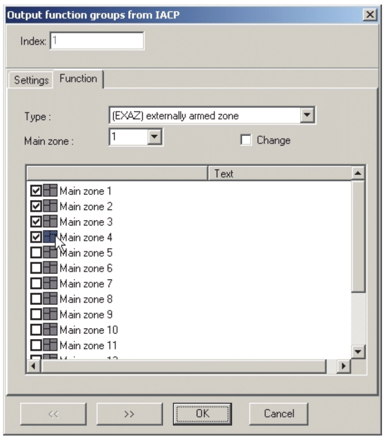
Index: 1

Type : (FRO) free output

Each of the 100 input function groups in the DS 6750 transmission device can be programmed individually, according to the individual object-specific requirements. The function groups permit fast and comprehensive programming of the transmission parameters. When you click on “Output function groups from IACP" in the configuration window, the available inputs and their configuration are displayed in the status window. The corresponding configuration menu is opened by double clicking on one Output function group from IACP. The intruder alarm control panel provides 100 virtual function group outputs, which are "virtual inputs" for the transmission device.

13.8.1 The Function tab

The "Function" tab is used for defining a function group from all possible output signals provided by the IACP. In a second step, any signal type can be assigned to this function group via the "Settings" tab. When the check box “Change” is activated, a transmission will take place whenever there is a change of a criterion of the function groups, i.e. for each actuation and reset.
The IACP output signal type is selected via the drop-down list field "Type"; this signal type determines the actuation of a transmission for the main zones or detector groups of a function group. Active main zones or detector groups of a function group are defined by clicking the available check box.
A function group can have a maximum of 64 individual criteria (main zones or detector groups); but if all possible detector group output signals (512 detector groups max. for IACP 561-MB100) are to be implemented, other function groups (100 max.) must be defined, which are determined by a new start value (e.g. +64) of the main zone or detector group in the drop-down list field (numeric values).



Index: 1

Type : (EXAZ) externally armed zone

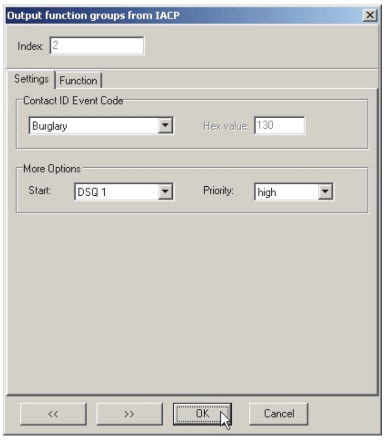
Main zone : 1 □ Change

☑ Main zone 1
☑ Main zone 2
☑ Main zone 3
☑ Main zone 4
□ Main zone 5
□ Main zone 6
□ Main zone 7
□ Main zone 8
□ Main zone 9
□ Main zone 10
□ Main zone 11

The relevant functionality for the transmission is assigned to the function detector group defined here via the tabs described below. In total, 64 output signals per signal type can be assigned to the 100 function groups. Section 21.2 contains an overview of the contents of the Contact ID transmission in case of function group programming.

13.8.2 The Settings tab

Here you can define the signal type which is assigned to the function group. This is the signal type which is communicated to the receiving center during transmission by means of a Contact ID Event Code.
The frequent signal types defined according to the Contact ID Event Code are offered for selection.



Index: 2

Contact ID Event Code

Burglary

Hex value: 130

More Options

Start: DSQ 1

Priority: high

If another signal type or a manufacturer-specific signal type is to be used for a signal type a Contact ID Event Code, "HEX value“ must be defined as signal type (bottom entry in the selection list). Another selection window will then open for assigning the value. Admissible range of values: 000-FFF (Hex digits B,C,D,E,F are also supported for Contact ID).

The dialing sequence which is to be executed when the transmission device is activated by the relevant function group is assigned in the drop-down list field "More Options". A dialing sequence from the AWUG dialing sequences defined before can be selected.

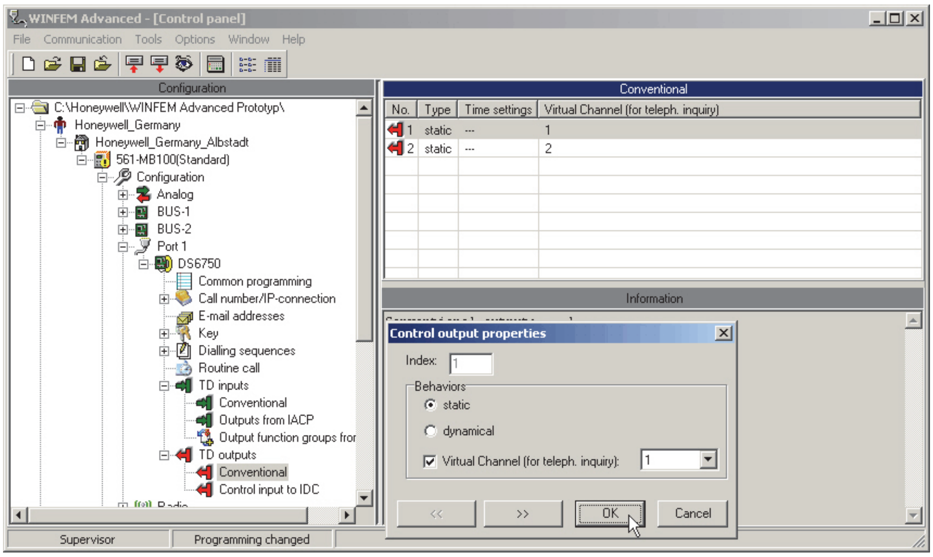
A transmission happens only to participants with assigned Contact ID protocol within the call number programming. All other call numbers will be ignored, I. e. no transmission will occur.

14. Remote control functions

If the transmission device is operated in stand-alone mode, they it has two control outputs. When control panels are connected via the RS-232 interface (IACP RS-232 mode), 40 virtual inputs are available, which are designated as "Control outputs to IACP".

14.1 Control outputs

The device is equipped with two semiconductor outputs (control output 1 and control output 2), which can be remote controlled with telephone keys via receiving devices from the NSL or in combination with voice transmission.
When you click on "Outputs" in the configuration window, the available control outputs and their configuration are displayed.
Double clicking on one control output will open the corresponding configuration menu.



Conventional

No.	Type	Time settings	Virtual Channel (for teleph. inquiry)
1	static	---	1
2	static	---	2

Control output properties

Index: 1

Behaviors
● static
○ dynamical
☑ Virtual Channel (for teleph. inquiry): 1

14.1.1 Switching behavior

Static: A separate command is required for switching the output on and off.
Dynamic: The switching command for "Switch on control output" causes activation of the respective output. No separate command is required for switching off. The output is automatically ("Time" selection window) returned to idle state (permissible value range 0.1 to 25.5 seconds).

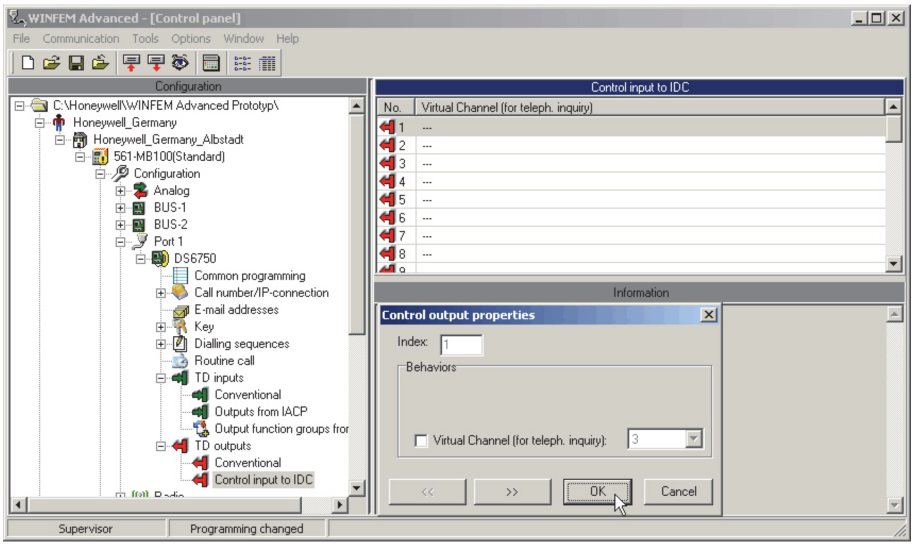
14.1.2 Virtual channel for control output

The transmission device has 9 virtual channels for detector group inputs which influence the paging device that is integrated in the device (AWAG function).
In addition to this, 9 virtual channels are available which can be assigned to the device's control outputs. Virtual channels are relevant only in conjunction with plain text announcements.

When extending the transmission device with BUS-2 output modules, the number of available control outputs can be much higher. Therefore it is possible to allocate the individual control outputs to a virtual channel (voice channel). In the corresponding selection window, one of the remaining available virtual channels of the respective control output can be assigned. The assignment of a virtual channel to several control outputs is not possible here.
Note: The number corresponding to the virtual channel is used for the announcement.
Please note the "Voice functions" section.

14.2 Control outputs in IACP RS-232 mode (only for VdS 2465 protocol)

The linked intruder alarm control panel has 40 "virtual inputs", which correspond to the remote control outputs of the transmission device in terms of functionality. The functions of the individual control outputs are assigned via the relevant programming options of the intruder alarm control panel (transmission device control signal). For further information on this subject, please refer to the programming instructions for the hazard detection control panel.
When you click on “Control outputs to IACP” in the configuration window, the available control outputs and their configuration are displayed in the status window. Double clicking on one control output will open the corresponding configuration menu.



Control input to IDC

No.	Virtual Channel (for teleph. inquiry)
1	---
2	---
3	---
4	---
5	---
6	---
7	---
8	---

Control output properties

Index: 1

Behaviors

□ Virtual Channel (for teleph. inquiry): 3

14.2.1 Virtual channel for control output

The only configuration option in this menu is assignment of a "virtual channel" for telephone queries. This makes it possible to control states or outputs of the intruder alarm control panel via a mobile phone or landline phone.
There are 9 virtual channels in total, which can be assigned to the control outputs of the device. These virtual channels are relevant in connection with plain text announcements and affect paging device (AWAG function) integrated in the device.

When coupling of the transmission device in IACP RS-232 mode, the number of available control outputs is much higher (max. 40). Therefore it is possible to allocate the individual control outputs to a virtual channel (max. 9 voice channels). The remaining available channels can be controlled e.g. via the connected control center (e.g. DEZ 9000) within the framework of remote control functions so that all 40 control outputs to IACP can be used. **This function is only possible in connection with the VdS 2465 protocol!** The assignment of a virtual channel to several control outputs is not possible.
Note: The number corresponding to the virtual channel is used for the announcement.
Please also refer to the "voice functions" section.

15. BUS-2 in master mode

If the transmission device is used as an integration module in compatible control panels, use of the bus interfaces or serial S1 is not possible.

When using the transmission device as a stand-alone device, the BUS-2 interface can be operated in master mode. The interface functions are similar to the BUS-2 interface of a intruder alarm control panel in this case. This makes it possible to connect conventional BUS-2 users to the transmission devices. The following bus users are currently supported by the DS 6700 / DS 6750:

- 5-input module (item no. 013130.10)
- 5-output module (item no. 013131.10)

This makes it possible to extend the number of inputs or control outputs.
Up to 16 BUS-2 modules can be connected and thus up to 80 additional control outputs or control inputs can be implemented.

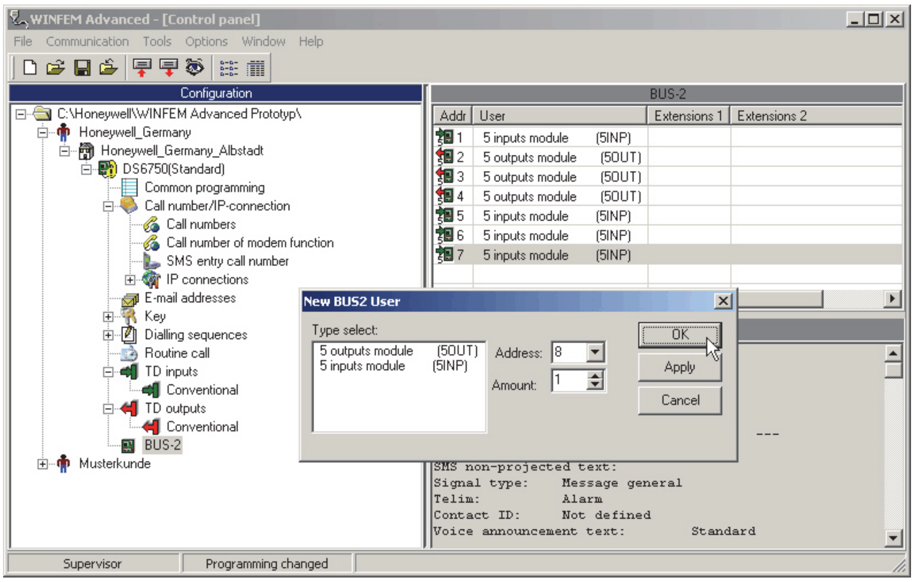
15.1 Automatically include user

After installing and commissioning the connected BUS-2 user, it is possible to have the transmission device automatically include the user.

Determination of BUS-2 users only works with if BUS-2 master mode of the transmission device is activated (see Section 20.5).

15.2 Insert user

To this end, select menu item "BUS-2“ in the configuration window and press the right mouse button. The "New" button is then displayed. Clicking on this button with the left mouse button displays the "New BUS-2 user" menu. Double clicking on the “BUS-2” menu item in the configuration window opens the corresponding configuration menu.



Addr	User	Extensions 1	Extensions 2
1	5 inputs module (5INP)		
2	5 outputs module (5OUT)		
3	5 outputs module (5OUT)		
4	5 outputs module (5OUT)		
5	5 inputs module (5INP)		
6	5 inputs module (5INP)		
7	5 inputs module (5INP)		

Type select:
5 outputs module (5OUT)
5 inputs module (5INP)

Address: 8

Amount: 1

```
                                    ---
SMS non-projected text:
Signal type:     Message general
Telim:           Alarm
Contact ID:      Not defined
Voice announcement text:        Standard
```

The following settings can be made.

- "Select type" selection window

Specification as to which type of user should be created (input module or output module).

- Address

  The BUS-2 address used. WINFEM recommends the lowest unused address.

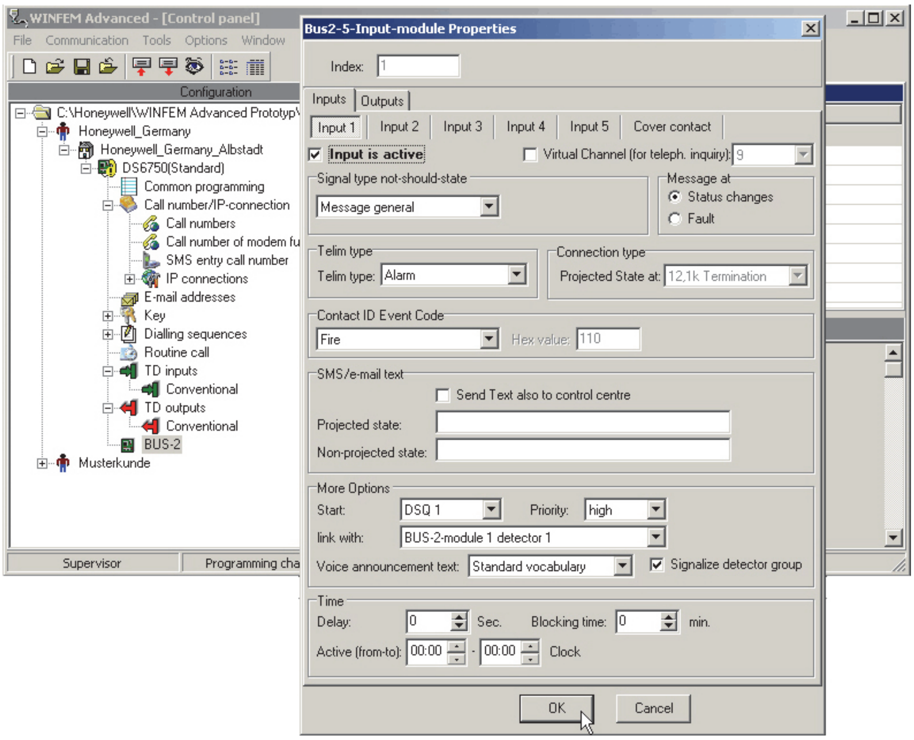
- Number

  Entry of the number of BUS users of the selected type. The number of bus users of the type selected in the "Select type" selection window is automatically created with uniform addressing.

The individual modules can be configured after creating the BUS-2 users.
On clicking "BUS-2" in the configuration window, the available BUS-2 modules are displayed in the status window.
Double clicking on the BUS-2 module to be edited (status window) opens the corresponding configuration menu.

15.3 Configuration of BUS-2 5-input modules

The configuration menu is divided into two tabs, one for configuration of the 5 inputs and the cover contact, and one tab labeled "Outputs" for buzzer configuration.



Index: 1

☑ Input is active

☐ Virtual Channel (for teleph. inquiry): 9

Signal type not-should-state: Message general

Message at: ● Status changes ○ Fault

Telim type: Telim type: Alarm

Connection type: Projected State at: 12,1k Termination

Contact ID Event Code: Fire Hex value: 110

SMS/e-mail text: ☐ Send Text also to control centre

Projected state:

Non-projected state:

More Options

Start: DSQ 1 Priority: high

link with: BUS-2-module 1 detector 1

Voice announcement text: Standard vocabulary ☑ Signalize detector group

Time

Delay: 0 Sec. Blocking time: 0 min.

Active (from-to): 00:00 - 00:00 Clock

15.3.1 Inputs and cover contact

A separate tab is available for each input (1 - 5) and the buzzer (output).
The 5 inputs are configured in the same way as configuration of detector groups of the transmission device.

In contrast to the detector groups of the transmission device, setting of the projected state is not possible. The inputs of the 5-input module are fundamentally designed as a differential detector group and have to be terminated with 12.1 KOhm for idle mode.

All other functions can be implemented as with the parallel S1 (detector groups of the transmission device).

Thus an individual SMS text for both detector group states (projected state / non-projected state) can be stored for each input and optionally (if the "Also send text to control center") to VdS 2465 receiving devices.
Links, and individual delay, blocking periods and active periods are also possible.

Note Section 22 with regard to the VdS 2465 addresses. "Address structures for VdS 2465". The cover contact of the 5-input modules is treated as a detector group input by the transmission device if marked as "Detector group active".

15.3.2 Outputs (buzzer)

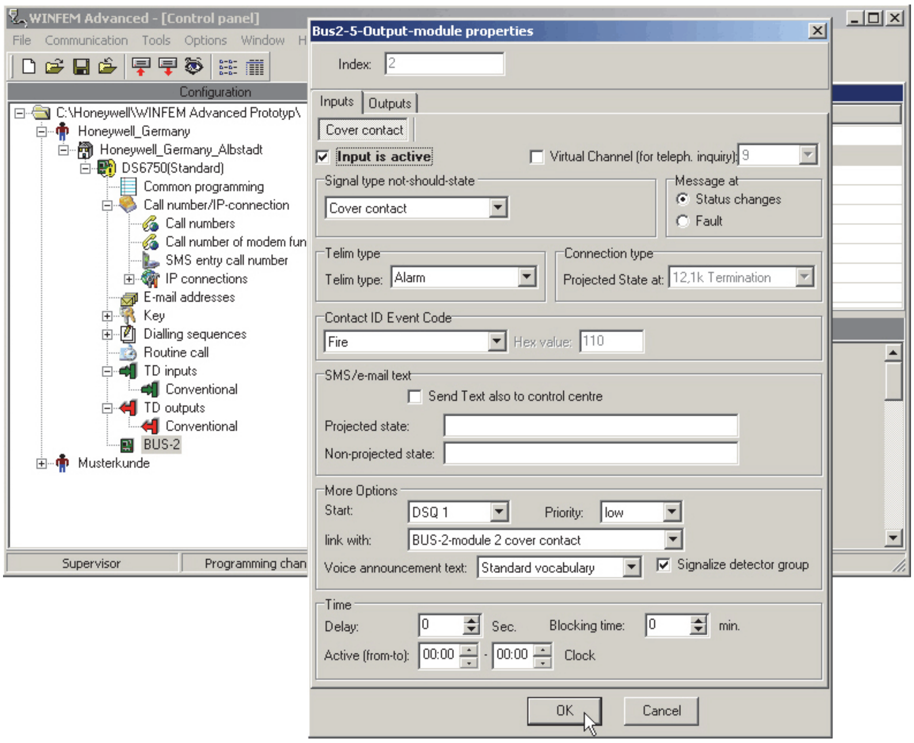
The buzzer is configured in the "outputs" tab.

Please see the section "Address structures for VdS 2465" regarding the used VdS 2465 addresses. The buzzer is handled by the transmission device as a remote control output.

The settings for the output are made in the same way as for the control outputs of the transmission device. Thus, for example, for transmission triggered by a particular module, the control center can automatically activate the buzzer (for a limited time or as a continuous signal). It is also possible, to activate and deactivate the buzzer via phone keys from a distance if a virtual channel is assigned.

15.4 Configuration of BUS-2 5-output modules

The configuration menu is divided into two tabs, namely the "Outputs" tab for configuration of the 5 outputs and the buzzer, and the "Inputs" tab for configuration of the cover contact.



Bus2-5-Output-module properties

Index: 2

Inputs | Outputs

Cover contact

☑ Input is active ☐ Virtual Channel (for teleph. inquiry): 9

Signal type not-should-state: Cover contact

Message at: ● Status changes ○ Fault

Telim type: Telim type: Alarm

Connection type: Projected State at: 12,1k Termination

Contact ID Event Code: Fire Hex value: 110

SMS/e-mail text: ☐ Send Text also to control centre

Projected state:

Non-projected state:

More Options
Start: DSQ 1 Priority: low
link with: BUS-2-module 2 cover contact
Voice announcement text: Standard vocabulary ☑ Signalize detector group

Time
Delay: 0 Sec. Blocking time: 0 min.
Active (from-to): 00:00 - 00:00 Clock

OK Cancel

The outputs and the buzzer are configured in the same way as the configuration of the control outputs of the transmission device. Static or time-limited activation is possible and a virtual channel can be assigned.
The same applies to the "Inputs" tab, which is used for configuration of the cover contact. The functionality is identical to the buzzer configuration of the 5-input module.

16. Communication using the Smartphone App

Communication can be established with the transmission device using a Smartphone. The statuses of the transmission device input channels and connected intrusion alarm control panel can be retrieved. In addition, programmed remote switching functions can be executed. Remote switching functions operate on the control outputs in the transmission device, and on their virtual inputs if control panels are connected over the RS-232 interface (IACP RS-232 mode).

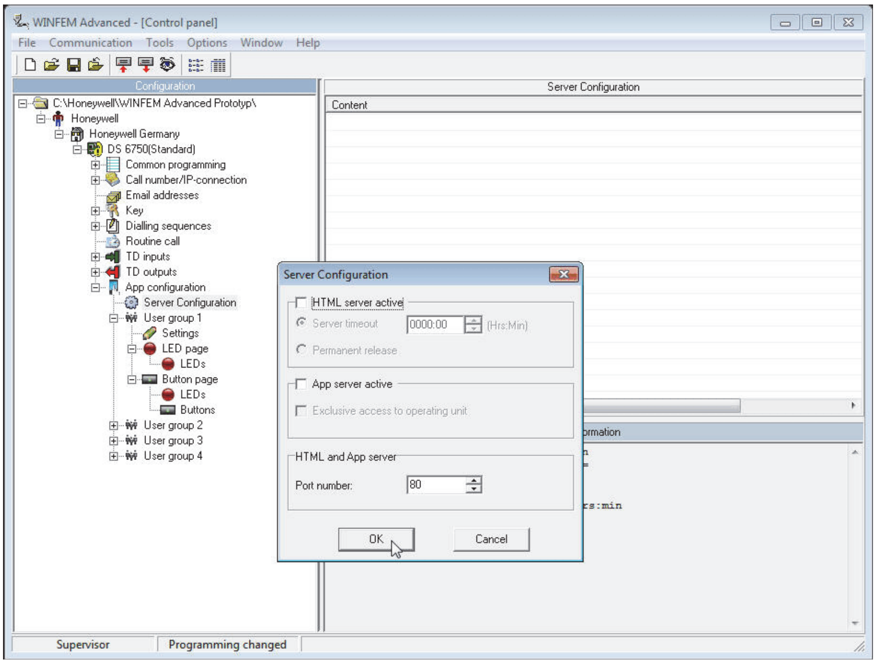
Requirements for operation:

- The Smartphone must run Android 2.1 or higher
- The Smartphone application "Honeywell App for Android" must be downloaded from the Google Play Store and installed on the Smartphone.
- The transmission device must be accessible on the Internet or on a local network.
- Using control panel series MB100.10, this functionality is available starting with control panel firmware version V.16.xx.

Fundamentally, communication parameters are programmed on the basis of user groups (user rights) and their corresponding display (LEDs) or control options (buttons).

The following parameters must be specified: Server configuration
User groups 1 - 4
Programming of display LEDs
Programming of buttons.

