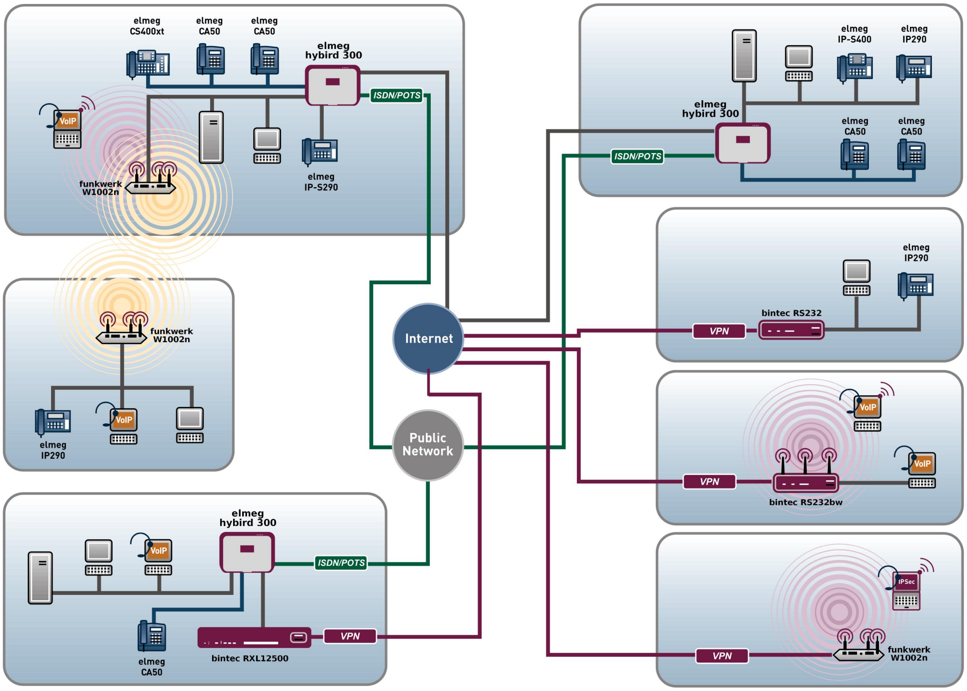

Manual
Release Notes

7.10.1

Legal Notice

Aim and purpose

This document is part of the user manual for the installation and configuration of funkwerk devices. For the latest information and notes on the current software release, please also read our release notes, particularly if you are updating your software to a higher release version. You will find the latest release notes under *www.funkwerk-ec.com* .

Liability

This manual has been put together with the greatest possible care. However, the information contained in this manual is not a guarantee of the properties of your product. Funkwerk Enterprise Communications GmbH is only liable within the terms of its conditions of sale and supply and accepts no liability for technical inaccuracies and/or omissions.

The information in this manual can be changed without notice. You will find additional information and also release notes for funkwerk devices under *www.funkwerk-ec.com* .

Funkwerk devices make WAN connections as a possible function of the system configuration. You must monitor the product in order to avoid unwanted charges. Funkwerk Enterprise Communications GmbH accepts no responsibility for data loss, unwanted connection costs and damage caused by unintended operation of the product.

Trademarks

funkwerk trademarks and the funkwerk logo, bintec trademarks and the bintec logo, artem trademarks and the artem logo, elmeg trademarks and the elmeg logo are registered trademarks of Funkwerk Enterprise Communications GmbH.

Company and product names mentioned are usually trademarks of the companies or manufacturers concerned.

Copyright

You will find information on guidelines and standards in the declarations of conformity under *www.funkwerk-ec.com* .