16.1 Server Configuration



Server Configuration

□ HTML server active
● Server timeout 0000:00 (Hrs:Min)
○ Permanent release

□ App server active
□ Exclusive access to operating unit

HTML and App server
Port number: 80

OK Cancel

- HTML Server

The HTML server is activated using this entry. Using an existing, correctly configured Ethernet connection, the transmission device can be accessed via a web browser. The server can be called up on Internet Explorer for instance, by entering the IP address of the transmission device. The status of the device as well as input/output statuses are displayed. Control functions can be assigned to channels that are programmed.

Server timeout:
This setting acts as a countdown timer which determines how long the server remains activated for access **after transmission of programming.** This HTML Server functionality is used mainly

to check if the transmission device is functioning properly after being placed in operation. (See chapter "Troubleshooting and Diagnostics Mode").

Permanent release:
Permanent release is suitable only for test purposes and should not be used, since communications with the transmission device are unencrypted in this mode.

- App Server

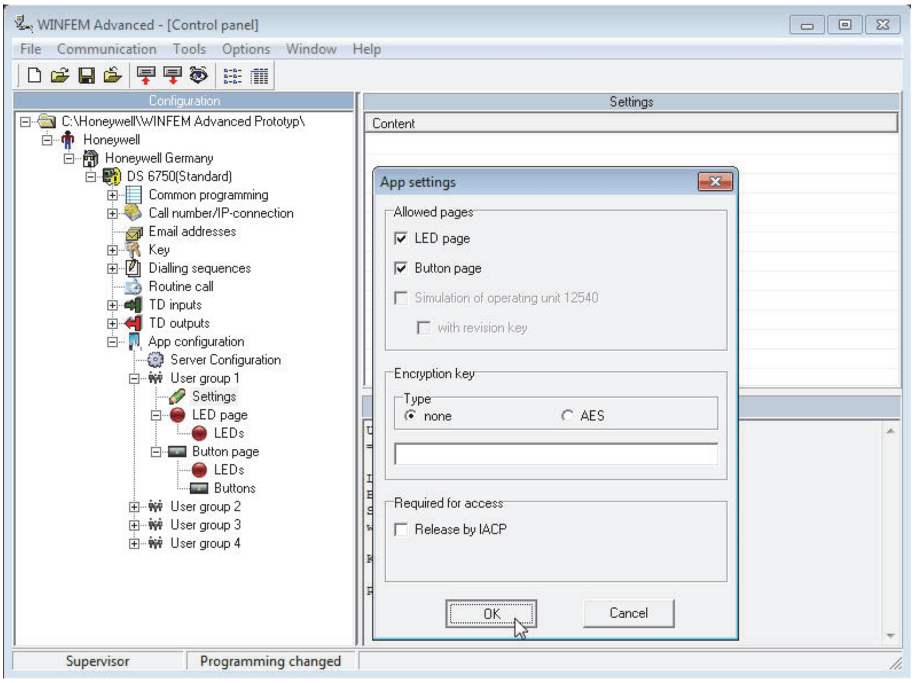
This entry activates the App Server. Using an existing, correctly configured Ethernet connection, the transmission device can be accessed with a Smartphone. Up to three active App connections can be established with a control panel or transmission device

Operating unit - exclusive access:
When exclusive access to the operating unit is enabled, the App server restricts access to the transmission device to one App connection with one operating unit page only. This requires activation of operating unit 12540 simulation on the Smartphone or access via a WINFEM operating unit.

- HTML and App Server

The port number which is used for the HTML or App server during a connection. You can obtain detailed information from the responsible network administrator. The default port for HTML is 80.
To configure the App, use the following entry: IP address:Port,
e.g.: 123.123.123.123:80

16.2 User Group



App settings

Allowed pages
☑ LED page
☑ Button page
□ Simulation of operating unit 12540
□ with revision key

Encryption key
Type
● none ○ AES

Required for access
□ Release by IACP

OK Cancel

User groups settings enable the pages allowed for each Smartphone user to be programmed. Up to 4 user groups can be assigned with different settings.
The App can be programmed to allow up to three different display pages on a Smartphone:

- LED page (to display status information),
- Button page (for control options) and the
- Operating Unit - page for the simulation of operating unit No. 012540 on the Smartphone.
  Only relevant if a connection is established with the control panel over the RS-232 interface.

Only experienced operators and installation engineers should be allowed to access the Operating Unit page. The Operating Unit view has an option that allows the revision key to be enabled, in this case all operating unit 012540 functions, except control panel function F519, are enabled.

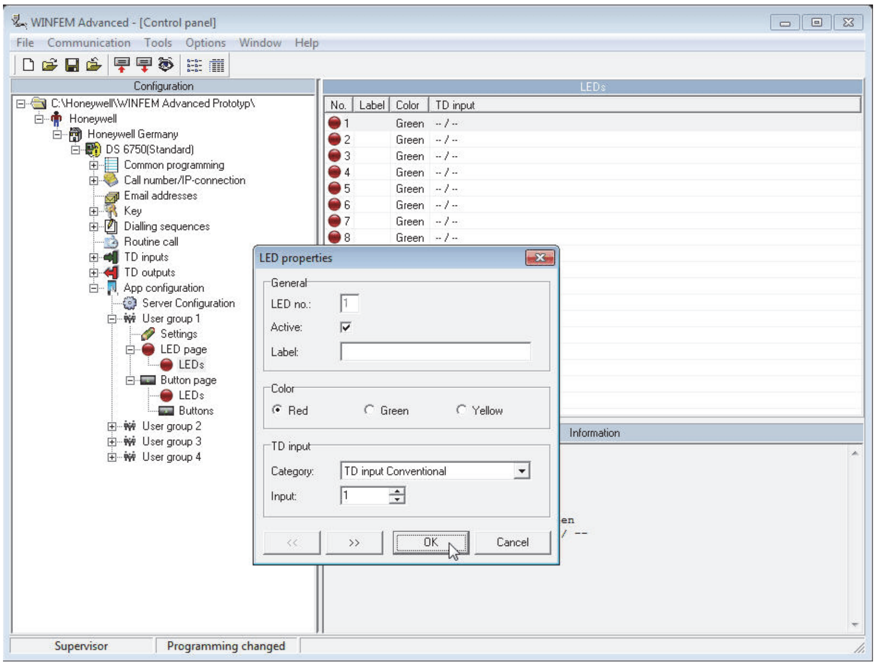
- Encryption key

  The 32 digit AES key not only enables encryption of data transmission, but also simultaneously restricts the operating rights of all users in the user group. For this reason, it is absolutely essential that, after determining which the pages are allowed (LED page/Button page) and how they should be programmed, the installer should restrict access authorizations by assigning different keys (for each user group used). In configuring the app on the Smartphone, this key must be entered once to assign an operator to the desired user group.

- Release by IACP

  When the checkbox "Release by IACP" is checked, access via the Smartphone is allowed only after operator release at the intrusion alarm control panel. Release for access is granted in the same way as release for remote access, namely through function 309 on the intrusion alarm control panel.

16.3 LED Page / Settings



No.	Label	Color	TD input
1		Green	-- / --
2		Green	-- / --
3		Green	-- / --
4		Green	-- / --
5		Green	-- / --
6		Green	-- / --
7		Green	-- / --
8		Green	-- / --

LED properties

General

LED no.: 1

Active: ☑

Label:

Color

● Red ○ Green ○ Yellow

TD input

Category: TD input Conventional

Input: 1

<< >> OK Cancel

8 different LED displays are available for display on the Smartphone.

- Active

  Activates the corresponding LED display.

- Label

  A unique name for the signal type displayed. The label can consist of up to 15 digits or letters. The label length should be adjusted to match the screen resolution of the Smartphone or tablet used, so that the label fits on the LED display.

- Color

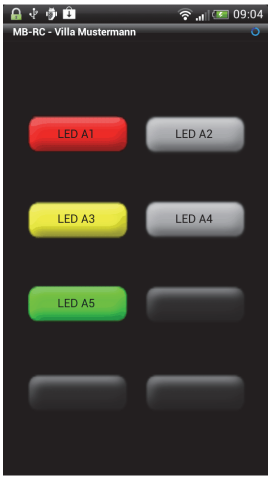
  The display color of the LED display can be selected from among red, green or yellow.

- TD Input / Category

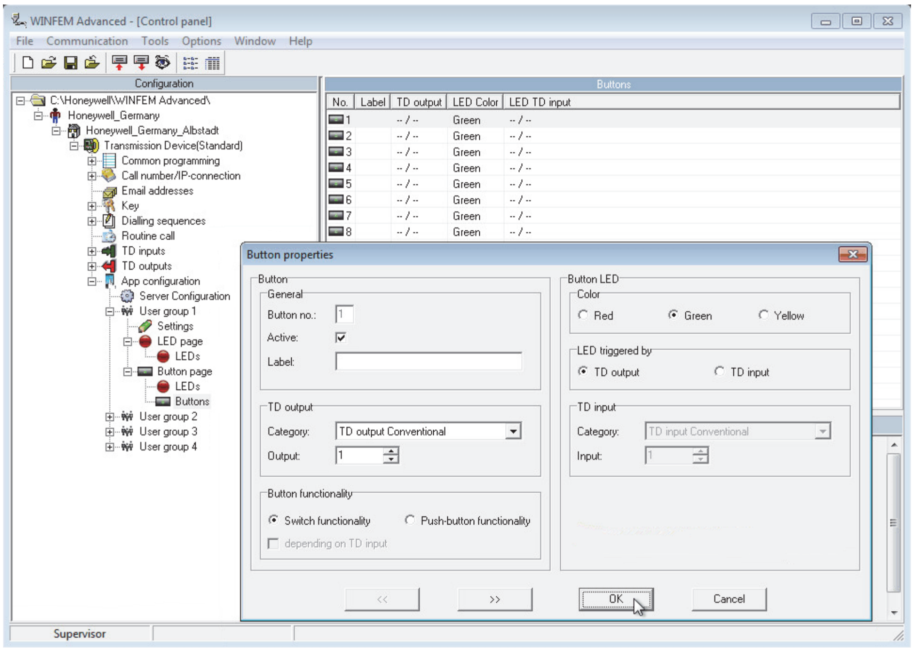
  If the transmission device is used as a standalone system, only conventional inputs 1 - 8 can be assigned as signal type for the LED display in the dropdown list "Category". Only static signals are meaningful as transmission criteria, because the input status is shown 1:1 on the LED display of the App.
  When a connection is established with the control panel via the RS-232 interface, "Output of IACP" can be selected as category. Any control panel output can be programmed with any output signal on this virtual LED. When connected to a control panel, signal types that remain in queue till cleared, irrespective of time of alarm, should be used. The following signal types are therefore preferred for the programming: Intrusion Alarm App, Tamper Alarm App, Hold-up Alarm App, Fire Alarm App, Collective Alarm App.
  The appropriate signal type (such as Tamper Alarm App) must be assigned to this output in the tab "IACP outputs " (see chapter 13.2) for transmission to the App.

16.3.1 Display on the Smartphone

The figure shows the LED page of the App. The LED page provides eight LED simulations. Any output signal on the control panel can be programmed on these virtual LEDs.
The example shows how different colors are assigned to the LEDs to enable individual signal types to be visually distinguishable.



16.4 Button Page / Properties



Buttons

No.	Label	TD output	LED Color	LED TD input
1		-- / --	Green	-- / --
2		-- / --	Green	-- / --
3		-- / --	Green	-- / --
4		-- / --	Green	-- / --
5		-- / --	Green	-- / --
6		-- / --	Green	-- / --
7		-- / --	Green	-- / --
8		-- / --	Green	-- / --

Button properties

Button
General
Button no.: 1
Active: ☑
Label:

TD output
Category: TD output Conventional
Output: 1

Button functionality
● Switch functionality ○ Push-button functionality
□ depending on TD input

Button LED
Color
○ Red ● Green ○ Yellow

LED triggered by
● TD output ○ TD input

TD input
Category: TD input Conventional
Input: 1

A total of three LED displays and up to 8 buttons each with an additional LED can be programmed on the Button page.

The LED display on the button must be programmed independently and can therefore display any criteria.

16.4.1 LEDs

The 3 LED displays are programmed as described in 16.3.

16.4.2 Buttons

- Active

Activates the corresponding button.

- Label

Unique name for the button. The label can consist of up to 15 digits or letters. The label length should be adjusted to match the screen resolution of the Smartphone or tablet used, so that the label fits on the button.

- TD Output / Category

If the transmission device is used as a standalone system (without BUS-2 output module), only the outputs 1 - 2 can be assigned in the dropdown list "Category".

Please note the switching behavior of the button: Smartphone App buttons have a switching function. First button press: function IN (input) is transmitted to the control panel. Second button press: function OUT (output) is transmitted to the control panel. Third button press: function IN again, and so on. This switching behavior can be changed by programming "Button Functions".

If connection with the control panel is established over an RS-232 interface, "Control input to IACP" can be selected as category. Any control panel control input can be actuated by pressing the selected button. This control input is then used as a trigger criteria for a macro to execute any desired macro function in the control panel.

- Button functionality

Switching can be changed by programming the "button functionality".
Switch function: A switch function is assigned to the selected button in the smartphone app, so that the first press of a button transfers the function ON signal to the control and indicating equipment. Second press of the button: function OFF signal is transferred to the control and indicating equipment. Third press of the button: function ON again, etc.

The "Control input on I-CIE" category can be selected for central connections via the RS-232 interface. Any control input from the control and indicating equipment can be controlled using the selected button. This control input is then used as a macro trigger criterion for implementing any macrofunction of the control and indicating equipment.

Button function: A button function is assigned to the selected button in the smartphone app, so that a press of the button transfers a short pulse (approx. 100 ms with a rising flank) to the control and indicating equipment.

The "Control input on I-CIE" category can be selected for central connections via the RS-232 interface. Any control input from the control and indicating equipment can be controlled using the selected button. This control input is then used as a macro trigger criterion for implementing any macrofunction of the control and indicating equipment.

- Button functionality ➜ depending on TD input

"Button Functions ➜ depending on TD input" can be programmed only when connected to a control panel over an RS-232 interface.

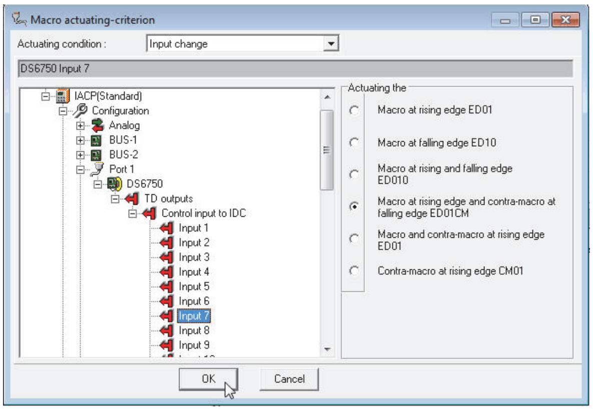
The switching behavior of the button can be set such that a switching command is sent only when a specific condition is reached (toggle switch principle). For example, the switching status can be set only if the corresponding TD input was set on the control panel. This functionality requires appropriate macro programming in the control panel along with the definition of macro trigger criteria corresponding to the desired functions.
The following table shows the relationship:

TD Output *Category*	**LED control**	**Button Functions**	**Function**
Control Input to IACP / TD output conventional	*by TD output*		Each press of the button switches the output state. The LED on the button corresponds to the last switching status transmitted
Control Input to IACP / TD Output conventional	*by TD input*		Each press of the button switches the output state. The LED on the button tracks the switching status of the programmed TD input.
Control input to IACP	*by TD input*	*depends on TD input*	The switching information upon button press depends on the display status of the LED. The LED is triggered by the TD input status.

Example:

A possible use, for example, is the internal activation/deactivation of a zone.
The current state of the zone must be taken into account (positive drive condition) for the correct control to be executed.

Setting "Button Functions" ensures that an internal deactivated zone can actually be activated.
This functionality is implemented by programming "Macro at rising edge and contra-macro at falling edge" as the trigger criterion.



Macro actuating-criterion

Actuating condition : Input change

DS6750 Input 7

Actuating the

○ Macro at rising edge ED01
○ Macro at falling edge ED10
○ Macro at rising and falling edge ED010
● Macro at rising edge and contra-macro at falling edge ED01CM
○ Macro and contra-macro at rising edge ED01
○ Contra-macro at rising edge CM01

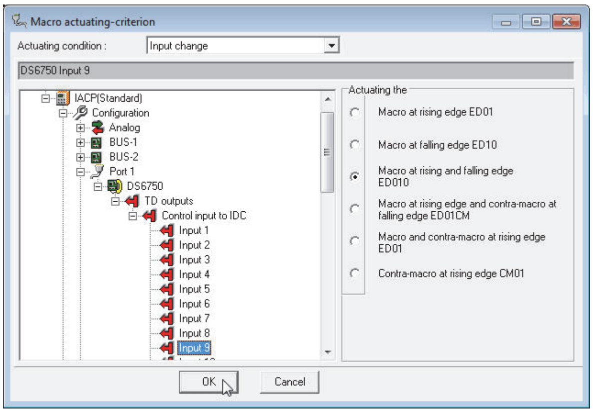
Principle:
If the App button is actuated, the trigger is transmitted to the control panel via the "Control Input to IACP 7" (example).
Due to the programmed dependence of TD input,
the macro is executed when the positive drive condition is met (in the example here, zone activated).
The macro is executed once when the button is pressed, because the contra-macro is executed (in the example, zone deactivated) if the button is pressed again.

More examples with the required parameterization can be found in the FAQ area of our home page.

Example:

An application where "Button Functions" would not be used, for example, is in programming a button which executes a clear function for a zone when activated. Here, the display and the function have no direct correlation, a press of the button always executes the same function, the function does not permit a contra-macro.

The "Button Functions" feature is not used, and a button actuation does not allow a contra-macro to run because the clear function is executed at each actuation.
The trigger criterion programmed for this function is "Macro at rising and falling edge".



Macro actuating-criterion

Actuating condition : Input change

DS6750 Input 9

Actuating the

○ Macro at rising edge ED01

○ Macro at falling edge ED10

● Macro at rising and falling edge ED010

○ Macro at rising edge and contra-macro at falling edge ED01CM

○ Macro and contra-macro at rising edge ED01

○ Contra-macro at rising edge CM01

Principle:
If the App button is actuated, the trigger is transmitted to the control panel via the "Control Input to IACP 9" (example). As a result, the macro is executed and the zone is cleared.
The macro is executed (in this example, the clear function) at each button press, since it was programmed both for rising and falling edge.

- Button LED / Color

The display color of the LED in the button can be selected from among red, green or yellow. This LED on the button is programmed independently and therefore can display any criteria.

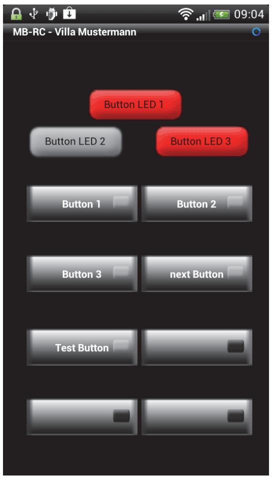
- LED control

This selection determines the control behavior of the LED integrated in the button.
In the simplest case, the selected LED is controlled "by TD output", that is to say, when the corresponding output is **set**, the LED is **simultaneously** controlled. This can be used as a transmission acknowledgement, for example.
However, if actual feedback has to be displayed, "by TD input " must be selected. The programming “depending on TD input” can be programmed only when connected to a control panel over an RS-232 interface. The "depending on th input" button is activated in this case. The relevant input that is supposed to provide feedback of control effected must be programmed in the input field for category and input number. The corresponding signal type must be assigned to this TD input in the "IACP Outputs" tab (see Chapter 13.2) for transmission to the App. In this programming, the selected LED is controlled only after the corresponding output is **set and feedback** is obtained.
If the LED on the button is meant to display **any criterion**, either the desired "TD Input conventional" or an "IACP output" can be assigned through the "TD Input" selection box. This criterion must then also be assigned to the corresponding signal type in the "IACP Outputs" tab (see Chapter 13.2). When connected to a control panel, signal types that remain in queue till cleared, irrespective of time of alarm, should be used.

16.4.3 Display on the Smartphone

The figure shows the Button page of the App. This view contains 3 LEDs as well as eight buttons with integrated LEDs, too. The description in Chapter 16.3 applies analogously to the 3 LEDs.

The sample shows the eight buttons with different labels and an integrated "Display LED". Each button controls the corresponding output via a control panel macro in order to implement the desired function.



17. Voice and remote control functions

The transmission device can transmit voice information via the analog (PSTN) connection or via GSM (in conjunction with RFW-4000).
The transmission devices are factory fitted with a standard vocabulary for this purpose, from which the appropriate announcement texts are formed for transmission. If these default language texts do not meet customer requirements, it is possible to record custom text and thus individually design the announcement to a certain degree (see Section 20.6.).

17.1 AWAG function (voice function) with standard vocabulary

When a call is received, the device responds after the user has answered the call first with a greeting message, in which the MSN of the transmission device is used as an identification feature. Then a message is communicated regarding the reason for activation (state of the triggering input).
Example: "Attention, this is an announcement from information system nine, zero, seven, seven, two. Input one has been triggered. Repeat by pressing the star key"

After the text has been played, the star key can be pressed on the telephone keypad to repeat the entire greeting message.

ℹ If the person called hangs up before all the outgoing message has been transmitted, another call is made or the next user in the assigned dialing sequence is called. If the voice message has to be acknowledged by the called party, then "voice acknowledgment" has to be configured when programming the call number (see Section 7.1.5). Acknowledgment is performed using the telephone keypad with the ID number assigned to the user.

17.1.1 Functionality with use of the standard vocabulary

ℹ If required, individual texts can be stored for the device name and the virtual (AWAG) input channels 1 - 4.

The sequence for activation of an input, for which customized text information has been assigned, is designed as follows:

When a call is made, the device issues the following standard text first when the person has answered the call: "Attention, this is an announcement from the information system". Immediately after this, the customized device name, e.g. "Sample Company in Sample City" is played back. Then a message is communicated regarding the reason for activation (state of the triggering input) with the standard vocabulary, e.g. "Input one has been triggered" followed by playback of the customized text that has been allocated to the input, such as "Attention, intrusion alarm". At the end the following announcement is made: "Repeat by pressing the star key".

ℹ If the activation behavior, "state change" was entered for the corresponding input, a call is also made when the input is reset.
The customized device name is played back here as well, but the standard text is played by as the status announcement (e.g. input one reset).
Important: Customized text information in the standard vocabulary (text type: virtual channel 1 - 4) can be stored only for non-projected states of the virtual inputs 1,2,3 and 4 and for the device name.

17.2 AWAG function (voice function) with customized vocabulary

17.2.1 Functionality with use of customized announcement texts

When a call is made, the device first plays the previously recorded location text (max 16 sec) after the person has answered the call: "Attention, this is an announcement from the information system, Sample Company in Sample City". Immediately after this, the message pertaining to the activation reason (status of the triggered input) is played back with the announcement text of the respective channel, e.g. "fault in heating system of main plant". At the end the following announcement is made: "Repeat by pressing the star key" so that the message can be heard again.

17.3 Remote control functions (DS 6750 only)

The transmission device can be called for remote control purposes.

Calls are only accepted from users, the call number of which (number type: voice) is stored in the call number batch and labeled as "Authorized to call".

17.3.1 Remote control function

The transmission device responds with "Please enter code". A corresponding release code must first be entered on the telephone keypad. The identification number assigned to the user is used as the release code.
Once the code is has been entered correctly, the announcement "control mode" is issued. You can switch to the query mode by pressing the "#" key. Pressing the "#" button again leads back to the control mode.

17.3.2 Control mode functions

First, press the button that corresponds to the virtual channel, which is assigned to the remotely controlled output. Then press "0" if the output is to be switched off or press "1" if the output is to be switched on.