How to reach Funkwerk Enterprise Communications GmbH

Funkwerk Enterprise Communications GmbH, Südwestpark 94, D-90449 Nuremberg, Germany,
Phone: +49 911 9673 0, Fax: +49 911 688 07 25
Funkwerk Enterprise Communications France S.A.S., 6/8 Avenue de la Grande Lande, F-33174
Gradignan, France, Phone: +33 5 57 35 63 00, Fax: +33 5 56 89 14 05
Internet: *www.funkwerk-ec.com*

Table of Contents

Chapter 1 Important Information

1.1 Preparation and update with the FCI

The update of the system software with the Funkwerk Configuration Interface uses a BLUP file (bintec Large Update) so as to update all necessary modules intelligently. All those elements that are newer in the BLUP than on your gateway are updated.

Note

The result of an interrupted updating operation could be that your gateway no longer boots. Hence, do not turn your gateway off during the update.

To prepare and perform an update with the **Systemsoftware 7.10.1** Funkwerk Configuration Interface, proceed as follows:

(1) For the update, you'll need the `XXXXX_bl71001.xxx`file, where `XXXXX` stands for you device. Ensure that the file that you require for the update is available on your PC. If the file is not available on your PC, enter *www.funkwerk-ec.com* in your browser. The Funkwerk homepage will open. You will find the required file in the download area for your gateway. Save it on your PC.

(2) Save the current boot configuration prior to the update. Export the current boot configuration with the menu **Maintenance**->**Software &Configuration** in the Funkwerk Configuration Interface. Select: **Action** = *Export configuration*, **Current File Name in Flash** = *boot*, **Include certificates and keys** = *enabled*, **Configuration Encryption** = *disabled* Select with **Go**. The window **Open <Name des Gateways>.cf** opens. Keep the selection *Save file* and click **OK** to save the configuration on your PC. The file `<Name of the gateway.cf>` is stored, the window **Downloads** shows the stored file.

(3) Perform the update on system software 7.10.1, via menu **Maintenance**->**Software &Configuration**. To do this, select: **Action** = *Update system software*, **Source Location** = *Local File*, **Filename** = *XXXXX_bl71001.xxx*. Confirm with **Go**. The message “System request. Please stand by. Operation in progress.” or “System Maintenance. Please stand by. Operation in progress.” shows that the selected file is being uploaded to the device. When the upload procedure is finished, you will see the message “System - Maintenance. Success. Operation completed successfully”. Click **Reboot**. You will see the message “System - Reboot. Rebooting. Please wait. This takes approximately 40 seconds”. The device will start with the new system software, and the browser window will open.

1.2 Downgrade with the FCI

If you wish to carry out a downgrade, proceed as follows:

(1) Replace the current boot configuration with the previous backup version. Import the backed-up boot configuration via the **Maintenance**->**Software &Configuration** menu). To do this, select: **Action** = *Import configuration*, **Configuration Encryption** = *disabled*, **Filename** = *<name of the device>.cf*. Confirm with **Go**. The message “System request. Please stand by. Operation in progress.” or “System Maintenance. Please stand by. Operation in progress.” indicates that the selected configuration is being uploaded to the device. When the upload procedure is finished, you will see the message “System - Maintenance. Success. Operation completed successfully.” Click **Reboot**. You will see the message “System - Reboot. Rebooting. Please wait. This takes approximately 40 seconds.” The device will start and the browser window will open. Log into your device.

(2) Carry out the downgrade to the desired software version over the **Maintenance**->**Software &Configuration** menu.
To do this, select: **Action** = *Update system software*, **Source Location** = *Local File*, **Filename** = *R3000_b17901.r3d*(example). Confirm with **Go**. The message “System request. Please stand by. Operation in progress.” or “System Maintenance. Please stand by. Operation in progress.” shows that the selected file is being uploaded to the device. When the upload procedure is finished, you will see the message “System - Maintenance. Success. Operation completed successfully”. Click **Reboot**. You will see the message “System - Reboot. Rebooting. Please wait. This takes approximately 40 seconds”. The device will start with the new system software, and the browser window will open.

You can log into your device and configure it.

1.3 Sierra Wireless MC8700 firmware update for RS232bu+

In order to insure UMTS functionality on the **RS232bu+** devices, please perform a firmware update specifically for the Sierra Wireless MC8700 module before using the UMTS SIM card.

Proceed as follows:

(a) On the Internet, download under *http://www.funkwerk-ec.com* in the download area for the **RS Series** with **Release 7.10.1** software file `MC8700_M3_0_9_0.ced` and save it on the PC on which you are performing the firmware update.

(b) Perform the update via menu **Maintenance**->**Software &Configuration**.

To do this, select: **Action** = *Update system software*, **Source Location** = *Local File*, **Filename** = *MC8700_M3_0_9_0.ced*. Confirm with **Go**. The message “System request. Please stand by. Operation in progress.” or “System Maintenance. Please stand by. Operation in progress.” shows that the selected file is being uploaded to the device. When the upload procedure is finished, you will see the message “System - Maintenance. Success. Operation completed successfully”.

⚠ **Important**

The update process takes about 4 minutes!

Chapter 2 New Functions

Systemsoftware 7.10.1 includes a number of new functions that significantly extend the performance over the previous version of the system software.

Note

Please note that not all new functions may be available for your device. Refer to the current data sheet of your device or to the respective manuals when in doubt.

2.1 FCI provider selection in Internet access assistant

The selection for configuration of an Internet access in the FCI assistant has been simplified. Here, you first select the **Type** of the provider, then choose between *User-defined* and *Predefined*. For *User-defined*, the user can perform her individual provider settings. For *Predefined* an additional field **Country** is displayed. When selecting the desired **Country**, only the corresponding entries appear in the **Internet Service Provider** field.

2.2 FCI - Display of the WAN interfaces on the status page

In the menu **System Management**->**Status** no more **System Messages** are displayed in the lower area. Now, the status of the **WAN Interfaces** is displayed here. Their **Description**, the **Connection Data** and the current status of the connection are displayed under **Link**.

2.3 FCI - Display of the UMTS interface

On status page **System Administration**->**Status** the status of any existing UMTS interface is displayed in the **Physical Interfaces** area. You'll see a graphic representation of reception quality, and of the corresponding signal strength in dBm.

You'll also find this display in the **Physical Interfaces**->**UMTS/HSDPA**->**UMTS/HSDPA/HSUPA** ->🔧 menu, under the **Network Quality** designation.

2.4 FCI - Modify mode of new interfaces

In the **System Management**->**Interface Mode / Bridge Groups**->**Interfaces** menu, you can edit the mode of additional interfaces by selecting the **Add** button. A page opens, on which you may select the desired interface in the **Interface** field. After clicking on **OK**, you can configure the interface mode as desired on the overview page (*Routing Mode* or *New Bridge Group* or select existing bridge groups).

2.5 FCI - Flow control for ethernet interfaces

In the **Physical Interfaces**->**Ethernet Ports**->**Port Configuration** menu, you can select whether to perform a **Flow Control** on an ethernet interface. The following possible values are available.

- *Disable* (default value): No flow control is performed.
- *Enabled*: Flow control is performed.
- *Auto*: Automatic flow control is performed.

2.6 FCI- IPSec callback via UMTS

IPSec callback is used to cause an IPSec peer to set up an Internet connection, thus allowing an IPSec tunnel over the Internet. With a direct call over the UMTS mobile phone network, you can signal that you are online and waiting for the peer to set up an IPSec tunnel over the Internet. If the called peer currently has no connection to the Internet, the mobile call causes a connection to be set up.

You configure the UMTS card in the **Physical Interfaces**->**UMTS/HSDPA**->**UMTS/HSDPA/HSUPA** ->**Edit** menu. The *IPSec* option for **Incoming Service Type** is now available for this purpose.