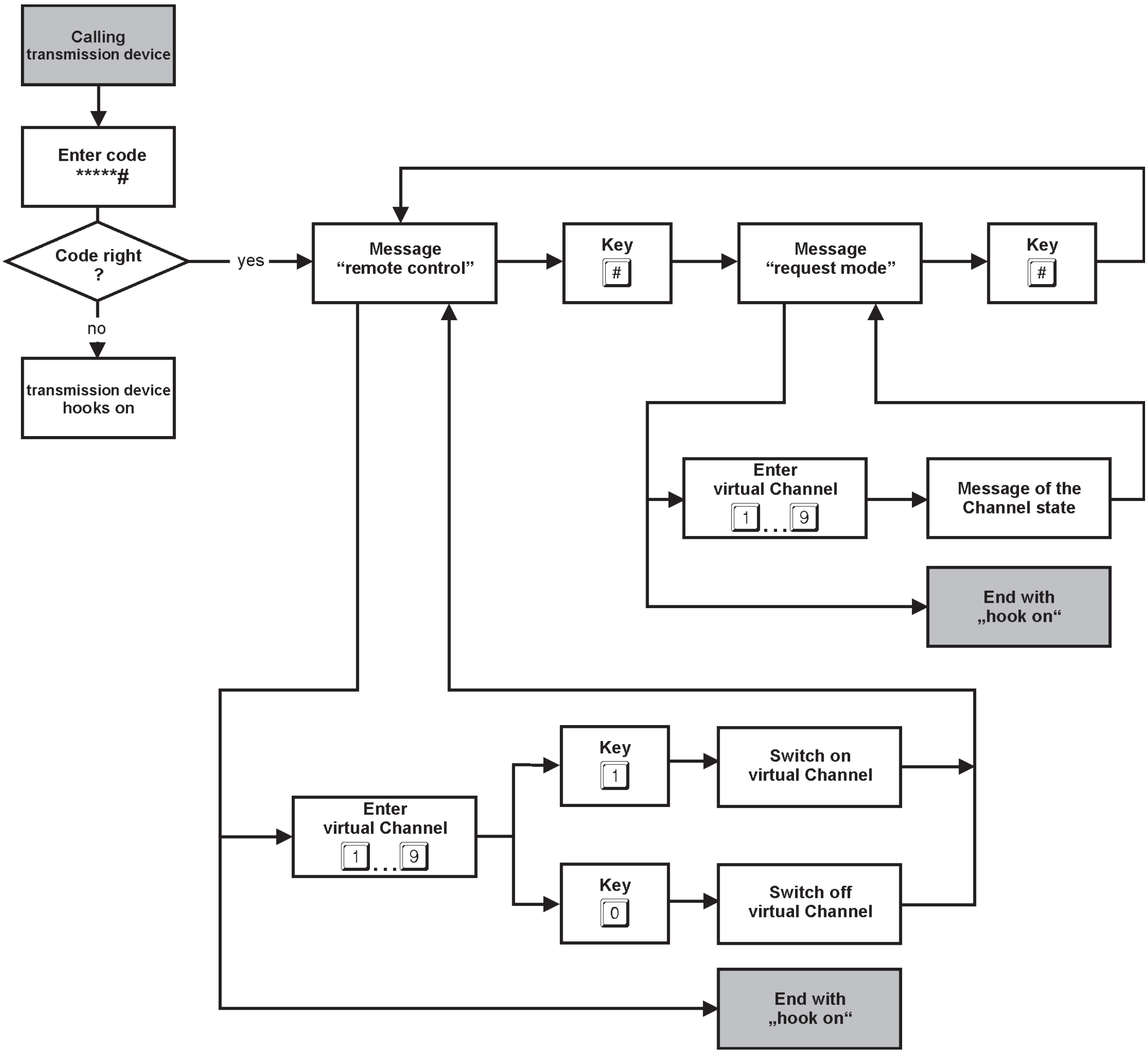
The device generates a confirmation after the switching operation has been performed: e.g. "Output one - ON - control mode". It is then possible to issue a further switching command or switch to query mode.

17.3.3 Functions in query mode

First press the button that corresponds to the virtual channel, which is assigned to the remotely controlling input.
The corresponding status announcement is issued, e.g.: "Input three - triggered. query mode"
It is then possible to issue a further query command or switch to control mode.

After all the desired control operations or query operations have been carried out, the connection can be terminated (hook on).

17.3.4 Remote control function sequence

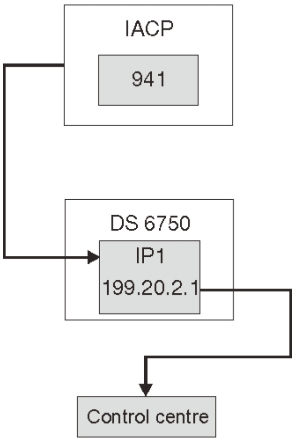

Calling transmission device
Enter code *****#
Code right ?
yes
no
transmission device hooks on
Message "remote control"
Key #
Message "request mode"
Key #
Enter virtual Channel 1 ... 9
Message of the Channel state
End with „hook on“
Enter virtual Channel 1 ... 9
Key 1
Switch on virtual Channel
Key 0
Switch off virtual Channel
End with „hook on“

18. Extended compatibility mode (DS 6750 only)

When using this option, MB control panels connected via BUS-2 and I-BUS (with IACP561-MB256) can transmit alarm notifications via Ethernet (IP connections). E-mail and AWAG functionalities can also be used.
Due to the fact that these transmission paths and protocols with BUS-2 and I-BUS use connection technology as used in older hazard detection systems are not configurable in the corresponding hazard detection systems, that is performed using a conversion table in the transmission device DS 6750.

18.1 Own call number - transmission path conversion table

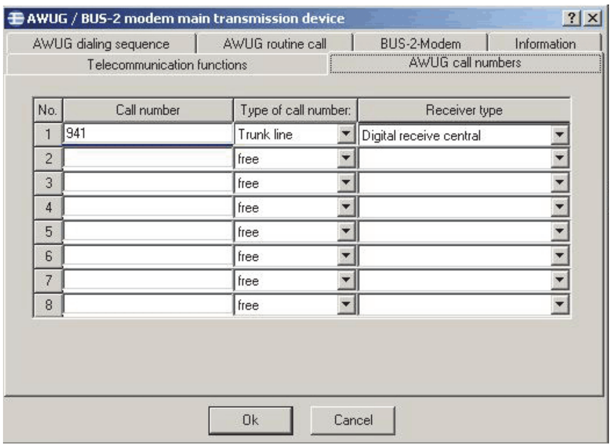
Transmission path in DS 6750	Call number in the hazard detection system connected via BUS-2 / I-BUS
Demand-actuated call number 1	901
Demand-actuated call number 2	902
Demand-actuated call number 3	903
Demand-actuated call number 4	904
Demand-actuated call number 5	905
Demand-actuated call number 6	906
Demand-actuated call number 7	907
Demand-actuated call number 8	908
Demand-actuated call number 9	909
Demand-actuated call number 10	910
Demand-actuated call number 11	911
Demand-actuated call number 12	912
Demand-actuated call number 13	913
Demand-actuated call number 14	914
Demand-actuated call number 15	915
Demand-actuated call number 16	916
Demand-actuated call number 17	917
Demand-actuated call number 18	918
Demand-actuated call number 19	919
Demand-actuated call number 20	920
1st dedicated line connection to security service	941
2nd dedicated line connection to security service	942
3rd dedicated line connection to security service	943
4th dedicated line connection to security service	944
1st dedicated IP connection for video control panels	951
2nd dedicated IP connection for video control panels	952



If call number 1 is configured with the target call number “941“ in the MB control panel for example, then the message is transmitted to the security service (see example image using the first dedicated IP connection if this call number 1 is activated in a dialing sequence of the DS 6750.
Both the intruder alarm control panel and the transmission device must be configured independently: on the one hand, the respective MB control panel with the DS 6750 as DGA 2400 in compatibility mode with

WINFEM-100 or WINFEM Advanced for IACP 561-MB 256, and on the other, the DS 6750 as a "stand-alone" device (with activated BUS-2 or I-BUS interface) with WINFEM Advanced.

The following image shows the respective dialog in WINFEM-100 for example:

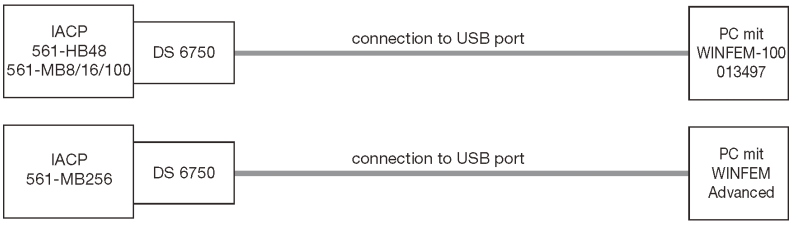

AWUG / BUS-2 modem main transmission device

No.	Call number	Type of call number:	Receiver type
1	941	Trunk line	Digital receive central
2		free	
3		free	
4		free	
5		free	
6		free	
7		free	
8		free	

18.2 USB connection in compatibility mode

When using this option, older MB control panels connected via BUS-2 and I-BUS, which require the programming software WINFEM-100 or WINFEM Advanced for IACP 561-MB256, can be programmed via the transmission device's USB interface. This requires the use and installation of the software version WINFEM Advanced V13.xx or higher.
When installing WINFEM Advanced, a special driver is installed which provides additional communication options. The transmission device is connected using a BUS-2 or I-BUS terminal card as used in older alarm systems.

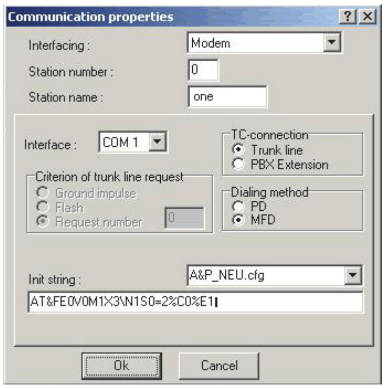
- USB
The WINFEM PC is then connected via the transmission device's USB port.



18.2.1 USB connection in WINFEM-100

In order to use the USB connection, the drop-down menu "Communication" is selected, and then the “Communication settings” dialog is selected and the “Modem” connection is chosen.

In the system “Connection settings”, a “*” is then entered as the call number modem.


Communication properties

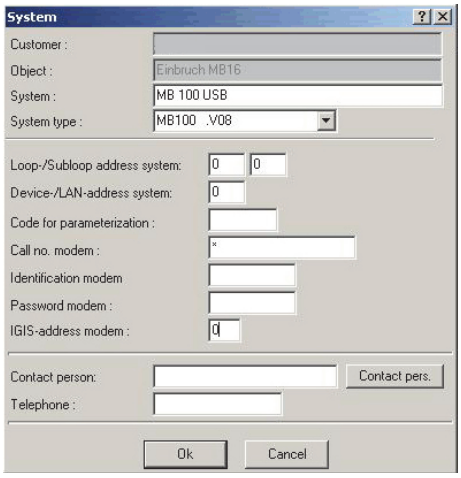
Interfacing : Modem
Station number : 0
Station name : one
Interface : COM 1

TC-connection
● Trunk line
○ PBX Extension

Criterion of trunk line request
○ Ground impulse
○ Flash
● Request number 0

Dialing method
○ PD
● MFD

Init string : A&P_NEU.cfg
AT&FE0V0M1X3\N1S0=2%C0%E1


System

Customer :
Object : Einbruch MB16
System : MB 100 USB
System type : MB100 .V08

Loop-/Subloop address system: 0 0
Device-/LAN-address system: 0
Code for parameterization :
Call no. modem : *
Identification modem
Password modem :
IGIS-address modem : 0

Contact person:
Telephone :

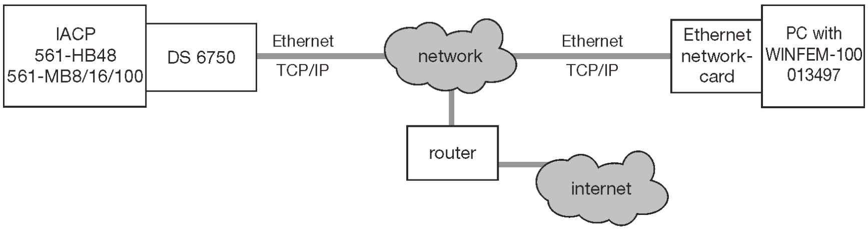
The actual connection set-up with WINFEM-100 is carried out via the commands:

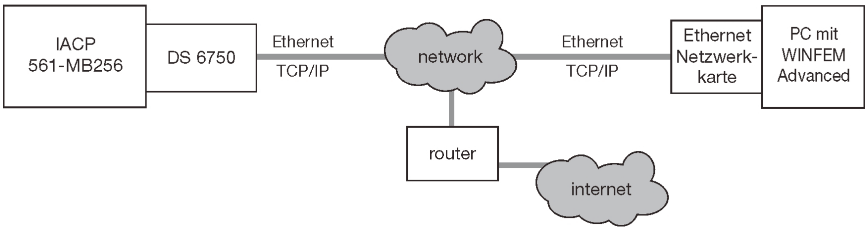
- Panel → PC	Transfer the system programming and configuration from the panel to the PC.
- PC → panel	Transfer system programming from the PC to the panel.
Operating module	Emulation of an LCD operating module 012540/012541 is launched on the PC/laptop.

18.3 Ethernet connection in compatibility mode

When using this option, older MB control panels connected via BUS-2 and I-BUS, which require the programming software WINFEM-100 or WINFEM Advanced for IACP 561-MB256, can be programmed via Ethernet (IP connection). This requires the use and installation of the software version WINFEM Advanced V13.xx or higher.
When installing WINFEM Advanced, a special driver is installed which provides additional communication options. The transmission device is connected using a BUS-2 or I-BUS terminal card as used in older alarm systems.

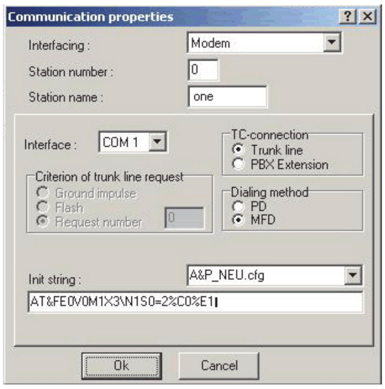
TCP/IP
The WINFEM PC is connected to the device via an Ethernet network. The PC is connected to the Ethernet network via an Ethernet network card.





18.3.1 TCP/IP connection in WINFEM-100

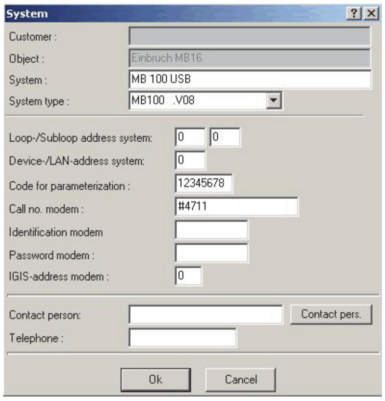
In order to use the TCP/IP connection option, the drop-down menu "Communication" is selected, and then the “Communication settings” dialog is selected and the “Modem” connection is chosen.


Communication properties

Interfacing : Modem
Station number : 0
Station name : one
Interface : COM 1
TC-connection
● Trunk line
○ PBX Extension
Criterion of trunk line request
○ Ground impulse
○ Flash
● Request number 0
Dialing method
○ PD
● MFD
Init string : A&P_NEU.cfg
AT&FE0V0M1X3\N1S0=2%C0%E1

In the system “Connection settings”, a “#” followed by a name for this connection (up to 22 alphanumeric characters) are then entered as the call number modem.

Based on the name of this connection, a configuration file is created in which the connection parameters for the TCP/IP connection of this system are stored.
If a configuration file is already available, the "#" character can be entered followed by the name of the connection to load a configuration.

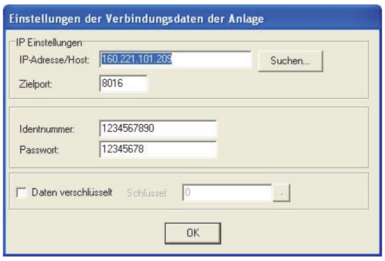

System

Customer :
Object : Einbruch MB16
System : MB 100 USB
System type : MB100 .V08
Loop-/Subloop address system: 0 0
Device-/LAN-address system: 0
Code for parameterization : 12345678
Call no. modem : #4711
Identification modem
Password modem :
IGIS-address modem : 0
Contact person:
Telephone :

The actual connection with WINFEM-100 is established using the commands:

- Panel → PC Transfer the system programming and configuration from the panel to the PC.
- PC → panel Transfer system programming from the PC to the panel.
Operating module Emulation of an LCD operating module 012540/012541 is launched on the PC/laptop.

The following dialog is displayed to enter the connection parameters of the TCP / IP connection before actual connection set-up.



IP-Adresse/Host: 160.221.101.209
Zielport: 8016
Identnummer: 1234567890
Passwort: 12345678
□ Daten verschlüsselt Schlüssel: 0

These parameters are to be entered in the same way as described in Section 4.3.2 .

After clicking "OK", a TCP / IP connection is established between the PC / laptop and the panel.

19. Firmware update

The program (firmware) of the transmission device is located in a flash memory on the device board. If required, the new firmware can be saved in the flash memory in connection with "WINFEM Advanced" via the USB interface of the transmission device.

The firmware should be installed only by authorized technical staff. Pay attention to electrostatic discharge!

It is generally recommended to load the current firmware version into the transmission device. A free download is available on our homepage.

EN Only registered and authorized installation companies are allowed access to the firmware download under: www.security.honeywell.de

19.1 Software modules

The entire firmware is subdivided into three sections, each of which is equipped with an own software module. These are in detail:

• Bootloader	From (**ABOTL**_00V0501.fdl)
• Firmware of the transmission device	(**ADS66**_01V07xx.fdl)
• Language (for AWAG function)	(**ADISM**_00V0201.fdl)

If a firmware update is required, in most cases only the firmware of the transmission device is concerned. In individual cases, it might however also be required to update the bootloader.

Please check that the device is equipped with the latest bootloader version before updating the firmware. If the bootloader has to be update, always update the bootloader first before installing the new firmware.

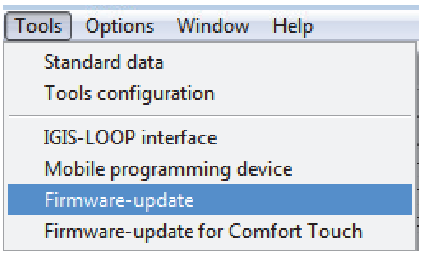
Updating the language is only required if the transmission device is not equipped with the current version or if it is to be switched to a foreign language.

19.2 Firmware update procedure

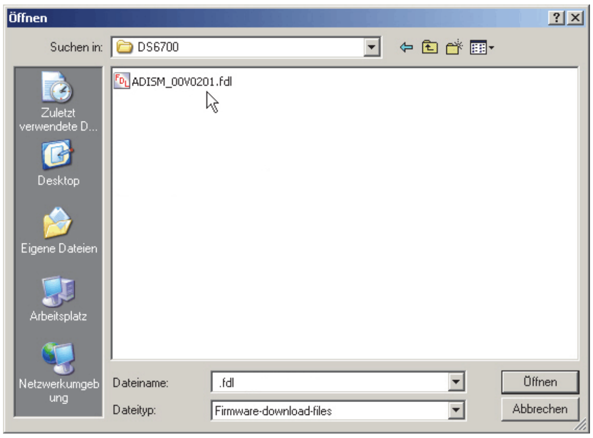
Before carrying out the firmware update, please save the programming data and all entries of the event memory data of the transmission device via WINFEM Advanced as the parameter memory is overwritten during a firmware update. It is recommended to disconnect all connections (e.g. I-BUS) and possible BUS-2 users, and to connect the transmission device separately to the voltage supply.

The transfer of a new firmware file is described in the following paragraphs. For updating the bootloader, proceed accordingly.

1. Activating the "Firmware update menu“ via the Menu “Tools” -> “Firmware-Update”.
   The update menu is opened, at the same time the available update files are displayed. You can use the known Windows mechanisms in order to change to another directory if another file than the one offered in the current directory is to be used.



Double clicking or pressing the ”Open” button loads the respective file (ADS66...) into the transmission menu.



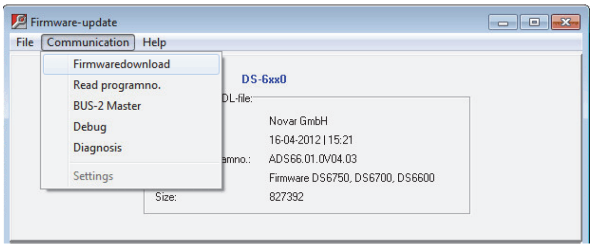
Suchen in: DS6700

ADISM_00V0201.fdl

Dateiname: .fdl

Dateityp: Firmware-download-files

Subsequently start transmission of the software into the transmission device using the menu “Communication” -> command “Firmware download”.



DL-file:

Novar GmbH

16-04-2012 | 15:21

amno.: ADS66.01.0V04.03

Firmware DS6750, DS6700, DS6600

Size: 827392

First, the entire flash-memory area of the transmission device is deleted, which might take some time (between 15 seconds and 2 minutes, depending on the flash type). During the deletion process, the progress is not shown. Once the flash memory has been deleted, the actual programming process starts and the progress will be indicated accordingly..

2. After the update, exit from the software module for the flash update by clicking "Close window".

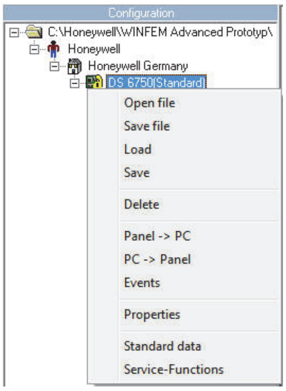
After the firmware has been transmitted, a manual reset (actuate Reset button) has to be carried out on the transmission device.

3. Now the transmission device can be newly configured or the configuration of the transmission device that was saved before is to be retransmitted.

If the transfer of the firmware is interrupted, e.g. due to power failure or interruption of the USB connection during the update process, the transmisson device will display this error after a reset by quickly flashing of the the yellow LED. In this case, the update process can be redone to successfully transfer the firmware.

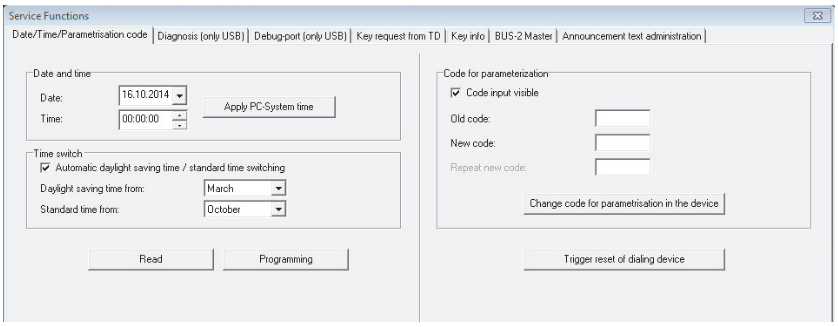
20. Service functions

The context menu “Service functions” opens the following tabs. When you click on an individual tab, the dialog box for setting date and time as well as the parameterization code, the dialog box for the debug mode, the dialog box for picking up keys for encrypted data transmission or the dialog box for including the BUS-2 user if the transmission device is operated in BUS-2 master mode opens. This context menu also includes the dialog for managing the announcement texts.



20.1 Tab “Date / Time / Parametercode / Reset”

The date and time can be set in this screen. When you click button "Apply PC System time", the PC time will be adopted in the input screen.
If the checkbox "Automatic daylight saving time / standard time" has been selected, the change between daylight saving time will be made in the months specified here.


Service Functions
Date/Time/Parametrisation code
Diagnosis (only USB)
Debug-port (only USB)
Key request from TD
Key info
BUS-2 Master
Announcement text administration
Apply PC-System time
Change code for parametrisation in the device
Read
Programming
Trigger reset of dialing device

Date and time
Date: 16.10.2014
Time: 00:00:00

Time switch
☑ Automatic daylight saving time / standard time switching
Daylight saving time from: March
Standard time from: October

Code for parameterization
☑ Code input visible
Old code:
New code:
Repeat new code:

- Programming button

  Transmits the previously set date and time to the transmission device.

- Read button

  The date and time are transmitted from the transmission device to the PC.

In each case, the connection type from the PC/laptop to the transmission device must be defined in the menu item "Communication/Settings/Connection" which is opened. With this kind of data transmission, only the date/time settings are programmed or read, no other parameters will be transmitted.

20.1.1 Code for programming

No parameterization code is stored in the transmission device on delivery. If a code has been programmed in the device, then this code has to match in the case of programming.

The code can not be read out of the device! If the code has been forgotten, then the device has to be flashed again using a firmware update. Parameterization and thus the parameterization code are deleted.

- Program code for parameterization

  “Old code” input window: No entry
  “New code” input window: Enter code for parameterization.
  "Repeat new code" input window: Confirm code for parameterization, (only if hidden code entry is activated).
  Click on the “Change code for parameterization in the device" button. The selection menu for the connection setting for the transmission device is opened if no connection exists.

- Change code for parameterization

  “Old code” input window: Enter the code programmed in the device.
  “New code” input window: Enter new code for parameterization.
  "Repeat new code" input window: Confirm new code for parameterization (only if hidden code entry is activated).
  Click on the “Change code for parameterization in the device" button. The selection menu for the connection setting for the transmission device is opened if no connection exists.

- Delete code for parameterization
  “Old code” input window: Enter the code programmed in the device.
  “New code” input window: No entry
  "Repeat new code" input window: No entry
  Click on the “Change code for parameterization in the device" button. The selection menu for the connection setting for the transmission device is opened if no connection exists.

20.1.2 Trigger reset of dialing device

After clicking on the button "Trigger reset of dialing device", a reset is performed after a confirmation query .

20.2 Tabs “Diagnosis” and “Debug port”

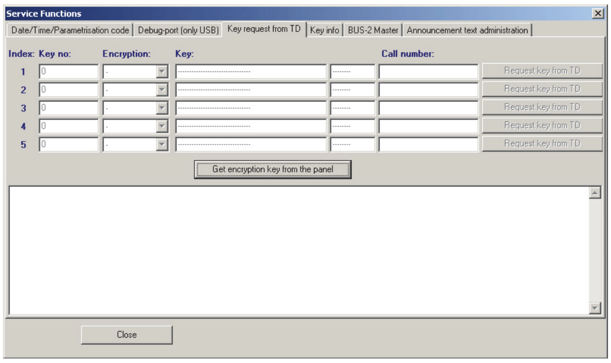
Activation of the integrated diagnostic tools. For further information, please see Section "22. Troubleshooting and diagnostic mode".

20.3 Tab “Key request from TD”

The “Request key from TD” (TD = transmission device) tab is used to open the dialog box for to pick up keys for encrypted data transmission.

- "Get encryption key from the panel" button
  If a call number has been programmed previously in the “Keys” parameter group, then the transmission device establishes a connection to the control center and requests a key.

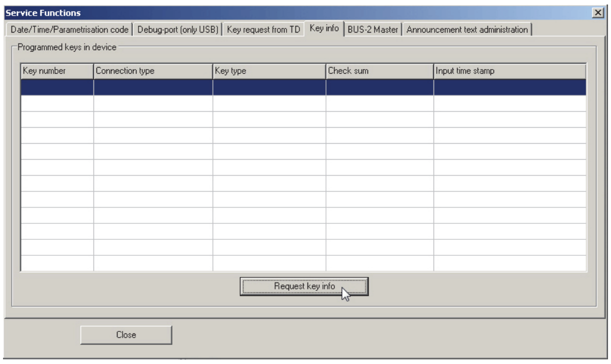
For more detailed information, see the Section "10.1.3 Automatic key assignment".



20.4 Tab "Key info"

The "Key info" tab is used to open the dialog box for displaying key information stored in the transmission device. For secure (encrypted) connections to alarm receiving centres (ARC) and management systems (WINMAG), inspection of the correct configuration or checking for manipulation is required. The currently available encryption parameters can be checked without reading out or displaying the keys themselves.

- "Request key info" button
  The key information will be read out. The key number, use of the key (connection type), key type, and checksum of the key as well as the integration time of all stored keys are displayed here. This can then be compared with the existing system documentation and checked for changes. The key information can be retrieved via all available routeways to the transmission device, namely USB, TCP/IP and PSTN.

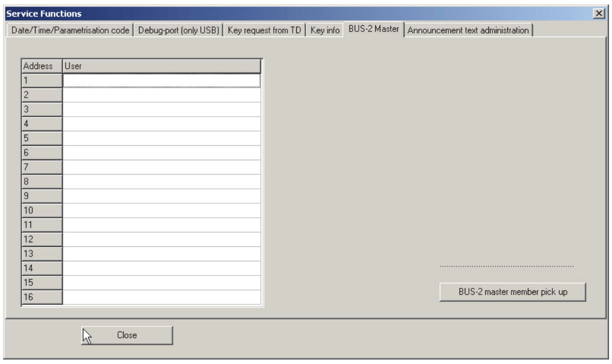


20.5 Tab “BUS-2 Master”

The "BUS-2 Master" tab opens the dialog box for detection of which BUS-2 users are connected to the BUS-2 connection of the transmission device.

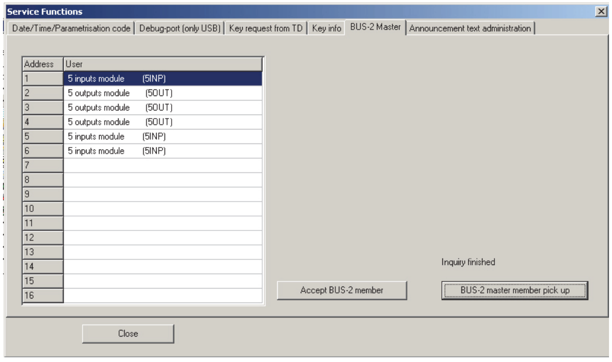
Determination of BUS-2 users only works with if BUS-2 master mode of the transmission device is activated (see Section 6.1.1.6).

- "BUS-2 master member pick up" button
  The connected BUS-2 users will be included and the sequence of the physical address is displayed.


Service Functions
Date/Time/Parametrisation code
Debug-port (only USB)
Key request from TD
Key info
BUS-2 Master
Announcement text administration
BUS-2 master member pick up
Close

Address	User
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	

- "Accept BUS-2 member" button
  The determined BUS-2 users are adopted in the programming of the BUS-2 master mode (see Section 15).

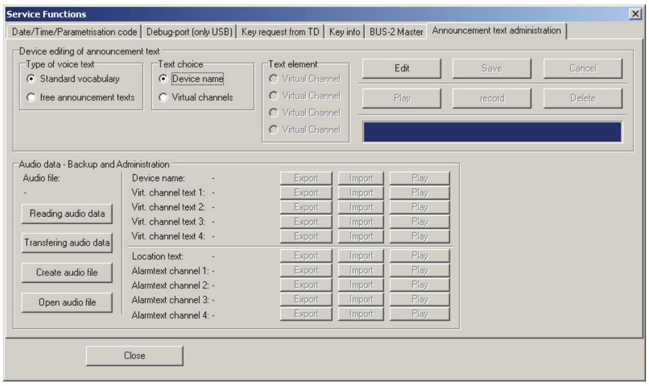


Address	User
1	5 inputs module (5INP)
2	5 outputs module (5OUT)
3	5 outputs module (5OUT)
4	5 outputs module (5OUT)
5	5 inputs module (5INP)
6	5 inputs module (5INP)
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	

Inquiry finished

20.6 Tab "Announcement text administration"

The "Announcement text administration" tab opens the dialog box for programming and backup/administration as well as recording the announcement texts.
The factory standard texts can be used and allocated in the "Options" tab during programming of message transmission.
If these default language texts do not meet customer requirements, it is possible to record custom text and thus individually design the announcement to a certain degree.
Text from the standard vocabulary and customized text can be recorded here.



Audio file:
-

Device name: -
Virt. channel text 1: -
Virt. channel text 2: -
Virt. channel text 3: -
Virt. channel text 4: -
Location text: -
Alarmtext channel 1: -
Alarmtext channel 2: -
Alarmtext channel 3: -
Alarmtext channel 4: -

20.6.1 Factory standard voice texts

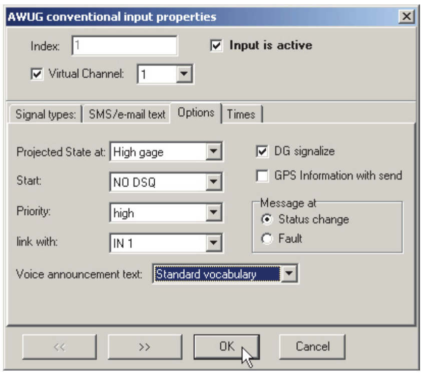
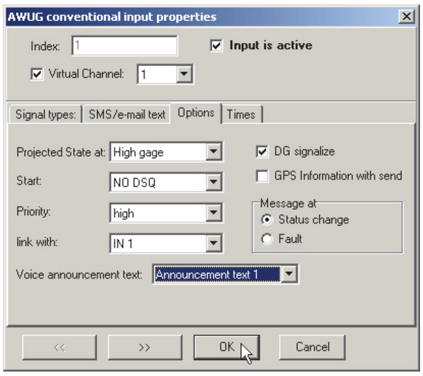
Inputs 1 to 9 for entry of the standard voice texts correspond to the virtual channels for programming the DS inputs (see Section 13). Depending on the programming for the "non-projected state VdS2465 (Sections 13.1 and 13.2), the following text takes the place of the "triggered" announcement:

Non-projected state VdS 2465	State	Text output
Protection area	Non projected state	Activated
	Projected state	Deactivated
Hold-up / intrusion	Non projected state	Alarm
	Projected state	Reset

In case of other programming, the announcement "triggered" is made in the "non-projected status" and the announcement "reset" is made once the "projected state" has been reached.

20.6.2 Overview of standard vocabulary - customized announcement texts

The texts of the standard vocabulary are allocated by programming the drop-down list field “Voice announcement text” to standard vocabulary and setting of channels 1 - 4 (virtual channel 1 - 4). If no customized text is programmed, then the factory standard text is issued and if a customized text has been programmed, then it will be used.
The customized announcement texts are allocated to the respective channels by programming the "Voice announcement text" drop-down list field to announcement text 1 - 4. The advantage of using customized announcement texts is the fact that they can be used (allocated) multiple times.

	Text type	Recording duration	Programming Transmission of messages
Standard vocabulary			 AWUG conventional input properties Index: 1 ☑ Input is active ☑ Virtual Channel: 1 Signal types: SMS/e-mail text Options Times Projected State at: High gage ☑ DG signalize Start: NO DSQ ☐ GPS Information with send Priority: high Message at ● Status change ○ Fault link with: IN 1 Voice announcement text: Standard vocabulary
	Device name	approx. 3.5 sec.	
	Virtual channel 1	approx. 3.5 sec.	
	Virtual channel 2	approx. 3.5 sec.	
	Virtual channel 3	approx. 3.5 sec.	
	Virtual channel 4	approx. 3.5 sec.	
Free announcement texts			 AWUG conventional input properties Index: 1 ☑ Input is active ☑ Virtual Channel: 1 Signal types: SMS/e-mail text Options Times Projected State at: High gage ☑ DG signalize Start: NO DSQ ☐ GPS Information with send Priority: high Message at ● Status change ○ Fault link with: IN 1 Voice announcement text: Announcement text 1
	Location text	max. 16.5 sec.	
	Announcement text 1	max. 4.1 sec.	
	Announcement text 2	max. 4.1 sec.	
	Announcement text 3	max. 4.1 sec.	
	Announcement text 4	max. 4.1 sec.	

20.7 Recording of customized voice information

A total of 10 customized texts with various durations per text can be stored. These can either be recorded and programmed directly using the transmission device of recorded using a PC and then copied to the transmission unit.

20.7.1 Requirements for recording the customized texts.

- Supply operating voltage (+12 V DC) to the transmission device.

- Connect the headset to the microphone and headphone jacks for recording and playback of the texts.
Headset specifications:
Headphone impedance. 200 Ohms
Microphone impedance: 2000 Ohms

- Switch PC/laptop on

- Launch WINFEM

- Connect USB cable (A-plug to B-plug) to the PC/laptop and the transmission device.

- “Announcement text administration” in the “Service functions” menu selection.

20.7.2 Record and playback the individual texts

- Procedure for recording and playback of the texts:
First select the required text by clicking on the radio buttons “Voice text type”, “Text selection” and “Text element”. To play the stored text, first click on the "Edit" button to load the audio data and then click on the “Play” button.

To record, click on the "Record" button. Recording is started immediately and therefore the voice message has to be spoken immediately after clicking on the button. Speak clearly and articulate, with a slightly raised voice as you would to a small group of listeners.
Observe the fact that only the respective recording time is available (see recording bar under the buttons).
If necessary, the recording procedure can be repeated by pressing the Record button each time.
After finishing the recording or playback procedure for the current text element, the text element is only saved permanently in the transmission device once the "Save" button has been clicked on. Another text element can then be selected, which can also be processed as described above.

If texts have been recorded or modified, it is essential that they be stored in the transmission device before the connection to WINFEM is terminated.
After all required texts have been recorded or played back, the headset can be removed.

The delete function may be required if no individual texts are required, but the transmission device was previously equipped with such text.

20.7.3 Audio data backup and administration

- Reading audio data

The audio data is transferred from the transmission device to the PC and saved in a file on the PC.

The connection type from the PC / laptop to the transmission device must be defined in the menu "Settings of the connection data to the system".

- Transferring audio data

The audio data is transferred from the PC to the transmission device.

- Create audio file

A new audio file (file extension .wfa) is created. A wfa audio file includes 10 “audio data segments” for the different text types and the respective recording durations.

- Open audio file

An existing audio file can be opened for further processing. The individual types of text can be checked by listening to them using the "Play" button. The individual audio files can be exported to wav format (wav file with CCITT A-Law 8kHz, 8 Bit, Mono encoding) using the “Export” button.
The “Import” button can be used to import existing audio file into the audio file.

For existing audio files, the maximum recording time and encoding of the individual text styles has to be observed! Longer recordings are automatically cut off. The standard Windows audio recorder is suitable for recording audio files. Observe the notes in the Help file of the audio recorder to record sound.

21. Message transmission and protocol structure

The following data protocols are transmitted to the alarm receiving centre (ARC).

21.1 Telim

Telim information

4+1Bit	Cause	'G'
3Byte	ID number	6 digits
1Byte	Record type	'ST'

Record type overview ('ST')

'A' Alarm,
'N' Hold-up,
'Q' Remote control
'W' zero setting

'K' Clear,
'S' In-house emergency call,

'L' Tech. Message
'F' Fault
'V' elevator emergency call
'1' Fire

Device-specific messages:

Low voltage
230 V fault
Battery fault
Telephone line fault
ST -> 'L' for non-projected state
ST -> 'K' for projected state
G -> Programmed 'Telim fault reason'

Bus fault
ST -> 'L' for non-projected state
ST -> 'K' for projected state
G -> 0x00 fault reason -> I-BUS, BUS-2
0x01 fault reason -> IACP RS232

Routine call
ST -> 'R'
G -> Programmed 'Telim routine call reason'

DS inputs, inputs from transmission device (outputs from IACP)
ST -> Programmed signal type
G -> Corresponds to input.
If input is greater than 16, then reason 16 is always transmitted

DS inputs, inputs from transmission device (function group outputs from IACP)
Are not transmitted via Telim

21.2 Contact ID

Contact ID
ACCT MT Q XYZ GG CCC

ACCT:	4 characters	Identification number (0-9, B-F)
MT:	2 characters	18
Q:	1 character	1 -> New event non-projected state or disarming 3 -> New event projected state or arming 6 -> Status messages
XYZ	3 characters	Event code (0-9, B-F)
GG	2 characters	Main zone. 00 if general message
CCC	3 characters	Detector group or Ident key ID data carrier system number

Low voltage

Q	= 1 / 3
XYZ	= 302 (Low System Battery)
GG	= 00
CCC	= 000

230 V fault

Q	= 1 / 3
XYZ	= 301 (AC Loss)
GG	= 00
CCC	= 000

Battery fault

Q	= 1 / 3
XYZ	= 311 (Battery Missing/Dead)
GG	= 00
CCC	= 000

Telephone line fault

Q	= 1 / 3	
XYZ	= 350 (Communication trouble)	
GG	= 00	
CCC	= 001	Telephone line fault

Routine call

Q	= 1
XYZ	= 602 (Periodic Test Report)
GG	= 00
CCC	= 000

Bus fault

Q	= 1 / 3
XYZ	= 300 (System trouble)
GG	= 00
CCC	= 000

DS inputs, inputs from transmission device (outputs from IACP)

Q	= 1 / 3	
XYZ	= Programmed Contact ID type	
GG	= 00	
CCC	= 001..008	Conventional inputs
	= 001..104	Bus-2 master inputs
	= 001..100	100 inputs from IACP

DS inputs, inputs from transmission device (function group outputs from IACP)

Q	= 1 / 3	
XYZ	= Programmed Contact ID type	
GG	= 00..16	Main zone
CCC	= 000..512	Detector group or
	= 000..512	Identkey ID data carrier system number

21.2.1 Contents of the Contact ID transmission code with function group programming

The following abbreviations are used:

MZ - Main zone
DG - detector group
IK - Identkey ID data carrier system number

Abbreviation	Signal	Triggering by	Contact ID message	
			GG	CCC
FRO	Free output			
EXAZ	Externally armed zone	Main zone externally armed	MZ	IK
EXDZ	Externally disarmed zone	Main zone externally disarmed	MZ	IK
IARZ	Internally armed zone	Main zone internally armed	MZ	0
INDZ	Internally disarmed zone	Main zone internally disarmed	MZ	0
INAZ	Internal alarm zone	Intrusion alarm Tamper alarm	MZ	DG
HUAZ	Hold-up alarm zone	Hold-up DG / hold-up code	MZ	DG
TAZ	Tamper alarm zone	Tamper DG / monitoring of signalling devices, switching devices, housings (BUS users)	MZ	DG
MALZ	Main alarm zone	Intrusion alarm Hold-up alarm Tamper alarm	MZ	DG
SIAZ	Siren alarm zone	Main alarm	MZ	DG
FLAZ	Flashlight alarm zone	Main alarm	MZ	DG
CALZ	Continuous alarm zone	Main alarm	MZ	DG
SAPZ	Store alarm pulse zone	Every alarm actuation	MZ	0
WATZ	Walk test zone	Switch on walk test	MZ	0
BUZZ	Buzzer zone	actuation zone buzzer	MZ	0
IADG	Internal alarm detector group	Intrusion alarm detector group x Tamper alarm detector group x	MZ	DG
MADG	main alarm detector group	Intrusion alarm detector group x Hold-up alarm detector group x Tamper alarm detector group x	MZ	DG
OSDG	ON-state detector group	Detector group x actuated	MZ	DG
DIDG	Disarmed detector group	Detector group x disarmed	MZ	DG
DADG	Disabled detector group	Detector group x disabeled (Internal / external)	MZ	DG
DGDI	Detector group display	Actuation LED indication detector group x	MZ	DG
AWIA	AWUG intrusion alarm zone	Intrusion alarm (main alarm) Zone x	MZ	DG
AWHA	AWUG hold-up alarm zone	Hold-up alarm zone x	MZ	DG

Abbreviation	Signal	Triggering by	Contact ID message	
			GG	CCC
AWTA	AWUG tamper alarm zone	Tamper alarm zone x (Pre-/main alarm)	MZ	DG
AWTM	AWUG tamper main alarm zone	Tamper alarm zone x (Main alarm)	MZ	DG
AWDG	AWUG detector group alarm	Main alarm from detector group x	MZ	DG
IDDG	Internally disabled detector group	Internal disabling of detector group x	MZ	DG
EDDG	Externally disabled detector group	External disabling of detector group x	MZ	DG
DMDG	Detector monitoring detector group	Activation detector group of a mini module by input 2 of the mini module	MZ	DG

21.3 VdS 2465 message structure record type 0x02

Messages are transmitted with set type 0x02 (message state change with acknowledgment request) of the VdS 2465 protocol. the set type 0x02 is structured as follows.

G/B Device / zone	A Address	AZ Address addition	AR Address extension	MA Message type
1 Byte	1 Byte	1Byte	1 Byte	1 Byte

The table shows the possible events of the transmission device and the respective VdS 2465 message with set type 0x02:

	G/B	A	AZ	AR	MA
Low voltage	0/0	0	0	1	0x37
230 V fault	0/0	0	0	1	0x32
Battery fault	0/0	0	0	1	0x33
Telephone line fault	0/0	0	0	1	0x34
Routine call	Special case set type 0x40 (test message)				
BUS fault	0/0	0	0	1	0x31
DS inputs (Outputs from IACP)	1/0	1..100 a*	0	1	0x00..0x7F b*
DS inputs (function groups outputs from IACP)	Function groups outputs from IACP are **not** transmitted according to VdS 2465!				

a* - output numbers of the "Outputs from IACP" programming.
b* - Programmed VdS 2465 state.

21.4 Messages for status changes of the transmission paths

Messages for status changes of the transmission paths

	Record type	Device/Zone	Address	Address addition	Address extension	Message type	Record type	Identifier	Record type	Identifier
GSM fault	0x02 Message with acknowledgement request	0x00	0x00	0x00	0x01	0x3B Fault transmission path 2	0x60 Network status	0x08 Failure	0x61 Transport service identifier	0x80 Mobile radio
GSM fault resetted	0x02 Message with acknowledgement request	0x00	0x00	0x00	0x01	0x6B Fault transmission path 2 Rectified (ok gain)	0x60 Network status	0x00 Gut	0x61 Transport service identifier	0x80 Mobile radio

	Record type	Device/Zone	Address	Address addition	Address extension	Message type	Record type	Identifier	Record type	Identifier
PSTN fault	0x02 Message with acknowledgement request	0x00	0x00	0x00	0x01	0x34 Fault transmission path	0x60 Network status	0x08 Failure	0x61 Transport service identifier	0x20 PSTN
PSTN fault resetted	0x02 Message with acknowledgement request	0x00	0x00	0x00	0x01	0x64 Fault transmission path Rectified (ok gain)	0x60 Network status	0x00 Rectified (ok gain)	0x61 Transport service identifier	0x20 PSTN

	Record type	Device/Zone	Address	Address addition	Address extension	Message type	Record type	Identifier	Record type	Identifier
Ethernet fault	0x02 Message with acknowledgement request	0x00	0x00	0x00	0x01	0x3B Fault transmission path 2	0x60 Network status	0x08 Failure	0x61 Transport service identifier	0x90 TCP/IP
Ethernet fault resetted	0x02 Message with acknowledgement request	0x00	0x00	0x00	0x01	0x6B Fault transmission path 2 Rectified (ok gain)	0x60 Network status	0x00 Rectified (ok gain)	0x61 Transport service identifier	0x90 TCP/IP

Messages for fault of the dedicated line via redundant transmission path
<u>(Rectified message (ok gain) of the redundant transmission path)</u>

	Record type	Gerät/Bereich	Address	Address addition	Address extension	Message type	Record type	Identifier	Record type	Identifier
IP Connection fault	0x02 Message with acknowledgement request	0x00	0x00	0x00	0x01	0x64 Fault transmission path Rectified (ok gain)	0x60 Network status	0x08 Failure	0x61 Transport service identifier	0x90 TCP/IP

In addition to the above indicated record types following record types are transmitted:

Priority	0x01	Manufacturer ID	0x51
Date Time	0x50	ID Number	0x56

22. Address structures for VdS 2465

When connecting to a VdS 2465 compatible control center, the following addresses are used.

22.1 Addresses for the activation criteria and control outputs of the transmission device

Criterion	Used address for VdS 2465				
	Device	Zone	Address	AZ*	Identification
System messages of the transmission device (e.g. power failure, etc.)	0	0	0	0	10
Detector group 1	0	1	1	0	1
Detector group 2	0	1	2	0	1
Detector group 3	0	1	3	0	1
Detector group 4	0	1	4	0	1
Detector group 5	0	1	5	0	1
Detector group 6	0	1	6	0	1
Detector group 7	0	1	7	0	1
Detector group 8	0	1	8	00	1
Control output 1	0	1	1	0	2
Control output 2	0	1	2	0	2

* = Address suffix

22.2 Addresses for the inputs and outputs of the 5-input modules and 5-output modules (transmission device operating mode: BUS-2 master mode)

Regardless of the module type (5-input module / 5-output module) 6 inputs and 6 outputs are reserved for each bus module and address assignment is as follows:

The inputs of the first module (BUS address 1) have the VdS addresses 9 - 13, the cover contact of the first module has the address 14.
The inputs of the second module (BUS address 2) have the VdS addresses 15 - 19, the cover contact of the first module has the address 20, etc.

Output addresses are also reserved for the input modules, but they are not used except for the buzzer. The buzzer of the first module has the address 8 regardless of whether this is an input or output module.

Table: VdS 2465 address allocation for the users

User	Criterion	Address formula for address	Used address for VdS 2465				
			Device	Zone	Address	AZ*	Identification
BUS 2 5-input module Bus address 1 (=n)	Detector group 1	n x 6 + 3	0	1	9	0	1
	Detector group 2	n x 6 + 4	0	1	10	0	1
	Detector group 3	n x 6 + 5	0	1	11	0	1
	Detector group 4	n x 6 + 6	0	1	12	0	1
	Detector group 5	n x 6 + 7	0	1	13	0	1
	Cover switch	n x 6 + 8	0	1	14	0	1
	Control output 1		Not available				
	Control output 2						
	Control output 3						
	Control output 4						
	Control output 5						
	Buzzer	n x 6 + 2	0	1	8	0	2
BUS 2 5-output module Bus address 2 (=n)	Detector group 1		Not available				
	Detector group 2						
	Detector group 3						
	Detector group 4						
	Detector group 5						
	Cover switch	n x 6 + 8	0	1	20	0	1
	Control output 1	n x 6 - 3	0	1	9	0	2
	Control output 2	n x 6 - 2	0	1	10	0	2
	Control output 3	n x 6 - 1	0	1	11	0	2
	Control output 4	n x 6	0	1	12	0	2
	Control output 5	n x 6 + 1	0	1	13	0	2
	Buzzer	n x 6 + 2	0	1	14	0	2
BUS 2 5-input module Bus address 3 (=n)	Detector group 1	n x 6 + 3	0	1	21	0	1
	Detector group 2	n x 6 + 4	0	1	22	0	1
	Detector group 3	n x 6 + 5	0	1	23	0	1
	Detector group 4	n x 6 + 6	0	1	24	0	1
	Detector group 5	n x 6 + 7	0	1	25	0	1
	Cover switch	n x 6 + 8	0	1	26	0	1
	Control output 1		Not available				
	Control output 2						
	Control output 3						
	Control output 4						
	Control output 5						
	Buzzer	n x 6 + 2	0	1	20	0	2

* = Address suffix

23. Troubleshooting and diagnostic mode

Often the indication facilities on the transmission device are not sufficient for detailed troubleshooting. Thus the display "RDT fault" can refer to PSTN, Ethernet and/or GSM.
For an exact determination of the fault, a special diagnostic mode can be activated via WINFEM (debug).
For an exact determination of the fault, a graphical diagnostic mode or a special diagnostic mode can be activated via WINFEM (debug). For this, the transmission device must be connected via USB with the PC/laptop.