In the **VPN**->**IPSec**->**IPSec Peers**->🔧->**Advanced Settings** menu, you may also select under **Transfer own IP address over ISDN/GSM** whether the IP address shall be sent along to IPSec tunnel setup in the callback UMTS call. This may shorten and simplify tunnel setup.

2.7 FCI - GSM Fallback

In the **Physical Interfaces**->**UMTS/HSDPA**->**UMTS/HSDPA/HSUPA** ->🔧 menu, you can enter the call number for the GSM Fallback function under **Fallback Number**. When a voice calls goes in on this number, any active connection is immediately disconnected and the operating mode of the modem reset to GSM, where the modem remains until another data call (PPP, ISDN login, IPSec callback) comes in. If flatrate mode is enabled for the WAN connection (Option **Always up** in **WAN**->**Internet + Dialup**->**GPRS/UMTS**->🔧), this leads to immediate restoration of connection setup.

Please note that the SIM card must support this function, and that not all mobile telephony providers relay voice calls over data SIM cards.

2.8 FCI - UMTS PUK entry field

An field for entry of the PUK is now displayed in the **Physical Interfaces**->**UMTS/HSDPA**->**UMTS/HSDPA/HSUPA** ->🔧 menu.

2.9 UMTS - Sierra Wireless AirCard 319U supported

The USB UMTS stick **Sierra Wireless AirCard 319U** is supported.

2.10 FCI - Advanced overview for network routes

In reorganised menu **Networking**->**Routes**->**IP Routes** are now displayed under **Type** the network type (*Direct* or *Indirect*), and the **Protocol**.

2.11 FCI - Modified QoS filter configuration

The configuration of QoS filters in menu **Networking**->**QoS**->**QoS Filter**->**New** has been extended. Now, you can select predefined services in the **Service** field, or perform individual settings via the *User defined* option.

For parameters **Destination IP Address/Netmask** and **Source IP Address/Netmask** you have the option of specifying the **Type** of the address. *Any*, *Host* and *Network* are available for selection.

2.12 FCI - Modified QoS interface configuration

The configuration of the QoS interfaces in menu **Networking**->**QoS**->**QoS Interfaces/ Policies**->**New** has been extended. Now, you can select predefined encryption methods in the **Encryption Method** field for packets sent on this IPSec interface.

Possible values are `DES, 3DES, Blowfish, Cast - (cipher block size = 64 Bit)` and `AES128, AES192, AES256, Twofish - (cipher block size = 128 Bit)`.

2.13 FCI - Configuration of access rules

The **Networking** menu has been completed with a new **Access Rules**.

In the **Networking**->**Access Rules** menu, you define whether and how access to data and functions is to be restricted (which user gets to use what services and files).

In the **Access Filter** menu, you define filters for IP packets in order to allow or block access from or to the various hosts in connected networks. This enables you to prevent undesired connections being set up via the gateway. For this, you define the type of IP traffic the gateway is to accept or deny.

In the **Rule Chains** menu, you define the actions to be performed if the conditions defined in **Access Filter** arise. You can create multiple, separate rule chains. The same filter can also be used in different rule chains.

In the **Interface Assignment** menu, you define which rule chain should be applied to which interface.

⚠ **Caution**

Make sure you don't lock yourself out when configuring filters!

2.14 FCI - Specify MTU for PPPoE connections

In the **WAN**->**Internet + Dialup**->**PPPoE** menu, it's now possible to specify the maximum packet size (Maximum Transfer Unit, **MTU**) in Bytes, that may be used for the connection.

With default value `Automatic`, the value is specified by link control at connection setup.

If you disable `Automatic`, you can enter a value.

Values up to *8192* are possible.

Default value is *0*, meaning automatic negotiation.

2.15 FCI - Timeout for inactivity of PPP connections modified

For PPP connections, a value between *0* and *10* can now be specified for the period in seconds which must elapse until the connection is released if no more payloads are sent. Configuration occurs in the menu **WAN**->**Internet + Dialup**->**<Connection type>**->**New** in the **Connection Idle Timeout** field.