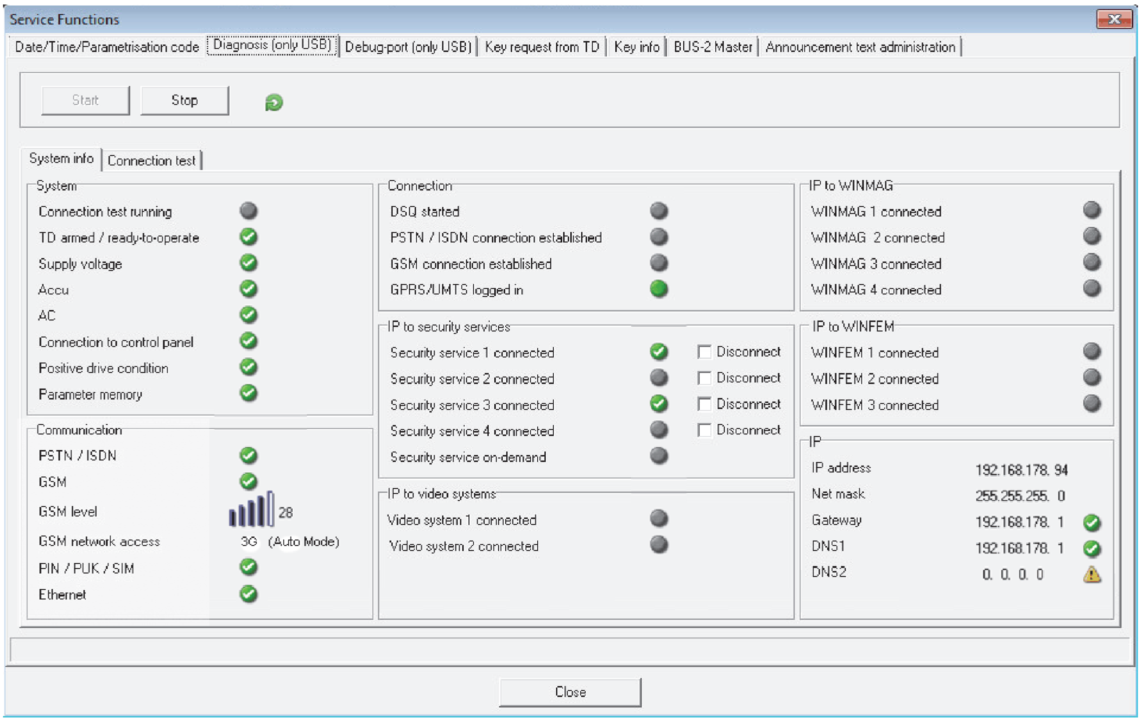
Functions which are not activated in the device and which are therefore not relevant for correct functioning of the device, are not relevant to observe.

23.1 Diagnosis

The graphical Diagnosis-window can be opened in the way described in chapter 20.2.

- Button Start

Starts the diagnostic mode and displays the status on the basis of graphic elements:



Service Functions

Date/Time/Parametrisation code | Diagnosis (only USB) | Debug-port (only USB) | Key request from TD | Key info | BUS-2 Master | Announcement text administration

Start | Stop

System info | Connection test

System
Connection test running ●
TD armed / ready-to-operate ✓
Supply voltage ✓
Accu ✓
AC ✓
Connection to control panel ✓
Positive drive condition ✓
Parameter memory ✓

Communication
PSTN / ISDN ✓
GSM ✓
GSM level 28
GSM network access 3G (Auto Mode)
PIN / PUK / SIM ✓
Ethernet ✓

Connection
DSQ started ●
PSTN / ISDN connection established ●
GSM connection established ●
GPRS/UMTS logged in ●

IP to security services
Security service 1 connected ✓ □ Disconnect
Security service 2 connected ● □ Disconnect
Security service 3 connected ✓ □ Disconnect
Security service 4 connected ● □ Disconnect
Security service on-demand ●

IP to video systems
Video system 1 connected ●
Video system 2 connected ●

IP to WINMAG
WINMAG 1 connected ●
WINMAG 2 connected ●
WINMAG 3 connected ●
WINMAG 4 connected ●

IP to WINFEM
WINFEM 1 connected ●
WINFEM 2 connected ●
WINFEM 3 connected ●

IP
IP address 192.168.178. 94
Net mask 255.255.255. 0
Gateway 192.168.178. 1 ✓
DNS1 192.168.178. 1 ✓
DNS2 0. 0. 0. 0 ⚠

Close

Function field	Function	Status display
System	Connection test running	red indicator ➜ active grey indicator ➜ inactive
	TD armed / ready-to-operate	green check ➜ transmission device armed yellow triangle ➜ transmission device disarmed
	Supply voltage	green check ➜ OK yellow triangle ➜ Warning
	Accu	green check ➜ OK yellow triangle ➜ Warning
	AC	green check ➜ OK yellow triangle ➜ Warning
	Connection to contol panel	green check ➜ OK yellow triangle ➜ Warning

	Positive drive connection	green check ➜ OK yellow triangle ➜ Warning
	Parameter memory	green check ➜ OK yellow triangle ➜ Warning
Communication	PSTN / ISDN	grey indicator ➜ inactive / not available / line monitoring off green check ➜ OK yellow triangle ➜ Fault
	GSM	grey indicator ➜ inactive / not available / line monitoring off green check ➜ OK yellow triangle ➜ Fault
	GSM level	Indicator bar ➜ shows graphically and as a value, the received field strength of the GSM module.
	GSM network access	Text (e.g. 3G) ➜Shows the currently used / embedded network. In the brackets, the actual programmed parameter is shown.
	PIN / PUK / SIM	green check ➜ OK yellow triangle ➜ Fault / PIN wrong or PUK expected / SIM missing
	Ethernet	grey indicator ➜ inactive / not available / line monitoring off green check ➜ OK yellow triangle ➜ Fault
Connection	all states	green indicator ➜ started / in work / established grey indicator ➜ not started / not established
IP to	all states	green check ➜ established grey indicator ➜ not established / not available
IP	all states	green check ➜ active yellow triangle ➜ fault / not established

- Button Stop

  Stops the diagnostic mode.

The graphical Diagnosis-window shows the live state of the transmission device. Changes of the state of the transmission device are displayed simultaneously or time-delayed (e.g. Fault of Mains-/ or Battery).

If the transmission device is equipped with a GSM-module (e.g. RFW-4000), the value of the received field strength of the GSM level in the field communication is read in only once a time during the start of the diagnosis modus.

- Checkbox Disconnect

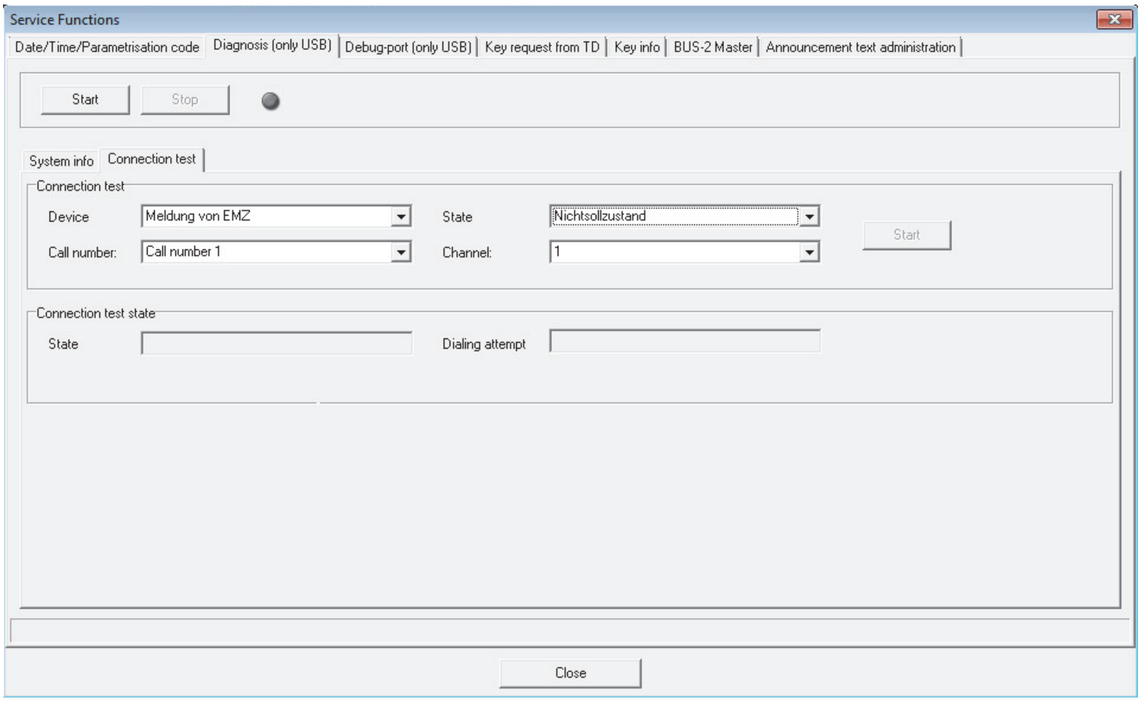
  By selecting individual connections a dedicated line connection can be interrupted to test the function of the redundant transmission way to another IP-Connection.

23.1.1 Connection test

First start the diagnosis mode then the Connection test can be used.
During the connection tests, all LEDs of the transmission device flash in seconds cycle.

With the tab Connection test different states can be transmitted to Call numbers for test proposes. After selecting the device, the state, the call number and the transmission channel start the test with the button Start.

If the alarm receiving center request a specific message, it can be defined here and transmitted via the call number. In the field connection test state a successful or failed transmission is displayed.



Connection test

Device: Meldung von EMZ

State: Nichtsollzustand

Call number: Call number 1

Channel: 1

Connection test state

State:

Dialing attempt:

23.2 Notes regarding European standards

EN

- A code with at least 6 characters must be saved for remote parameterization. This guarantees 1,000,000 variables for remote access.
- If three successive attempts are made to access the DS 6700 with an incorrect code for remote parameterization, a blocking period of 90 seconds begins.
- Routine calls must be parameterized in categories DP2 to DP4 with: Missing acknowledgement of routine call sets the associated dedicated IP connection to fault.
- If the serial interface is used, the routine only needs to be parameterized when BUS communication is working.

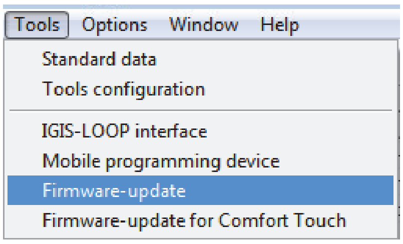
EN EN - conform programming by category:

SP2:	SP3:	SP4 … SP6:
Possible call numbers: • PSTN VdS2465, • PSTN Telim, • PSTN Contact ID, • GSM VdS2465, • GSM Telim, • GSM Contact ID • IP demand-actuated Ethernet VdS2465 • IP demand-actuated GPRS/UMTSVdS2465 • IP dedicated Ethernet VdS2465 • IP dedicated GPRS/UMTS VdS2465 DSQ for ALARM: • DSQ 1 Monitoring time: • GSM 18h • IP dedicated 18h • Ethernet 18h • PSTN 18h Routine call: • Distance 24h • DSQ 1	Possible call numbers: • dedicated IP Connection 1 -IP dedicated Ethernet VdS2465 -IP dedicated GPRS/UMTS VdS2465 DSQ for ALARM: • DSQ 1 -dedicated IP Connection 1 Monitoring time: • GSM 30min • Ethernet 30min • dedicated IP Connection 1, 30min	Possible call numbers: • dedicated IP Connection 1 -encrypted IP dedicated Ethernet VdS2465 -encrypted IP dedicated GPRS/UMTS VdS2465 DSQ für ALARM: • DSQ 1 -dedicated IP Connection 1 Monitoring time SP4: • GSM 3min • Ethernet 3min • dedicated IP Connection 1, 3min Monitoring time SP5: • GSM 90sek • IP dedicated 90sek • Ethernet 90sek • dedicated IP Connection 1, 90sek Monitoring time SP6: • GSM 20sek • IP dedicated 20sek • Ethernet 20sek • dedicated IP Connection 1, 20sek
DP2:	**DP3:**	**DP4:**
Call numbers First transmission path: • dedicated IP Connection 1 -IP dedicated Ethernet VdS2465 Call numbers Second transmission path: • demand-actuated IP Connection -GPRS/UMTS VdS2465 • dedicated IP Connection 2 (redundant to Connection 1) -IP dedicated GPRS/UMTS VdS2465 DSQ: • DSQ1 für Alarmübertragung -First transmission path oder Second transmission path (dedicated) or Second transmission path (demand actuated) • DSQ2 für Routine call -Second transmission path (dedicated) oder Second transmission path (demand actuated) Monitoring time: • First transmission path -Ethernet 30min -dedicated IP Connection 1, 30min • Second transmission path -GSM 18h -dedicated IP Connection 2, 30min Routine calls: • Routine call 1 for monitoring Second transmission path -Distance 24h -DSQ 2	Call numbers First transmission path: • dedicated IP Connection 1 -encrypted IP dedicated Ethernet VdS2465 Call numbers Second transmission path: • demand-actuated IP Connection -encrypted GPRS/UMTS VdS2465 • dedicated IP Connection 2 (redundant to Connection 1) -encrypted IP stehend GPRS/UMTS VdS2465 DSQ: • DSQ1 für Alarmübertragung -First transmission path or Second transmission path (dedicated) oder Second transmission path (demand actuated) • DSQ2 für Routine call -Second transmission path (dedicated) or Second transmission path (demand actuated) Monitoring time: • First transmission path -Ethernet 3min -dedicated IP Connection 1, 3min • Second transmission path -GSM 18h -encrypted dedicated IP Connection 2, 3min Routine calls: • Routine call 1 for monitoring Second transmission path -Dictance 24h -DSQ 2	Call numbers First transmission path: • dedicated IP Connection 1 -encrypted IP dedicated Ethernet VdS2465 Call numbers Second transmission path: • Demand actuatede IP Connection -encrypted GPRS/UMTS VdS2465 • dedicated IP Connection 2 (redundant to Connection 1) -encrypted IP dedicated GPRS/UMTS VdS2465 DSQ: • DSQ1 für Alarmübertragung -First transmission path oder Second transmission path (dedicated) oder Second transmission path (demand actuated) • DSQ2 für Routine call -Second transmission path (dedicated) oder Second transmission path (demand actuated) Monitoring time: • First transmission path -Ethernet 90sek -encrypted dedicated IP Connection 1, 90sek • Second transmission path -GSM 5h min -encrypted dedicated IP Connection 2, 90sek Routine calls: • Routine call 1 for monitoring Second transmission path -Distance 4h -DSQ 2

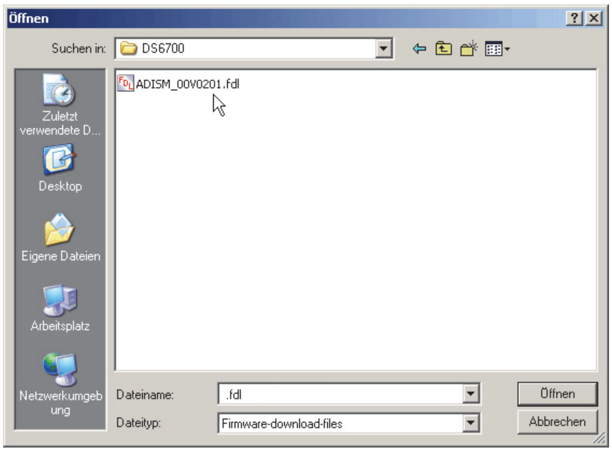
23.3 Debug interface

The debug input window can be alternatively opened by the route described in Section 20.2.

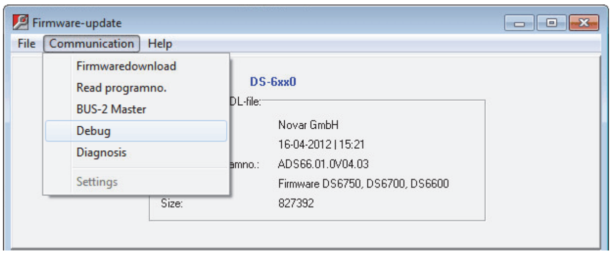
1. Activating the "Firmware update menu“ via the menu “Tools” -> “Firmware-Update (FFAST)”.
   The update menu is opened, at the same time the available update files are displayed. You can use the known Windows mechanisms in order to change to another directory if another file than the one offered in the current directory is to be used.



   Double clicking loads the respective firmware file (ADIST...) into the transmission menu.



   Then start the debug mode via menu "Communication" -> command "Debug".



DS-6xx0

DL-file:

Novar GmbH

16-04-2012 | 15:21

amno.: ADS66.01.0V04.03

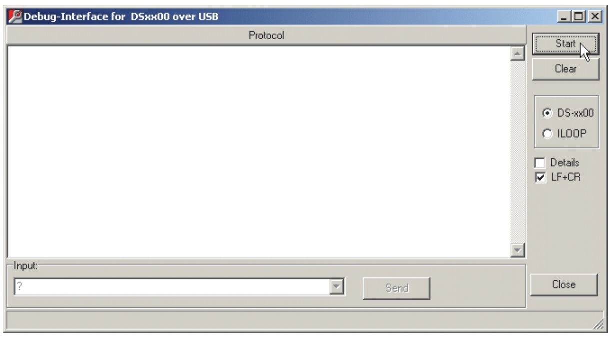
Firmware DS6750, DS6700, DS6600

Size: 827392

2. This opens the debug input window.

   The checkbox "LF-CR" and the device version (DS xx00) must be selected.
   When the "Start" button is clicked, the information "connected" is displayed.

   The debug interface via the existing USB connection is opened.



3. The drop-down list field "Input" is available for entering the debug commands. For making the entries, click into the drop-down list field, make the relevant entry and complete it by either actuating the "Return" key or the "Send" button.

The **syntax must be strictly observed** when entering the Debug commands.
The following commands are available for activating the individual diagnostic modes or outputs:

?: Output of the supported debug instructions
With entry of ? When ? is entered (confirm with “Return” key), the commands which are accepted by the device are displayed.

```
?
INFO            Information pertaining to the system state
TIME     Retrieval of system time
TIME s          Send time query to NTP server
TRACE    Recording of  VDS2456 messages and system information
STACK    User stack of the individual tasks
VER      Version and device information display
MESSAGE         Creation of (test) messages
SWITCH   Switching channels
STATUS          Statuses of connections or inputs and outputs
MEMINFO         Information pertaining to dynamic memory
NETINFO         Information pertaining to the IP network
PING     Send PING to an IP address
CON      Control dedicated IP connections
STANDBY  Arm/disarm transmission device
```

INFO: The conditions which might cause a fault are output.

Example:
Entry: info (confirm with “Return” key)

```
info
TELEPHON: Good
GSM: Good 18        -> The number in the entered GSM line indicates the received field strength of the GSM module!
TCP: Good
POWER: Good
UNDERVOLTAGE: Good
AKKU: Good
DATA BUS: Good
PARAMETER: Good
VOICE MODUL: Good
CODE MODUL: Good
BLOCKING TIME*
```

Functions which are not activated in the device and which are therefore not relevant for correct functioning of the device, are marked as not relevant by ---.

*Note of blocking time: After 3 incorrect WINFEM connection attempts, no more connections are accepted for a period of 30 minutes. If this is the case, then the remaining time in which no calls will be accepted is displayed here.

TIME: shows the date and time of the real-time clock of the device

Example:
time (confirm with “Return” key)

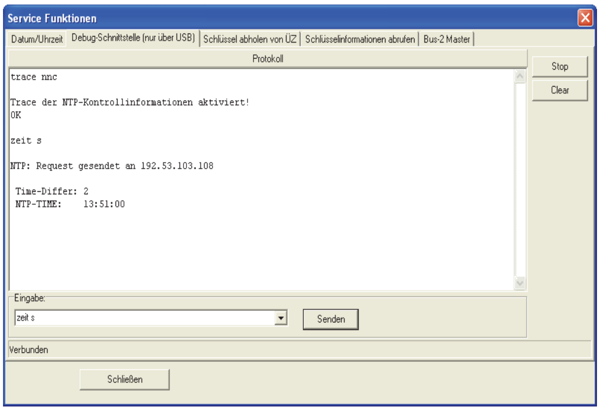
```
13:24:02   Tu 21.11.05
```

TIME s: This command can be used to send a time request to the NTP service if there is an active dedicated IP connection to a receiving control panel and programmed NTP server. If the time difference between the transmission device and NTP server is more than 30 seconds, then the transmission device will adopt the NTP time. If the “trace nnc” is entered previously, then evaluation can be traced in the debug window:

Example:

Entry: trace nnc (confirm with the “Return” key)
Entry confirmation is carried out with OK
Entry: time s (confirm with “Return” key), time request is sent to the NTP server.

Time-Differ: 2 (output of the time difference between the transmission device and the NTP server)



```
trace nnc

Trace der NTP-Kontrollinformationen aktiviert!
OK

zeit s

NTP: Request gesendet an 192.53.103.108

 Time-Differ: 2
 NTP-TIME:    13:51:00
```

Eingabe: zeit s

Verbunden

TRACE S/X/B/G/E/N

With the Trace command, the different protocol analyzers of the device can be activated.
When the debug instruction "Trace“ has been entered, the possible trace functions are displayed as a kind of help function. Meaning of the individual "Trace commands”:

TRACE S	Recording of system information
TRACE B	Recording of the B channel VDS2465 usage data
TRACE G	Recording of the GSM VDS2465 usage data
TRACE E	Recording of the IACP I-BUS / BUS-2 information
TRACE Nxyz	Invokes the network trace function:

x: Protocol (layer)
A -> ARP, E -> Ethernet, I -> IP, T -> TCP, U -> UDP, V -> VdS2465, M -> E-Mail,
P -> PPP, N -> NTP, D -> DNS

y: Type of information
C -> Control information, D -> (usage) data

z: Output ON or OFF
nothing or + -> on, – -> off

Example 1: TRACE NVD + -> Switch on output of the VdS2465 usage data
TRACE – -> End tracing

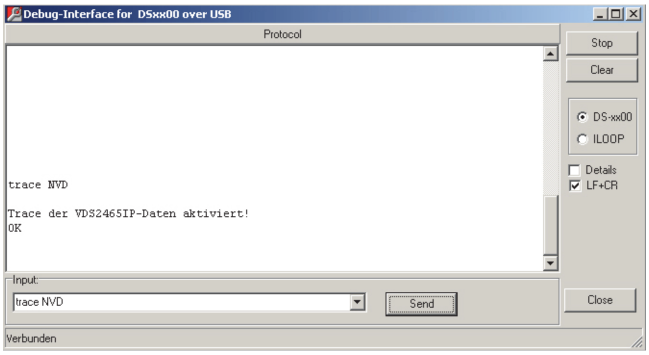
Example 2: TRACE NMC + -> Switch on output of data transmission to the e-mail server
TRACE – -> End tracing

The Trace function can be useful when there are problems with the transmission of messages to the control center.

Example:
Entry: trace NVD (terminate with "Return" key), entries are confirmed with OK

Subsequent activation of the transmission device (message to control center) causes display and output of the data transfer.

The trace mode has to be deactivated by entering "Trace –".



```
trace NVD

Trace der VDS2465IP-Daten aktiviert!
OK
```

● DS-xx00
○ ILOOP
□ Details
☑ LF+CR

Input: trace NVD

Verbunden

VER: Shows the versions of the individual software module. In addition to this, other device-specific information such as serial number, device type etc. are output.

Example:

```
ver (confirm with “Return” key)
Bootloader: ABOTL.00.0V03.00
Firmware: ADIST.10.0V03.00
CHK: DB00
Voice module: ADISM.00.0V02.00
System: DS 7700
MAC: 00 50 5E 1F E0 2F
ID:FFFF
Snr:FFFFFF
Date: FF FF
Location: 0F
Circuit board:
```

MESSAGE G A NR Z: The state of individual detector groups can be simulated with this instruction. Therefore it is possible to test the transmission behaviour of the device without the necessity to change the physical state of the detector group inputs. If a Trace has been activated before the simulation, the relevant data transfer can be viewed.

```
MESSAGE G A NR Z      Create a message
 G:         Device (0 DS, 1 hazard detection systems)
 A:         Message type
            M -> Message channel
             T -> Routine call
 NR:        Channel number (2 digits 01..99) etc.
            Routing call module (2 digits for routine call cycle 01..04)
 Z:         State
             1 --> Non-projected state
             0 --> Projected state
```

Example:

```
message 0 m 08 1 (terminate with "Return” key)
OK
```

This command simulates triggering of detector group 8 of the transmission device.

```
message 1 m 14 0 (terminate with "Return” key)
OK
```

This command simulates resetting of detector group 14 of the intruder alarm system.

SWITCH G NR Z:permits the activation or deactivation of control outputs.

```
SWITCH G NR Z      Generate a message
 G:         Device (0 DS, 1 hazard detection systems)
 NR:        Channel number (2 digits 1..99)
 Z:         State
            1 --> on
    0 --> off
```

Example:

```
switch 0 09 1 (confirm with “Return” key)
OK
```

The control output 09 is switched on. (09 is the output of a BUS-2 5-output module here)

```
switch 0 09 0 (confirm with “Return” key)
OK
```

The control output 09 is switched off

STATUS E/A/I: Used for displaying the state of the detector group inputs and status indicator active IP connections.