2.16 FCI - Status modification of IPSec connections

In the **VPN**->**IPSec**->**IPSec Peers** menu, it's now possible to activate or deactivate an IPSec connection. You configure it peer table column **Action**.

2.17 FCI - Lifetime of an IPSec IKE phase 1 key in percentage

In menu **VPN**->**IPSec**->**Phase-1 Profiles**->**New** you can now also enter the **Lifetime** of an IKE phase 1 key in percentage.

2.18 FCI - IKE Version 2

Note

IKE V. 2 is currently available only for the devices of the RS and R(T)xx02 series.

For administration of the Security Association (SA) for IPSec tunnel setup, use of version 2 of the Internet Key Exchange Protocol (IKE) is now also available.

In menu **VPN IPSec IPSec Peers** two separate areas are thus now displayed in the overview of the IPSec peers. The lower table displays all IPSec peers for which use of IKEv2 was selected. You perform the selection in the **VPN IPSec IPSec Peers** 🔧 / **New** menu, in the **Internet Key Exchange** field. Possible values here are *IKEv1* and *IKEv2*.

Moreover, in the **VPN**->**IPSec**->**Phase-1 Profiles** menu, the profiles are divided according to IKEv1 and IKEv2 use. Under **Create new IKEv2 Profile** select the **New** button to perform your required phase 1 settings with IKEv2.

2.19 IPSec - NAT-T

For IPSec connections with enabled NAT negotiation, switching to UDP port 4500 can be forced, even if no NAT has been recognised on either side. Please note that this function only operates in Initiator mode, and that the IPSec partner must also have NAT negotiation activated. The feature is configured in menu **VPN**->**IPSec**->**Phase-1 Profiles**->**New**->**Advanced Settings** with the new option *Enforce* for the field **NAT Traversal** (other options *Enabled* and *Disabled*).

2.20 IPSec - Precise calculation of the IPSec protocol header

A function has been integrated that allows precise automatic calculation of the size of IPSec packet headers. This proves necessary in rare cases, e.g. with parallel use of the QoS functionality.

2.21 FCI - Own PPTP IP Pool

In the **VPN**->**PPTP**->**IP Pools** menu, you configure the IP address areas for address assignment with PPTP connections.

Your device can operate as a dynamic IP address server for PPTP connections. You can use this function by providing one or more pools of IP addresses. These IP addresses can be assigned to dialling-in connection partners for the duration of the connection.

2.22 FCI - Complete filtering for firewall

In the **Firewall**->**Policies**->**Options** menu, the option **Full Filtering** is now available.

2.23 FCI - Media Gateway - TLS option missing

In the **VoIP**->**Media Gateway**->**SIP Accounts**->**New** menu, the option *TLS* for **Protocol** can now be configured.

2.24 Media Gateway - RFC 4040 - ISDN via IP

With application of the RFC 4040, it is now possible to convey 64 kbit/s channel data transparently in RTP packets, using a pseudo codec "clearmode".

2.25 Media Gateway - Display of the redirected call number

With extension of SIP P protocol support through the UPDATE element, the call number of forwarded calls can be displayed.

2.26 FCI - DHCP IP Poolname

In the **Local Services**->**DHCP Server**->**DHCP Pool**->**New** menu, a freely selected description for the IP addresspool can now be entered under **IP Pool Name**.

2.27 FCI - Extended Scheduling

The scheduling function has been fundamentally reworked for this release.

Your device now features an advanced event scheduler. Apart from default and easily configured standard applications like time- or volume-controlled activation or deactivation of interfaces, the event scheduler allows access to any MIB parameter. This means that any event in the MIB can be defined as the initiator of any desired action. You configure scheduling in the **Local Services**->**Scheduling** menu.

Note

To run the event scheduler, the date configured on your device must be 1.1.2000 or later.