STATUS E	State of the inputs
STATUS A	State of the outputs
STATUS I	Status of the TCP/IP connections
STATUS -	Switch off status information display

Status detector group inputs:
When "Status e“ has been entered for activation, first the current state of all active detector inputs of the device is output. The inputs of BUS-2 modules that might be available are also taken into account.
Then the device will remain in status "display input status"; whenever there is a change of an input, this will be displayed accordingly.
This mode can be terminated by entering "Status -“.

Example:

```
status e (confirm with “Return” key)
OK
Input 001: High     M:-- A:--  V:1
Input 002: High     M:-- A:--  V:2
Input 003: High     M:-- A:--  V:3
Input 004: High     M:-- A:--  V:4
Input 005: High     M:-- A:--  V:5
Input 006: High     M:-- A:--  V:6
Input 007: High     M:-- A:--  V:7
Input 008: High     M:-- A:--  V:8
Cover contact 014: Termination M:01 A:06  V:-
Input 015: Termination M:02 A:01  V:-
Input 016: Termination M:02 A:02  V:9
Input 017: Termination M:02 A:03  V:-
Input 018: Termination M:02 A:04  V:-
Input 019: Termination M:02 A:05  V:-
Cover contact 020: Termination M:02 A:06  V:-
Input 001: Low      M:-- A:--  V:1
Input 001: High     M:-- A:--  V:1
```

M: Module address
A: Number of the input
V: Virtual channel

```
status I (confirm with “Return” key)
OK
01: IP connection NSL 1, dedicated: offline
02: IP connection NSL 2, dedicated: offline
03: IP connection NSL X demand-actuated: offline
04: IP connection              (03): offline
05: IP connection              (04): offline
06: IP connection              (05): offline
07: IP connection              (06): offline
08: IP connection              (07): offline
09: IP connection              (08): offline
10: IP connection              (09): offline
11: IP connection              (10): offline
12: IP connection              (11): offline
13: IP connection              (12): offline
14: IP connection VIDEO 1          : offline
15: IP connection VIDEO 2          : offline
status a (confirm with “Return” key)
OK
Output 001: Off     M:-- A:--  V:1
Output 002: Off     M:-- A:--  V:2
Output 003: Off     M:01 A:01  V:-
Output 004: Off     M:01 A:02  V:-
Output 005: Off     M:01 A:03  V:-
Output 006: Off     M:01 A:04  V:-
Output 007: Off     M:01 A:05  V:-
Buzzer 008: Off     M:01 A:06  V:-
Buzzer 014: Off     M:02 A:06  V:-
```

MEMINFO:

Is only required for in-house factory testing functions.

Example:
meminfo (confirm with “Return” key)

```
Data of dynamic memory allocation:
Free memory:  97656
Largest block:  97656
Memory check:   OK
```

NETINFO:

Returns information about the connected IP network.

Invoking NETINFO:

```
 NETINFO A  -> ARP table output
 NETINFO E  -> Ethernet information output
 NETINFO I   -> IP connections output
 NETINFO P  -> PPP connections output
 NETINFO T  -> TCP connections output
 NETINFO U  -> UDP connections output
```

Example:
netinfo t (confirm with “Return” key)

```
Occupied TCP sockets:
Rem. IP address RPort LPort Type  State     MTU   Wnd txCnt rxCnt Alive IdleT
 165.195.20.166  5001  1025 Cli.  CONNECT   512  2048     0     0   400   300
 165.195.20.166  5001  1026 Cli.  CONNECT   512  2048     0     0   400   300
End of the list.
OK
```

PING:

Can be used for example if the IP address of the receiving device is to be tested.

Invoking of PING with optional routeway entry (interface):

```
0  -> Ethernet
1  -> PSTN-PPP
2  -> GPRS-PPP
```

Example:

```
ping 165.195.20.166 0
```

```
Ping is sent to address 165.195.20.166 via interface 0...
 1: Ping response time from 165.195.20.166: 5 ms
 2: Ping response time from 165.195.20.166: 4 ms
 3: Ping response time from 165.195.20.166: 4 ms
 4: Ping response time from 165.195.20.166: 5 ms
OK
```

CON V KK Z: Used for simulation of connection faults with dedicated line connections.

This debug function can be used to disconnect individual dedicated line connections to test the function of the dual path signaling back-ups.

This can be used to check whether transmission via the PSTN channel in case of failure of a dedicated connection via IP.

V: Connection type
I -> IP connection
KK: Connection no.
Z: State
- -> Disconnect and block connection
+ -> Restore connection

Example:
con I 01 - (confirm with "Return" key)
OK
con I 01 + (confirm with "Return" key)
OK

The connection always has to be restored after testing, (entry: con I 01 **+**).

STANDBY:	Arm/disarm transmission device	
	standby a	Arm transmission device
	standby e	Disarm transmission device

24. Appendix

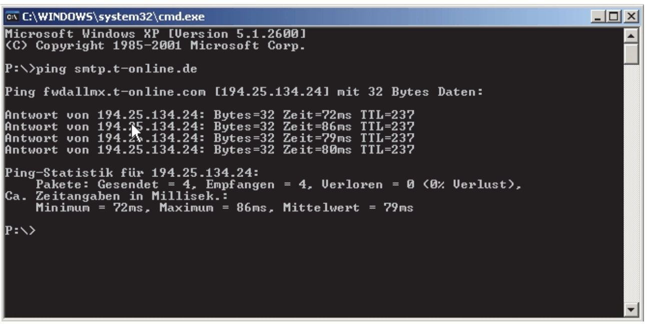
24.1 Converting a domain name into an IP address - determining numeric IP address

A numeric IP address can be entered in some cases to configure the NTP server address, the SMTP server name and the POP3 server name. Conversion of the IP address, which is usually described as the domain name, can be determined as follows using a PC/laptop with an Internet connection:

- Click on the Start button in WINDOWS.
- Click on "Run".
- Enter "cmd" and press the "Enter" key.

If you are looking for the numeric IP address of the SMTP outgoing mail server of t-online, then "ping" is to be entered followed by the server name (in this example smtp.t-online.de):

Entry of "ping smtp.t-online.de" and pressing the Enter key. The screen should display the following (the IP address may differ, it serves as an example):



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

P:\>ping smtp.t-online.de

Ping fwdallmx.t-online.com [194.25.134.24] mit 32 Bytes Daten:

Antwort von 194.25.134.24: Bytes=32 Zeit=72ms TTL=237
Antwort von 194.25.134.24: Bytes=32 Zeit=86ms TTL=237
Antwort von 194.25.134.24: Bytes=32 Zeit=79ms TTL=237
Antwort von 194.25.134.24: Bytes=32 Zeit=80ms TTL=237

Ping-Statistik für 194.25.134.24:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 72ms, Maximum = 86ms, Mittelwert = 79ms

P:\>
```

The resolved IP address is important for the entry:
In this example: 194.25.134.24
This returned IP address corresponds to the domain name "smtp.t-online.de" and can be entered in WINFEM for example.

If possible, the domain should always be used for NTP, SMTP, and POP3 addresses to allow the provider to perform load balancing or redundancy functions.

24.2 IP transmission of messages - Requirements and guidelines according to the VdS

The following notes to the guidelines 2471-S1 correspond to the state 2015-06(01). Find out about the latest guidelines and requirements that correspond to the current application. You will also find programming examples and instructions for programming the transmission device here.

24.2.1 Requirements IP Single path ATS SP4 (only VdS-Class A)

Requirements according to 2471-S1
For remote alarm, different transmission paths can be used within alarm transmission systems (ATS).

The description first transmission path or second transmission path refers to the communication interfaces of the supervised premises transceicer (SPT).

The paths are divided into two types of connection:

- **IP Single path ATS SP4**

The transmission path must be approved in accordance with VdS 2471-S1. With ≤25-hour routine call and 180 sec. function monitoring and at least 97% availability in a 7-day period.

- **IP Dual path ATS DP4**

One transmission path must be approved in accordance with VdS 2471-S1. The second transmission path must at least meet the requirements of DIN EN 50136. An ATP must be supplied with emergency power (SPT, ATS…). Function monitoring of first transmission path 90 sec. Function monitoring of second transmission path when untroubled 5 hours and with troubled first transmission path 90 sec. Switching from the troubled first transmission path to the second transmission path within 90 sec. Availability at least 99.8% in a 7-day period.

Arming prevention: With disarmed alarm panel, a failure of both transmission paths must lead to an arming prevention. If one transmission path fails, no arming prevention is required for a maximum period of 36 hours.

24.2.1.1 Requirements IP Single path ATS SP4 (Only VdS-Class A)

- ATP must be approved according to VdS 2471-S1

- Message time (monitoring of the ATS function)
  - Faults of the ATP must be recognized within 180 seconds (through cyclic exchange of Data telegrams between RCT and SPT).
  - Arming prevention in case of trouble or failure of the transmission path.
  - Intervention in case of ATP failure may be delayed by 30 minutes with the consent of the insurer.

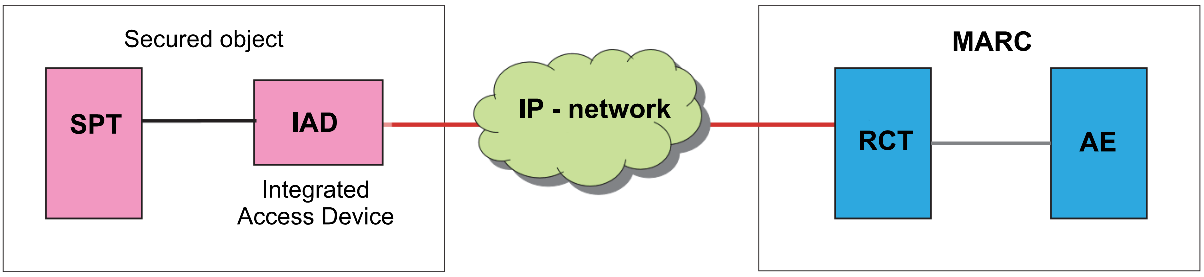
- Routine call
  - SPT sends a test message ≤25 h, RCT acknowledges and logs (Monitoring the application layer (Application Layer))

- Availability in any 7-day period - At least 97%

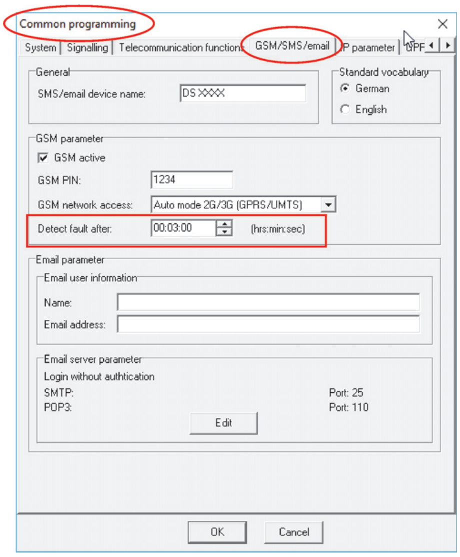
- Transmission time - Max. 60 sec .; arithmetic mean 20 sec.

24.2.1.2 Programming SP4 (simple single path alarm transmission)

- VdS compliant
  - 1 Alarm Transmission path (ATP), Ethernet or mobile network.
  - Primary Transmission path: dedicated line connection (e.g. Ethernet) encrypted.



- Tab Common programming
  - Detect fault line to 180 sec = 3 min. Depending on ATP GSM mobile network or Ethernet (IP Parameter).
  - Set “Delayed arming prevention of redundant permanent IP connections” to **inactive**.


Common programming

System | Signalling | Telecommunication functions | GSM/SMS/email | IP parameter | GPF

General

SMS/email device name: DS XXXX

Standard vocabulary: ● German ○ English

GSM parameter

☑ GSM active

GSM PIN: 1234

GSM network access: Auto mode 2G/3G (GPRS/UMTS)

Detect fault after: 00:03:00 (hrs:min:sec)

Email parameter

Email user information

Name:

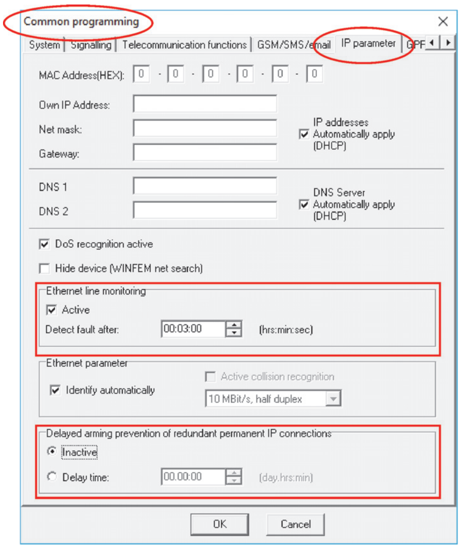
Email address:

Email server parameter

Login without authtication

SMTP: Port: 25

POP3: Port: 110


Common programming

System | Signalling | Telecommunication functions | GSM/SMS/email | IP parameter | GPF

MAC Address(HEX): 0 - 0 - 0 - 0 - 0 - 0

Own IP Address:

Net mask:

Gateway:

☑ IP addresses Automatically apply (DHCP)

DNS 1

DNS 2

☑ DNS Server Automatically apply (DHCP)

☑ DoS recognition active

□ Hide device (WINFEM net search)

Ethernet line monitoring

☑ Active

Detect fault after: 00:03:00 (hrs:min:sec)

Ethernet parameter

☑ Identify automatically

□ Active collision recognition

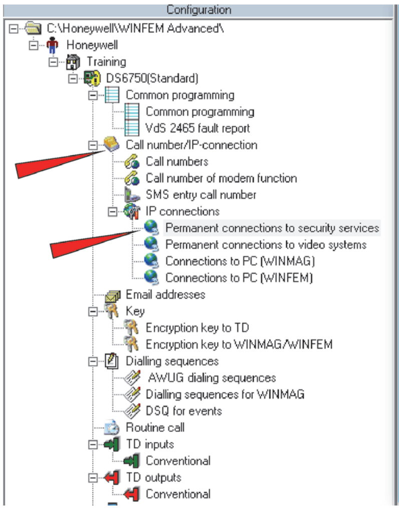
10 MBit/s, half duplex

Delayed arming prevention of redundant permanent IP connections

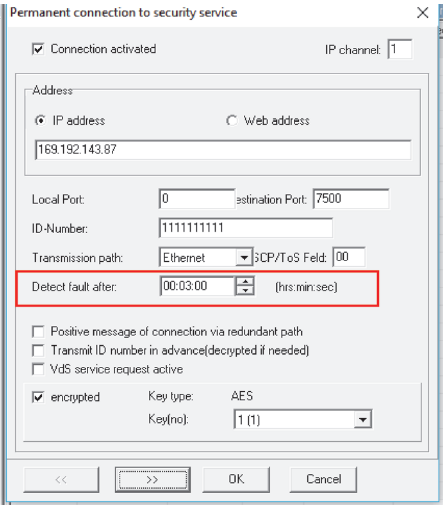
● Inactive

○ Delay time: 00.00:00 (day.hrs:min)

- Programming Call number/ IP-connection
  - First permanent connection encrypted ATP 1 to the RCT (Receiving Centre Tranceiver) .
  - Detect fault line each on 180 sec = 3 min. Depending on ATP Ethernet or GPRS/UMTS.


Configuration

- C:\Honeywell\WINFEM Advanced\
  - Honeywell
    - Training
      - DS6750(Standard)
        - Common programming
          - Common programming
          - VdS 2465 fault report
        - Call number/IP-connection
          - Call numbers
          - Call number of modem function
          - SMS entry call number
          - IP connections
            - Permanent connections to security services
            - Permanent connections to video systems
            - Connections to PC (WINMAG)
            - Connections to PC (WINFEM)
        - Email addresses
        - Key
          - Encryption key to TD
          - Encryption key to WINMAG/WINFEM
        - Dialling sequences
          - AWUG dialing sequences
          - Dialling sequences for WINMAG
          - DSQ for events
        - Routine call
        - TD inputs
          - Conventional
        - TD outputs
          - Conventional


Permanent connection to security service

☑ Connection activated IP channel: 1

Address

● IP address ○ Web address

169.192.143.87

Local Port: 0 estination Port: 7500

ID-Number: 1111111111

Transmission path: Ethernet SCP/ToS Feld: 00

Detect fault after: 00:03:00 (hrs:min:sec)

□ Positive message of connection via redundant path

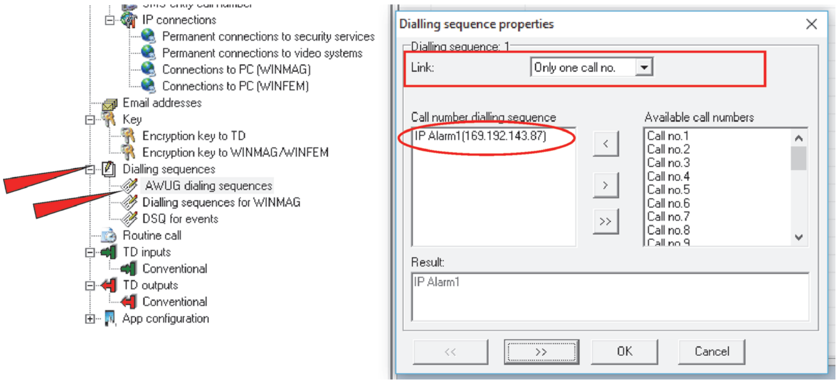
□ Transmit ID number in advance(decrypted if needed)

□ VdS service request active

☑ encrypted Key type: AES

Key(no): 1 (1)

- Programming Dialing sequences
  - DSQ 1 for alarm transmission and 24 hours line monitoring.



SMS-entry call number
IP connections
- Permanent connections to security services
- Permanent connections to video systems
- Connections to PC (WINMAG)
- Connections to PC (WINFEM)

Email addresses
Key
- Encryption key to TD
- Encryption key to WINMAG/WINFEM

Dialling sequences
- AWUG dialing sequences
- Dialling sequences for WINMAG
- DSQ for events

Routine call
TD inputs
- Conventional

TD outputs
- Conventional

App configuration

Dialling sequence properties

Dialling sequence: 1

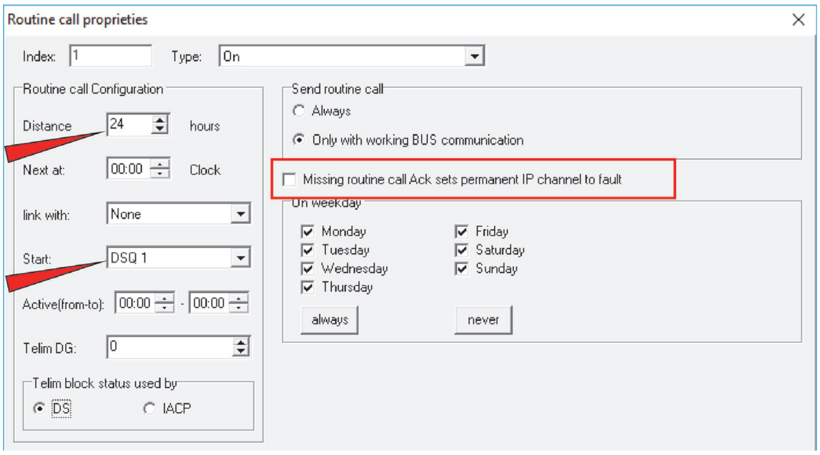
Link: Only one call no.

Call number dialling sequence: IP Alarm1(169.192.143.87)

Available call numbers: Call no.1, Call no.2, Call no.3, Call no.4, Call no.5, Call no.6, Call no.7, Call no.8, Call no.9

Result: IP Alarm1

- Programming Routine call
  - Routine call 1 Abstand 24 Std.
  - **Not active**: Missing routine call Ack sets permanent IP channel to fault.



Routine call proprieties

Index: 1   Type: On

Routine call Configuration

Distance: 24 hours

Next at: 00:00 Clock

link with: None

Start: DSQ 1

Active(from-to): 00:00 - 00:00

Telim DG: 0

Telim block status used by: ● DS ○ IACP

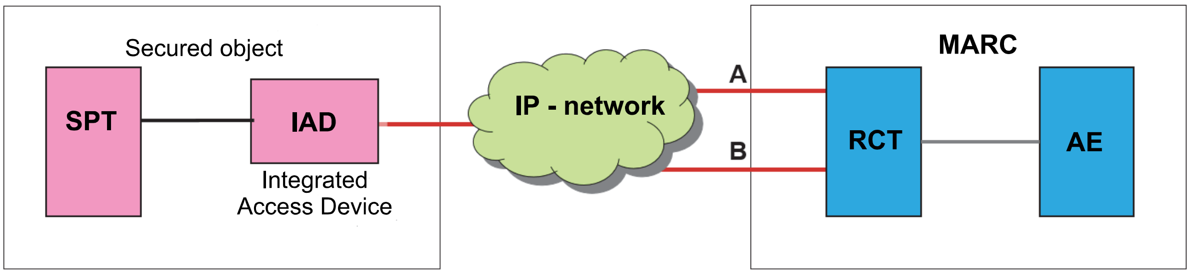
Send routine call: ○ Always ● Only with working BUS communication

☐ Missing routine call Ack sets permanent IP channel to fault

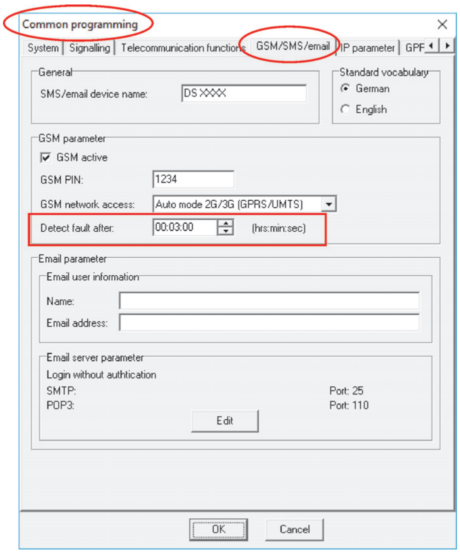
On weekday: ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

24.2.1.3 Programming for SP4 (Single path alarm transmission)

- VdS compliant, BHE reference. To achieve the required availability of 97% or better.
  - 1 Alarm Transmission path (ATP), Ethernet or mobile network.
  - RCT has 2 separate access points to the IP network.
  - Primary Transmission path: first permanent connection (e.g. Ethernet) to access point A of the RCT.
  - Alternative Primary Transmission path: second permanent connection (e.g. Ethernet) to access point B of the RCT. To achieve the required availability of 97% or better.



- Tab Common programming
  - Detect fault line to 180 sec. = 3 min. Depending on ATP Ethernet or GPRS/UMTS.
  - Set “Delayed arming prevention of redundant permanent IP connections” to **inactive**.



Common programming

System | Signalling | Telecommunication functions | GSM/SMS/email | IP parameter | GPF

General

SMS/email device name: DS XXXX

Standard vocabulary

● German

○ English

GSM parameter

☑ GSM active

GSM PIN: 1234

GSM network access: Auto mode 2G/3G (GPRS/UMTS)

Detect fault after: 00:03:00 (hrs:min:sec)

Email parameter

Email user information

Name:

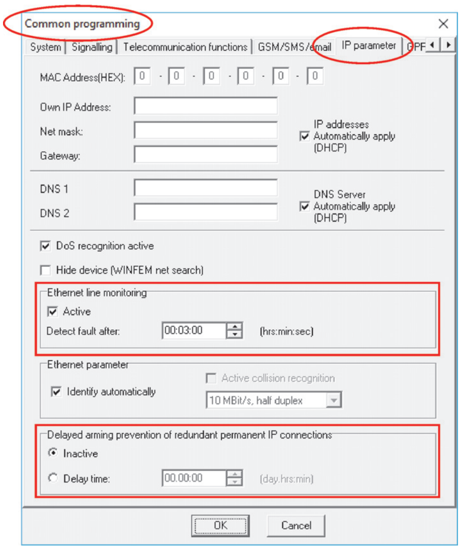
Email address:

Email server parameter

Login without authtication

SMTP: Port: 25

POP3: Port: 110



Common programming

System | Signalling | Telecommunication functions | GSM/SMS/email | IP parameter | GPF

MAC Address(HEX): 0 - 0 - 0 - 0 - 0 - 0

Own IP Address:

Net mask:

Gateway:

IP addresses ☑ Automatically apply (DHCP)

DNS 1

DNS 2

DNS Server ☑ Automatically apply (DHCP)

☑ DoS recognition active

□ Hide device (WINFEM net search)

Ethernet line monitoring

☑ Active

Detect fault after: 00:03:00 (hrs:min:sec)

Ethernet parameter

☑ Identify automatically

□ Active collision recognition

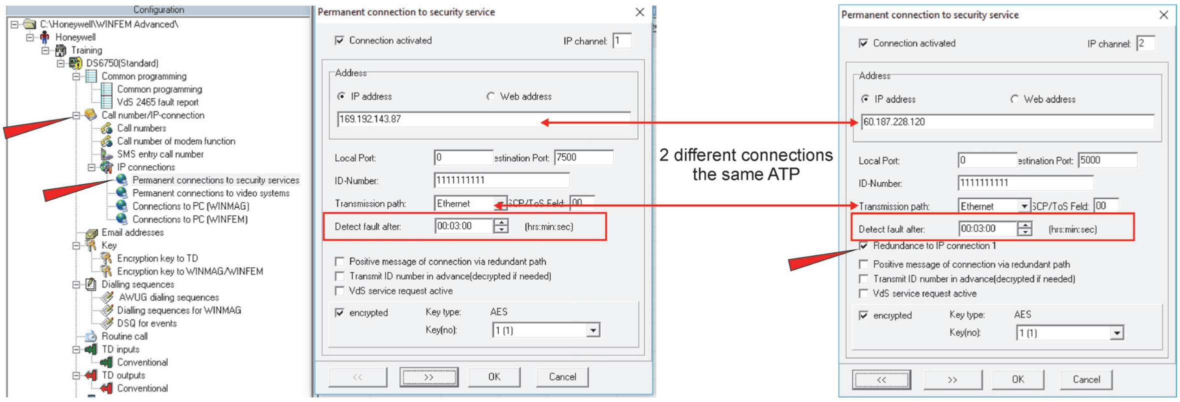
10 MBit/s, half duplex

Delayed arming prevention of redundant permanent IP connections

● Inactive

○ Delay time: 00.00:00 (day.hrs:min)

- Programming Call numbers / IP-connections
  - First permanent connection encrypted ATP 1 to access point A of the RCT
  - Second permanent connection encrypted ATP 1 to access point B of the RCT redundant to the first.
  - Detect fault line each on 180 sec. = 3 min. Depending on ATP Ethernet or GPRS/UMTS.



2 different connections the same ATP

Permanent connection to security service

☑ Connection activated IP channel: 1

Address

● IP address ○ Web address

169.192.143.87

Local Port: 0 estination Port: 7500

ID-Number: 1111111111

Transmission path: Ethernet SCP/ToS Feld: 00

Detect fault after: 00:03:00 (hrs:min:sec)

□ Positive message of connection via redundant path

□ Transmit ID number in advance(decrypted if needed)

□ VdS service request active

☑ encrypted Key type: AES

Key(no): 1 (1)

Permanent connection to security service

☑ Connection activated IP channel: 2

Address

● IP address ○ Web address

60.187.228.120

Local Port: 0 estination Port: 5000

ID-Number: 1111111111

Transmission path: Ethernet SCP/ToS Feld: 00

Detect fault after: 00:03:00 (hrs:min:sec)

☑ Redundance to IP connection 1

□ Positive message of connection via redundant path

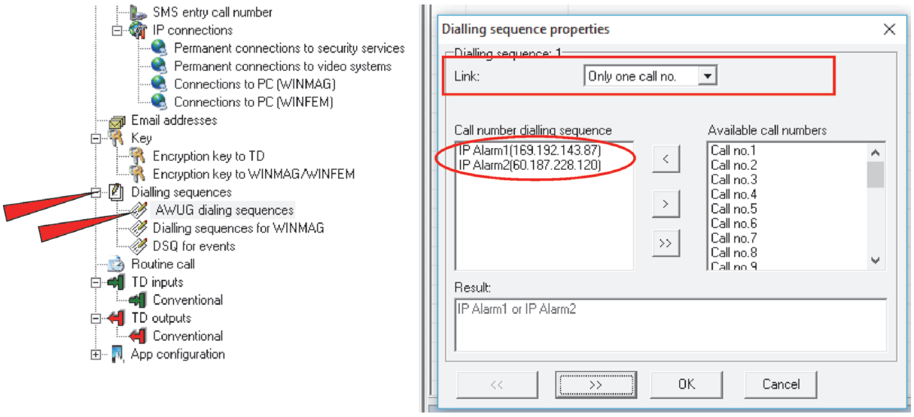
□ Transmit ID number in advance(decrypted if needed)

□ VdS service request active

☑ encrypted Key type: AES

Key(no): 1 (1)

- Programming Dialing sequences
  - DSQ 1 for alarm transmission and 24 hours line monitoring.



Dialling sequence properties

Dialling sequence: 1

Link: Only one call no.

Call number dialling sequence

IP Alarm1(169.192.143.87)

IP Alarm2(60.187.228.120)

Available call numbers

Call no.1

Call no.2

Call no.3

Call no.4

Call no.5

Call no.6

Call no.7

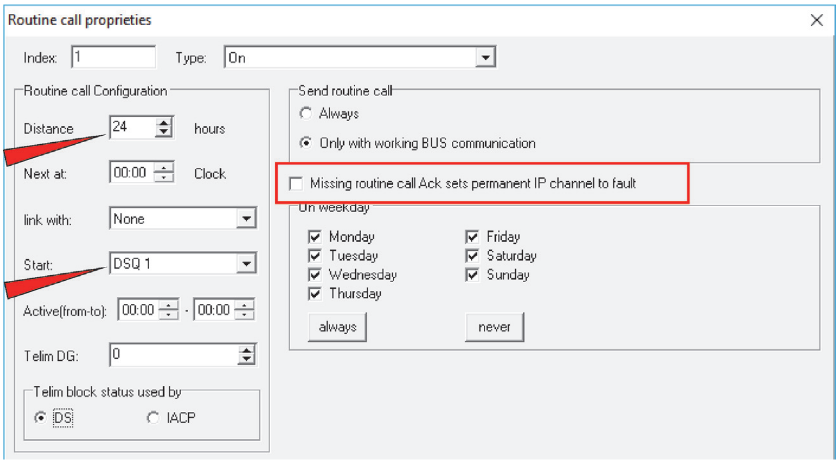
Call no.8

Call no.9

Result:

IP Alarm1 or IP Alarm2

- Programming Routine call
  - Routine call 1 Distance 24 hours.
  - **Not active:** Missing routine call Ack sets permanent IP channel to fault.



Routine call proprieties

Index: 1 Type: On

Routine call Configuration

Distance: 24 hours

Next at: 00:00 Clock

link with: None

Start: DSQ 1

Active(from-to): 00:00 - 00:00

Telim DG: 0

Telim block status used by

● DS ○ IACP

Send routine call

○ Always

● Only with working BUS communication

☐ Missing routine call Ack sets permanent IP channel to fault

On weekday

☑ Monday ☑ Friday
☑ Tuesday ☑ Saturday
☑ Wednesday ☑ Sunday
☑ Thursday

24.2.2 Requirements IP Dual path ATS DP4 (for VdS-Class A, B, C)

- At least one ATP must be approved according to VdS 2471-S1.
- Second ATP must fulfill at least requirements according to DIN EN 50136.
- Message time (monitoring of the ATS function).
  - Faults of the first ATP must be recognized within 90 seconds.
  - Faults of the second ATP must be recognized within 5 hours with undisturbed first ATP and be recognized within 90 seconds if the first ATP has a fault.
  - Switching from the disturbed first ATP to the second ATP within 90 sec.
- in case of failure of one ATP -> Arming prevention after 36 hours.
- in case of failure of both ATP -> Arming prevention and intervention.
- Routine call

  SPT sends a test message = 25 h. via Primary Transmission path and Alternative Primary Transmission path, RCT acknowledges and logs (Monitoring the application layer (Application Layer)) .
- Separate network access points

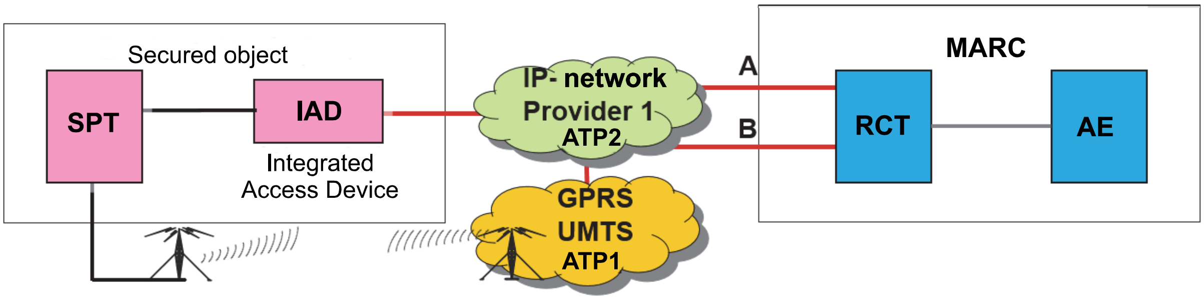
  A single act of tamper on the transmission network must not result in the simultaneous failure of both ATPs.
- Availability in any 7-day period

  At least 99.8 %
- Transmission time

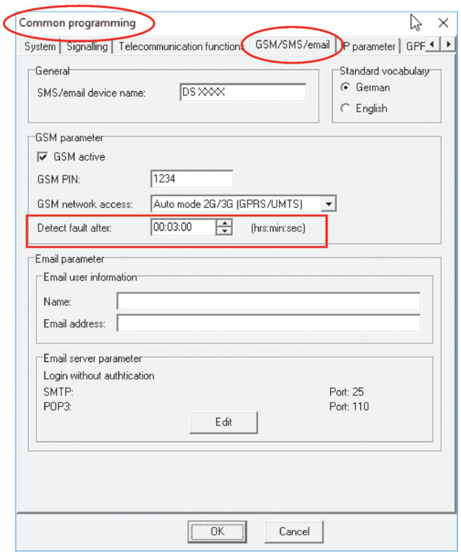
  Max. 30 Sec.; arithmetic mean 20 sec..

24.2.2.1 Programming for DP4 (simple Dual path alarm transmission)

- VdS compliant
  - 2 Alarm Transmission paths (ATP), Ethernet and mobile network.
  - ATS has 2 separate access points to the IP network.
  - Primary Transmission path: first dedicated line connection (Ethernet) to access point A of the RCT.
  - Secondary Transmission path: second dedicated line connection (GPRS/UMTS) and call no. 1 to access point B of the RCT.



- Tab Common programming
  - (GSM) Detect fault after to 180 sec.= 3 min.
  - **Not active:** Ethernet line monitoring because monitoring is programmed in the individual connections.
  - Set “Delayed arming prevention of redundant permanent IP connections” to 36 hours.


Common programming
System | Signalling | Telecommunication functions | GSM/SMS/email | IP parameter | GPF
OK
Cancel
Edit

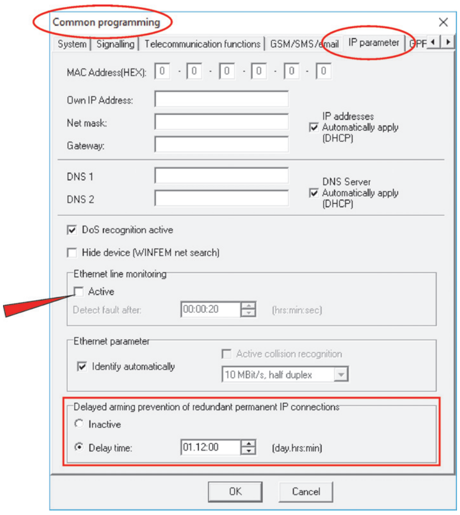
General
SMS/email device name: DS XXXX

Standard vocabulary
● German
○ English

GSM parameter
☑ GSM active
GSM PIN: 1234
GSM network access: Auto mode 2G/3G (GPRS/UMTS)
Detect fault after: 00:03:00 (hrs:min:sec)

Email parameter
Email user information
Name:
Email address:

Email server parameter
Login without authtication
SMTP: Port: 25
POP3: Port: 110


Common programming
System | Signalling | Telecommunication functions | GSM/SMS/email | IP parameter | GPF
OK
Cancel

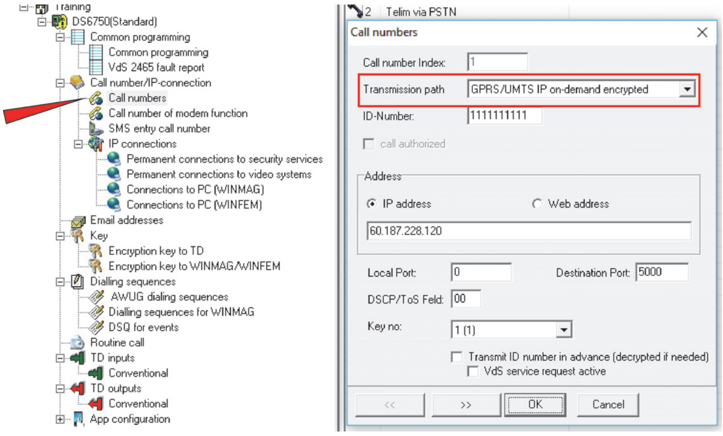
MAC Address(HEX): 0 - 0 - 0 - 0 - 0 - 0
Own IP Address:
Net mask:
Gateway:
☑ IP addresses Automatically apply (DHCP)
DNS 1
DNS 2
☑ DNS Server Automatically apply (DHCP)
☑ DoS recognition active
☐ Hide device (WINFEM net search)

Ethernet line monitoring
☐ Active
Detect fault after: 00:00:20 (hrs:min:sec)

Ethernet parameter
☑ Identify automatically
☐ Active collision recognition
10 MBit/s, half duplex

Delayed arming prevention of redundant permanent IP connections
○ Inactive
● Delay time: 01.12:00 (day.hrs:min)

- Programming Call number / IP-connection
  - Call number 1 GPRS/UMTS IP on-demand encrypted with the parameters of the second permanent connection. ATP 2 (GPRS/UMTS) to access point B of the RCT.

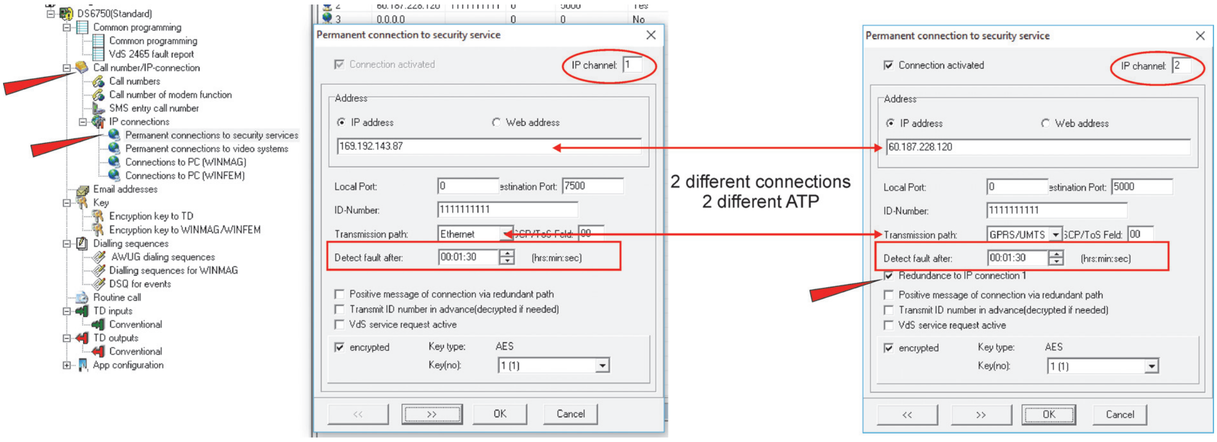


Call number Index: 1
Transmission path GPRS/UMTS IP on-demand encrypted
ID-Number: 1111111111
☐ call authorized

Address
● IP address ○ Web address
60.187.228.120

Local Port: 0 Destination Port: 5000
DSCP/ToS Feld: 00
Key no: 1 (1)