Warning

Configuration of actions not available as defaults requires extensive knowledge of the system's mode of operation. An incorrect configuration can cause considerable disruption during operation. If applicable, save the original configuration on your PC.

You'll find information on MIB variables and their possible values in the online help of the configuration interface's SNMP browser view. Please note that this requires an active Internet connection.

2.28 FCI - E-mail RE in email notification

In the **External Reporting**->**E-mail Alert**->**E-mail Alert Recipient** menu, any text can now be entered in the **E-Mail Subject** field, which will appear in the subject line of the e-mail.

2.29 FCI - Modified interface monitoring details

In the **Monitoring**->**Interfaces** menu you can display the statistical data for the individual interfaces in detail via the 🔍 button. With the filter bar, you can select whether to display **Transfer Totals** or **Transfer Throughput**. You'll be able to consult the following data on interfaces: **Description**, **MAC Address**, **Tx Packets**, **Tx Bytes**, **Rx Packets**, **Rx Bytes**. The following values are displayed for the TCP connections active on the interface: **State**, **Local Address**, **Local Port**, **Remote Address**, **Remote Port**.

Chapter 3 Changes

The following modifications have been performed in **Systemsoftware 7.10.1** .

3.1 FCI - Modified wireless LAN controller configuration

The wireless LAN controller for setup and management of a WLAN infrastructure with several access points (AP's) has been modified and upgraded.

- In the **System Management**->**Global Settings**->**System** you can enter the static IP address of the wireless LAN controller at access points to be managed via a wireless LAN controller and located in an IP network operating exclusively with static IP addresses.
- In the **Wireless LAN Controller**->**Slave AP configuration**->**Slave Access Points** menu, table columns **Channel** and **Search Channel** are now displayed.
- In the **Wireless LAN Controller**->**Slave AP configuration**->**Slave Access Points** menu, an option for renewed channel selection is now offered. Click on the **Channel reallocation** button under **START** in order to reassign any assigned channels, e.g. when a new access point has been added.
- In the menu **Wireless LAN Controller**->**Slave AP configuration**->**Slave Access Points**->🔧 the data for wireless module 1 and wireless module 2 are now displayed, if the corresponding device contains two wireless modules. With devices featuring a single wireless module, the data for wireless module 1 are displayed. The previous **Wireless LAN Controller**->**Slave AP configuration**->**Radio Modules** thus lapses.
- In the menu **Wireless LAN Controller**->**Slave AP configuration**->**Wireless Networks (VSS)**->🔧 the option *AES and TKIP* in the**WPA Cipher** field and **WPA2 Cipher** lapses.
- In the new menu **Wireless LAN Controller**->**Monitoring**+**Wireless Networks** an overview of available wireless networks for currently-used access points is displayed. You see which wireless module is assigned to which wireless network. For each wireless a parameter set is displayed (**Location**, **VSS**, **MAC Address (VSS)**, **Channel**, **Clients**). New wireless networks can be added using the **Add** button. They are edited using 🔧.
- In the **Wireless LAN Controller**->**Monitoring**->**Neighbor APs** menu, a message now appears during an active scan, warning that the scanning process may take a long time, depending on the number of installed access points.
- The **Wireless LAN** menu and the **Wireless LAN** assistant are disabled on access points managed by a wireless LAN controller.

3.2 FCI - Modified routing configuration

The **Routing** menu has been modified, expanded and in the process divided into several areas.

3.2.1 Network

You can now configure the network routes in the **Networking** network. Here, the previous **Routes**, **NAT**, **Load Balancing**, **QoS** submenus are available.

Moreover, the **Networking** menu has been completed with a new **Access Rules**.

3.2.2 Apply routing protocol

In the new **Routing Protocols** menu, you can configure RIP and OSPF.

3.2.2.1 RIP

The **RIP** menu has been taken over unchanged from the previous software version.