☐ Transmit ID number in advance (decrypted if needed)
☐ VdS service request active

- Programming Call number / IP-connection
  - First permanent connection encrypted ATP 1 (Ethernet) to access point A of the RCT.
  - Second permanent connection encrypted ATP 2 (GPRS/UMTS) to access point B of the RCT, redundant to the first.
  - Detect fault line each on 90 sec..



Permanent connection to security service (IP channel 1)

☑ Connection activated IP channel: 1

Address
● IP address ○ Web address
169.192.143.87

Local Port: 0 Destination Port: 7500
ID-Number: 1111111111
Transmission path: Ethernet DSCP/ToS Feld: 00
Detect fault after: 00:01:30 (hrs:min:sec)
☐ Positive message of connection via redundant path
☐ Transmit ID number in advance(decrypted if needed)
☐ VdS service request active
☑ encrypted Key type: AES
Key(no): 1 (1)

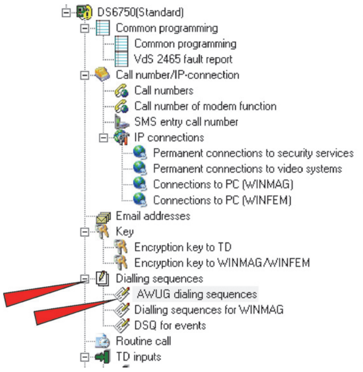
Permanent connection to security service (IP channel 2)

☑ Connection activated IP channel: 2

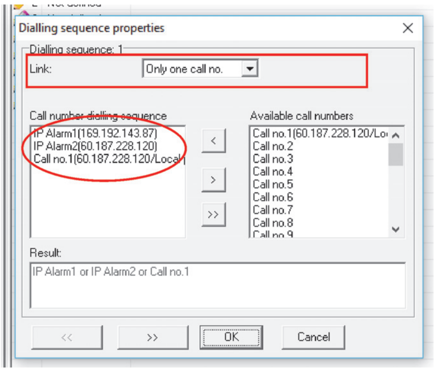
Address
● IP address ○ Web address
60.187.228.120

Local Port: 0 Destination Port: 5000
ID-Number: 1111111111
Transmission path: GPRS/UMTS DSCP/ToS Feld: 00
Detect fault after: 00:01:30 (hrs:min:sec)
☑ Redundance to IP connection 1
☐ Positive message of connection via redundant path
☐ Transmit ID number in advance(decrypted if needed)
☐ VdS service request active
☑ encrypted Key type: AES
Key(no): 1 (1)

- Programming Dialing sequences
  - DSQ 1 for alarm transmission and 24 hours line monitoring.



- DS6750(Standard)
  - Common programming
    - Common programming
    - VdS 2465 fault report
  - Call number/IP-connection
    - Call numbers
    - Call number of modem function
    - SMS entry call number
    - IP connections
      - Permanent connections to security services
      - Permanent connections to video systems
      - Connections to PC (WINMAG)
      - Connections to PC (WINFEM)
  - Email addresses
  - Key
    - Encryption key to TD
    - Encryption key to WINMAG/WINFEM
  - Dialling sequences
    - AWUG dialing sequences
    - Dialling sequences for WINMAG
    - DSQ for events
  - Routine call
  - TD inputs



Dialling sequence properties

Dialling sequence: 1

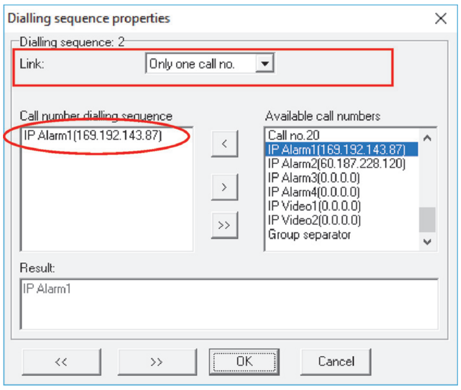
Link: Only one call no.

Call number dialling sequence:
IP Alarm1(169.192.143.87)
IP Alarm2(60.187.228.120)
Call no.1(60.187.228.120/Local)

Available call numbers:
Call no.1(60.187.228.120/Lo
Call no.2
Call no.3
Call no.4
Call no.5
Call no.6
Call no.7
Call no.8
Call no.9

Result: IP Alarm1 or IP Alarm2 or Call no.1

  - DSQ 2 for <25 h Monitoring ATP1, IP Alarm1.
  - DSQ 3 for <5 h Monitoring ATP2, IP Alarm2 or call no. 1.



Dialling sequence properties

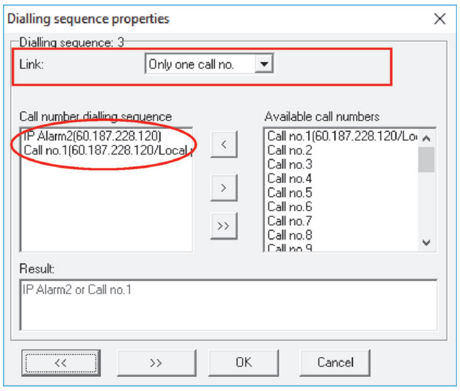
Dialling sequence: 2

Link: Only one call no.

Call number dialling sequence:
IP Alarm1(169.192.143.87)

Available call numbers:
Call no.20
IP Alarm1(169.192.143.87)
IP Alarm2(60.187.228.120)
IP Alarm3(0.0.0.0)
IP Alarm4(0.0.0.0)
IP Video1(0.0.0.0)
IP Video2(0.0.0.0)
Group separator

Result: IP Alarm1



Dialling sequence properties

Dialling sequence: 3

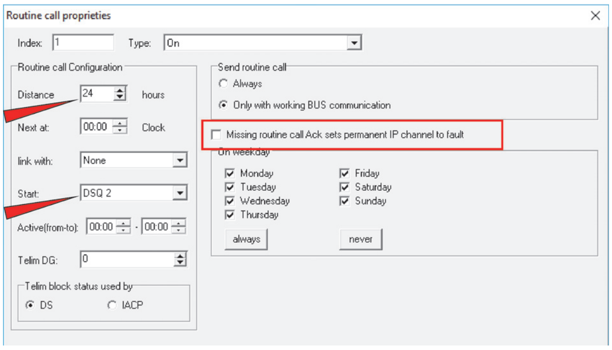
Link: Only one call no.

Call number dialling sequence:
IP Alarm2(60.187.228.120)
Call no.1(60.187.228.120/Local)

Available call numbers:
Call no.1(60.187.228.120/Lo
Call no.2
Call no.3
Call no.4
Call no.5
Call no.6
Call no.7
Call no.8
Call no.9

Result: IP Alarm2 or Call no.1

- Programming Routine call
  - Routine call 1, Distance 24 hours, start DSQ 2.
  - Routine call 2, Distance 4 hours, start DSQ 3.
  - **Set active:** Missing routine call Ack sets permanent IP channel to fault.



Routine call proprieties

Index: 1 Type: On

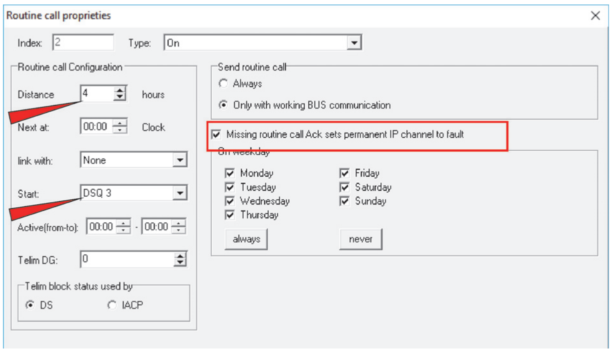
Routine call Configuration
Distance 24 hours
Next at: 00:00 Clock
link with: None
Start: DSQ 2
Active(from-to): 00:00 - 00:00
Telim DG: 0

Telim block status used by: ● DS ○ IACP

Send routine call: ○ Always ● Only with working BUS communication

□ Missing routine call Ack sets permanent IP channel to fault

On weekday: ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday



Routine call proprieties

Index: 2 Type: On

Routine call Configuration
Distance 4 hours
Next at: 00:00 Clock
link with: None
Start: DSQ 3
Active(from-to): 00:00 - 00:00
Telim DG: 0

Telim block status used by: ● DS ○ IACP

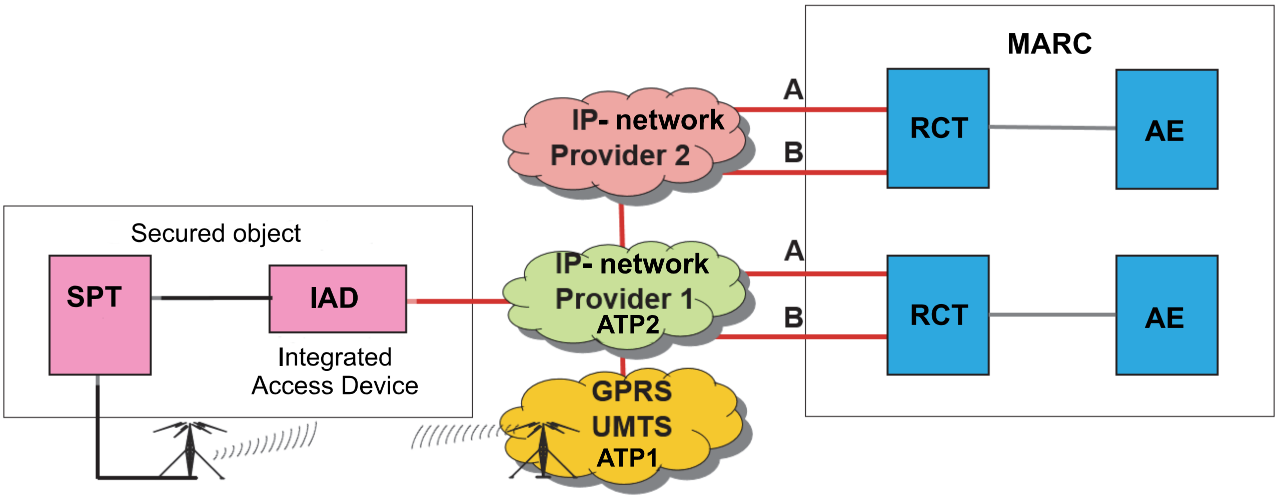
Send routine call: ○ Always ● Only with working BUS communication

☑ Missing routine call Ack sets permanent IP channel to fault

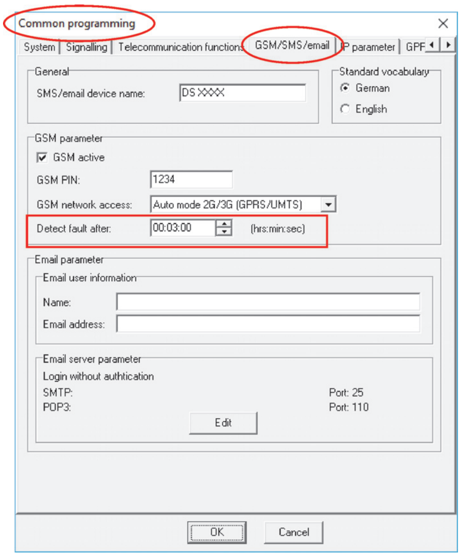
On weekday: ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

24.2.2.2 Programming for DP4 (Dual Path 4) Dual path alarm transmission

- VdS compliant, BHE reference. To achieve the required availability of 99.8%:
  - 2 Alarm Transmission paths (ATP), Ethernet and mobile network.
  - the MARC has 2 separate access points and 2 RCT to the IP network.
  - Primary Transmission path: first dedicated line connection (Ethernet) to access point A (RCT1) of the MARC.
  - Alternative Primary Transmission path: second dedicated line connection (Ethernet) to access point A (RCT2) of the MARC.
  - Secondary Transmission path: third dedicated line connection (GPRS/UMTS) and Call no. 1 to access point B (RCT1) of the MARC.
  - Alternative Secondary Transmission path: forth dedicated line connection (GPRS/UMTS) and Call no. 2 to access point B (RCT2) of the MARC.



- Tab Common programming
  - (GSM) Detect fault after to 180 sec.= 3 min..
  - **Not active:** Ethernet line monitoring because monitoring is programmed in the individual connections.
  - Set "Delayed arming prevention of redundant permanent IP connections" to 36 hours.



General

SMS/email device name: DS XXXX

Standard vocabulary

● German

○ English

GSM parameter

☑ GSM active

GSM PIN: 1234

GSM network access: Auto mode 2G/3G (GPRS/UMTS)

Detect fault after: 00:03:00 (hrs:min:sec)

Email parameter

Email user information

Name:

Email address:

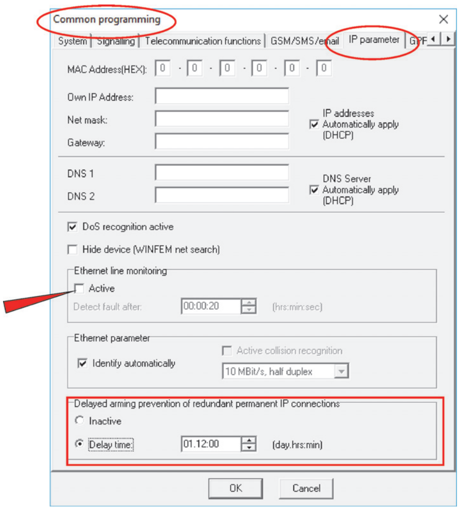
Email server parameter

Login without authtication

SMTP: Port: 25

POP3: Port: 110

Edit



MAC Address(HEX): 0 - 0 - 0 - 0 - 0 - 0

Own IP Address:

Net mask:

Gateway:

IP addresses

☑ Automatically apply (DHCP)

DNS 1

DNS 2

DNS Server

☑ Automatically apply (DHCP)

☑ DoS recognition active

□ Hide device (WINFEM net search)

Ethernet line monitoring

□ Active

Detect fault after: 00:00:20 (hrs:min:sec)

Ethernet parameter

☑ Identify automatically

□ Active collision recognition

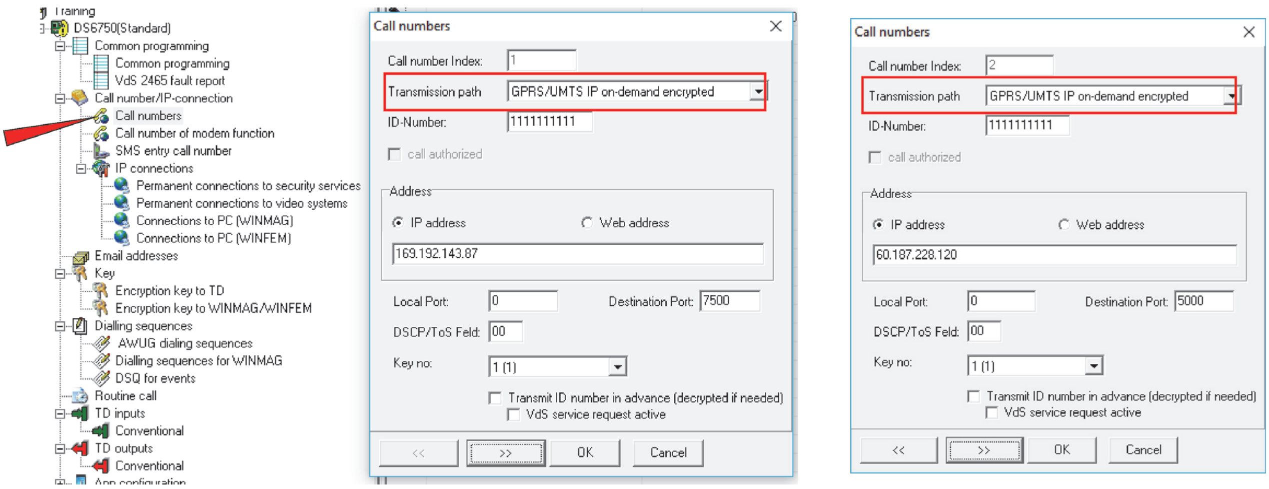
10 MBit/s, half duplex

Delayed arming prevention of redundant permanent IP connections

○ Inactive

● Delay time: 01.12:00 (day.hrs:min)

- Programming Call number / IP-connection
  - Call no. 1 GPRS/UMTS IP on-demand encrypted with the parameters of the third permanent connection. ATP 2 (GPRS/UMTS) to access point B (RCT1) of the MARC.
  - Call no. 2 GPRS/UMTS IP on-demand encrypted with the parameters of the forth permanent connection. ATP 2 (GPRS/UMTS) to access point B (RCT2) of the MARC.



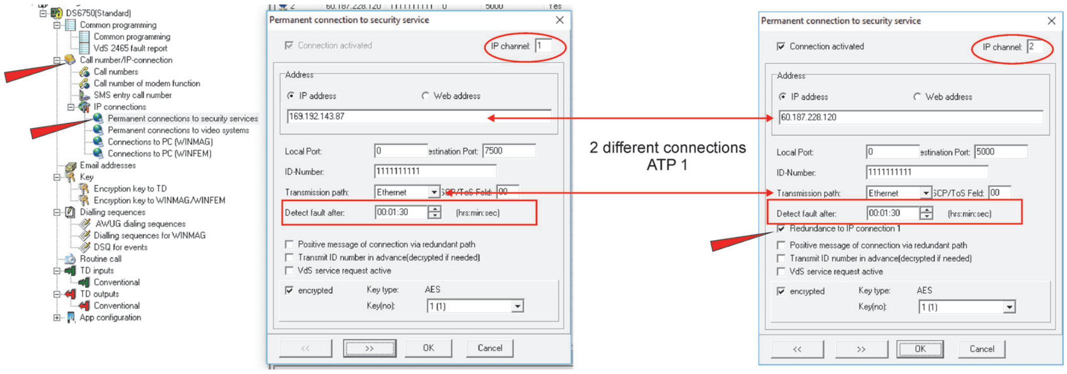
Call numbers

Call number Index: 1
Transmission path: GPRS/UMTS IP on-demand encrypted
ID-Number: 1111111111
□ call authorized
Address
● IP address ○ Web address
169.192.143.87
Local Port: 0 Destination Port: 7500
DSCP/ToS Feld: 00
Key no: 1 (1)
□ Transmit ID number in advance (decrypted if needed)
□ VdS service request active

Call numbers

Call number Index: 2
Transmission path: GPRS/UMTS IP on-demand encrypted
ID-Number: 1111111111
□ call authorized
Address
● IP address ○ Web address
60.187.228.120
Local Port: 0 Destination Port: 5000
DSCP/ToS Feld: 00
Key no: 1 (1)
□ Transmit ID number in advance (decrypted if needed)
□ VdS service request active

- Programming Call number / IP-connection
  - First permanent connection encrypted ATP 1 (Ethernet) to Transmission path A (RCT1) of the MARC.
  - Second permanent connection encrypted ATP 1 (Ethernet) to Transmission path A (RCT2) of the MARC, redundant to the first permanent connection.
  - Detect fault line each on 90 sec..



2 different connections ATP 1

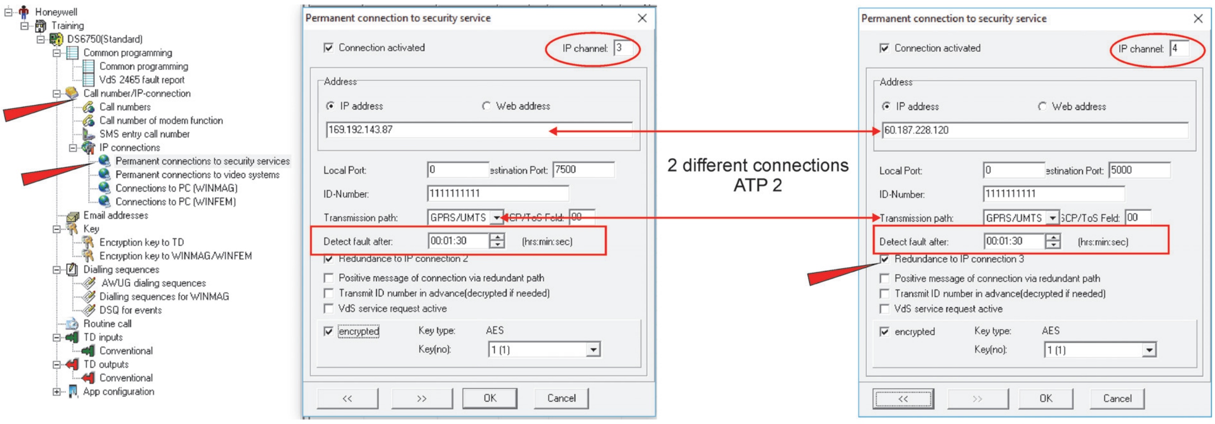
Permanent connection to security service

☑ Connection activated IP channel: 1
Address
● IP address ○ Web address
169.192.143.87
Local Port: 0 Destination Port: 7500
ID-Number: 1111111111
Transmission path: Ethernet DSCP/ToS Feld: 00
Detect fault after: 00:01:30 (hrs:min:sec)
□ Positive message of connection via redundant path
□ Transmit ID number in advance(decrypted if needed)
□ VdS service request active
☑ encrypted Key type: AES
Key(no): 1 (1)

Permanent connection to security service

☑ Connection activated IP channel: 2
Address
● IP address ○ Web address
60.187.228.120
Local Port: 0 Destination Port: 5000
ID-Number: 1111111111
Transmission path: Ethernet DSCP/ToS Feld: 00
Detect fault after: 00:01:30 (hrs:min:sec)
☑ Redundance to IP connection 1
□ Positive message of connection via redundant path
□ Transmit ID number in advance(decrypted if needed)
□ VdS service request active
☑ encrypted Key type: AES
Key(no): 1 (1)

- Programming Call number / IP-connection
  - Third permanent connection encrypted ATP 2 (GPRS/UMTS) to Transmission path B (RCT1) of the MARC, redundant to the second permanent connection.
  - Forth permanent connection encrypted ATP 2 (GPRS/UMTS) to Transmission path B (RCT2) of The MARC, redundant to the third permanent connection.
  - Detect fault line each on 90 sec..



2 different connections ATP 2

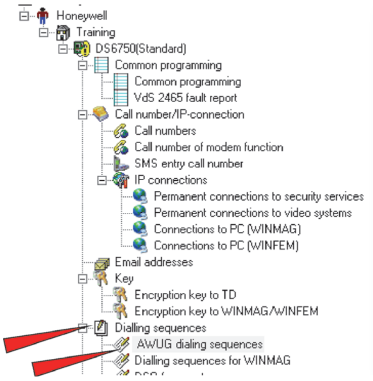
Permanent connection to security service

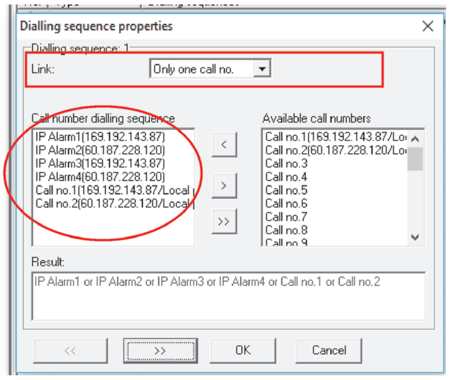
☑ Connection activated IP channel: 3
Address
● IP address ○ Web address
169.192.143.87
Local Port: 0 Destination Port: 7500
ID-Number: 1111111111
Transmission path: GPRS/UMTS DSCP/ToS Feld: 00
Detect fault after: 00:01:30 (hrs:min:sec)
☑ Redundance to IP connection 2
□ Positive message of connection via redundant path
□ Transmit ID number in advance(decrypted if needed)
□ VdS service request active
☑ encrypted Key type: AES
Key(no): 1 (1)

Permanent connection to security service

☑ Connection activated IP channel: 4
Address
● IP address ○ Web address
60.187.228.120
Local Port: 0 Destination Port: 5000
ID-Number: 1111111111
Transmission path: GPRS/UMTS DSCP/ToS Feld: 00
Detect fault after: 00:01:30 (hrs:min:sec)
☑ Redundance to IP connection 3
□ Positive message of connection via redundant path
□ Transmit ID number in advance(decrypted if needed)
□ VdS service request active
☑ encrypted Key type: AES
Key(no): 1 (1)

- Tab Dialling sequences
  - DSQ 1 for Alarm transmission with all programmed Call numbers.
  - DSQ 2 for <25 h Monitoring ATP1, IP Alarm1 or IP Alarm2.


Honeywell
Training
DS6750(Standard)
Common programming
Common programming
VdS 2465 fault report
Call number/IP-connection
Call numbers
Call number of modem function
SMS entry call number
IP connections
Permanent connections to security services
Permanent connections to video systems
Connections to PC (WINMAG)
Connections to PC (WINFEM)
Email addresses
Key
Encryption key to TD
Encryption key to WINMAG/WINFEM
Dialling sequences
AWUG dialing sequences
Dialling sequences for WINMAG


Dialling sequence properties

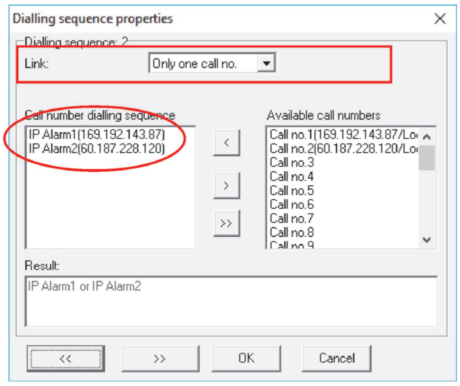
Dialling sequence: 1

Link: Only one call no.

Call number dialling sequence:
IP Alarm1(169.192.143.87)
IP Alarm2(60.187.228.120)
IP Alarm3(169.192.143.87)
IP Alarm4(60.187.228.120)
Call no.1(169.192.143.87/Local
Call no.2(60.187.228.120/Local

Available call numbers:
Call no.1(169.192.143.87/Lo
Call no.2(60.187.228.120/Lo
Call no.3
Call no.4
Call no.5
Call no.6
Call no.7
Call no.8
Call no.9

Result: IP Alarm1 or IP Alarm2 or IP Alarm3 or IP Alarm4 or Call no.1 or Call no.2


Dialling sequence properties

Dialling sequence: 2

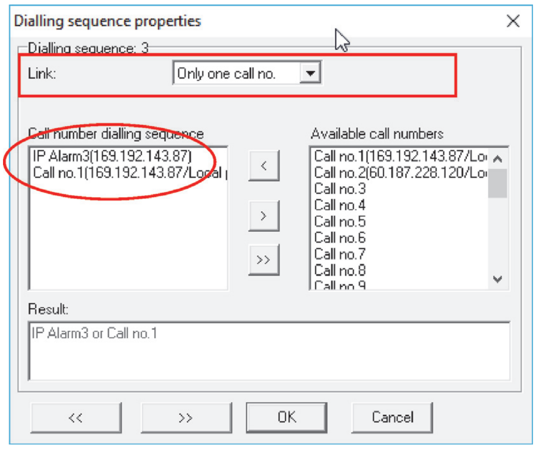
Link: Only one call no.

Call number dialling sequence:
IP Alarm1(169.192.143.87)
IP Alarm2(60.187.228.120)

Available call numbers:
Call no.1(169.192.143.87/Lo
Call no.2(60.187.228.120/Lo
Call no.3
Call no.4
Call no.5
Call no.6
Call no.7
Call no.8
Call no.9

Result: IP Alarm1 or IP Alarm2

- Tab Dialling sequences
  - DSQ 3 for <5h Monitoring AÜW2 Transmission path A, IP Alarm3 or Call no.1.
  - DSQ 4 for <5h Monitoring AÜW2 Transmission path B, IP Alarm4 or Call no. 2.


Dialling sequence properties

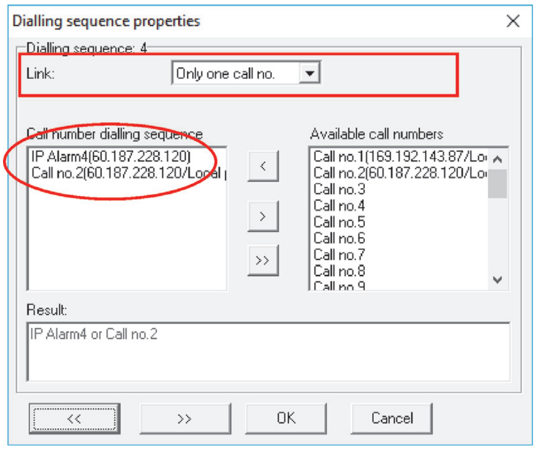
Dialling sequence: 3

Link: Only one call no.

Call number dialling sequence:
IP Alarm3(169.192.143.87)
Call no.1(169.192.143.87/Local

Available call numbers:
Call no.1(169.192.143.87/Lo
Call no.2(60.187.228.120/Lo
Call no.3
Call no.4
Call no.5
Call no.6
Call no.7
Call no.8
Call no.9

Result: IP Alarm3 or Call no.1


Dialling sequence properties

Dialling sequence: 4

Link: Only one call no.

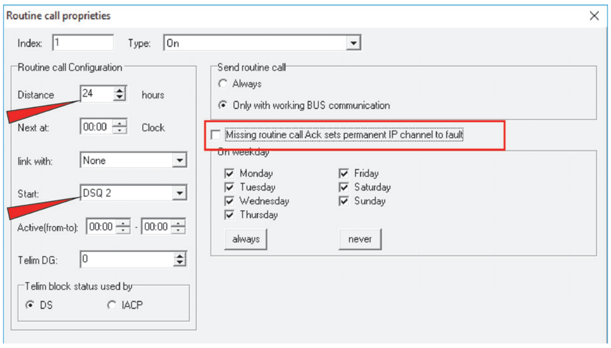
Call number dialling sequence:
IP Alarm4(60.187.228.120)
Call no.2(60.187.228.120/Local

Available call numbers:
Call no.1(169.192.143.87/Lo
Call no.2(60.187.228.120/Lo
Call no.3
Call no.4
Call no.5
Call no.6
Call no.7
Call no.8
Call no.9

Result: IP Alarm4 or Call no.2

- Tab Routine call
  - Routine call 1 Abstand 24 Std. Starte AWF 2,
  - **Not active:** Missing routine call Ack sets permanent IP channel to fault.
  - Routine call 2 not active.

Routine call 1 -> permanent IP Connection 1
Routine call 2 -> permanent IP Connection 2
Routine call 3 -> permanent IP Connection 3
Routine call 4 -> permanent IP Connection 4


Routine call proprieties

Index: 1
Type: On

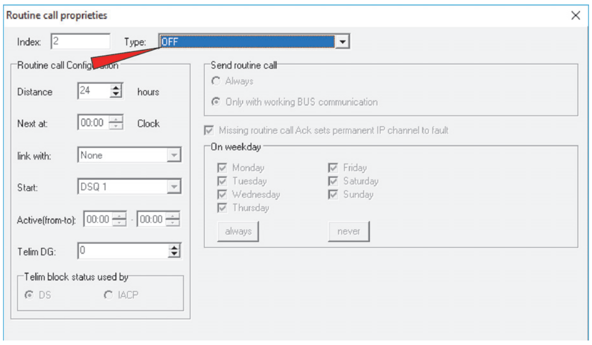
Routine call Configuration
Distance: 24 hours
Next at: 00:00 Clock
link with: None
Start: DSQ 2
Active(from-to): 00:00 - 00:00
Telim DG: 0

Telim block status used by
● DS ○ IACP

Send routine call
○ Always
● Only with working BUS communication

□ Missing routine call Ack sets permanent IP channel to fault

On weekday
☑ Monday ☑ Friday
☑ Tuesday ☑ Saturday
☑ Wednesday ☑ Sunday
☑ Thursday


Routine call proprieties

Index: 2
Type: OFF

Routine call Configuration
Distance: 24 hours
Next at: 00:00 Clock
link with: None
Start: DSQ 1
Active(from-to): 00:00 - 00:00
Telim DG: 0

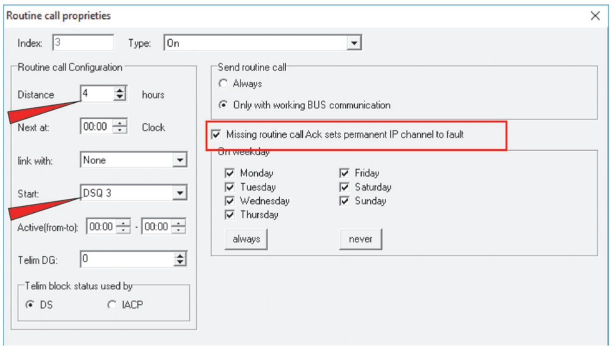
Telim block status used by
● DS ○ IACP

Send routine call
○ Always
● Only with working BUS communication

☑ Missing routine call Ack sets permanent IP channel to fault

On weekday
☑ Monday ☑ Friday
☑ Tuesday ☑ Saturday
☑ Wednesday ☑ Sunday
☑ Thursday

- Tab Routine call
  - Routine call 3, Distance 4 hours. Start DSQ 3, active: Missing routine call Ack sets permanent IP channel to fault.
  - Routine call 4, Distance 4 hours. Start DSQ 4, active: Missing routine call Ack sets permanent IP channel to fault.



Routine call proprieties

Index: 3 Type: On

Routine call Configuration

Distance 4 hours

Next at: 00:00 Clock

link with: None

Start: DSQ 3

Active(from-to): 00:00 - 00:00

Telim DG: 0

Telim block status used by

● DS ○ IACP

Send routine call

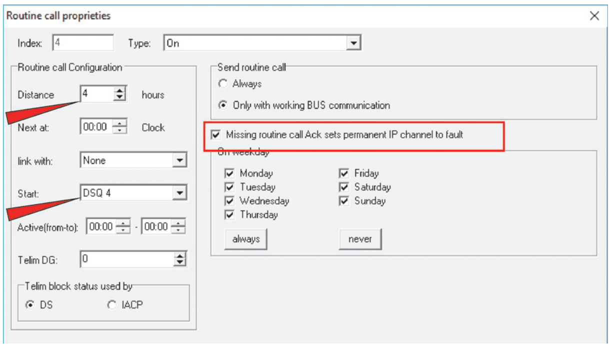
○ Always

● Only with working BUS communication

☑ Missing routine call Ack sets permanent IP channel to fault

On weekday

☑ Monday ☑ Friday
☑ Tuesday ☑ Saturday
☑ Wednesday ☑ Sunday
☑ Thursday



Routine call proprieties

Index: 4 Type: On

Routine call Configuration

Distance 4 hours

Next at: 00:00 Clock

link with: None

Start: DSQ 4

Active(from-to): 00:00 - 00:00

Telim DG: 0

Telim block status used by

● DS ○ IACP

Send routine call

○ Always

● Only with working BUS communication

☑ Missing routine call Ack sets permanent IP channel to fault

On weekday

☑ Monday ☑ Friday
☑ Tuesday ☑ Saturday
☑ Wednesday ☑ Sunday
☑ Thursday

25. Index

26. Notes

Honeywell Commercial Security

Novar GmbH
Johannes-Mauthe-Strasse 14
72458 Albstadt, Germany
www.honeywell.com/security/de

Honeywell

P03178-20-0G0-06
2018-05-07

P03178-20-0G006