3.2.2.2 OSPF

OSPF (Open Shortest Path First) is a dynamic routing protocol that is frequently used in larger networks as an alternative to RIP. It was originally developed to avoid a number of limitations of RIP (when used in larger networks).

You enter the addresses of the OSPF areas in the **Areas** submenu. In **Interfaces**, you specify for each existing interface whether, and in which mode, OSPF shall be activated. Under **Global Settings** you have the option of enabling or disabling the OSPF function, and of modifying its basic settings.

Monitoring

In the **Monitoring**->**OSPF** menu, information on OSPF is monitored . The OSPF monitor is arranged horizontally in three sections and shows information about OSPF interfaces, the detected neighbor and the Link State Database entries.

3.3 FCI - Modified and extended multicast configuration

The **Multicast** menu has been extended with a **General** submenu and **PIM**.

3.3.1 General

In the **General** menu, you now have the option of enabling or disabling the multicast function.

3.3.2 PIM

Protocol Independent Multicast (**PIM**) is a multicast-routing process that makes possible dynamic routing from multicast packets. With PIM the distribution of information is regulated via a central point, which is known as the rendezvous point. Data packets are initially routed here before being made available to other recipient routers.

Multicast routing protocols differentiates between sparse mode and dense mode. In dense mode, all packets are forwarded and only packets to groups that have been explicitly cancelled are rejected. In sparse mode, packets are only forward to groups if they have been ordered. Your device uses PIM in sparse mode.

Monitoring

The status of all configured PIM components is displayed in the **Monitoring**->**PIM**->**Global Status** menu.

3.4 FCI - QoS-Queue DEFAULT cannot be deleted

In the **Networking**->**QoS**->**QoS Interfaces/Policies**->**New**menu, no QoS Queue with **Priorisation queue** can be manually created under **Queues/Policies** *`Default`*. The required DEFAULT queue is automatically generated by the system at configuration, and cannot be deleted by the user. This DEFAULT Queue can be edited (except values for **Description**, **Outbound Interface**, **Priorisation queue** and **Priority**).

Chapter 4 Bugfixes

The following bugs have been eliminated in **Systemsoftware 7.10.1** :

4.1 IPSec - No dynamic peers with proxy ARP

(ID 11744)

For an IPSec peer with dynamic IP address configuration and configured proxy ARP, proxy ARP has been disabled at tunnel setup.

The problem has been solved.

4.2 FCI - Import of a configuration file is taking very long or has failed.

(ID 13055)

Import of a configuration file via the option *Import configuration* for **Action** in menu **Maintenance**->**Software &Configuration**->**Options** took a long time, and then failed.

The problem has been solved.

4.3 xDSL - No DSL data transmission

(ID 13301)

In DSL lines with a high number of CRC and HEC errors, there is a chance that no payloads could be transmitted over the connection.

The problem has been solved.

4.4 IPSec - Wrong IPSec Phase-2 policy leads to disconnection

(ID 13354)

In case of an existing IPSec connection, this could lead to disconnections at renegotiation, as the wrong Source IP address was used, triggering ISAKMP message 18 (INVALID-ID-INFORMATION) from the connection partner.

The problem has been solved.

4.5 FCI - Faulty Keepalive configuration for IPSec Phase-2

(ID 13443)

Disabling of Keepalive messages by selecting option `Inactive` for **Alive Check** in menu **VPN**->**IPSec**->**Phase-1 Profiles**->**New** was faulty and led to numerous error messages at the third-party product on the remote terminal.

The problem has been solved.

4.6 Certificates - Deletion of temporary certificates led to stacktrace/reboot

(ID 14051)

Deleting a temporary certificate can lead to a stacktrace or system reboot.

The problem has been solved.

4.7 FCI - No VLAN option for PPPoE connections available

(ID 14065)

In the **WAN**->**Internet + Dialup**->**PPPoE**->**New** menu, there was none and opening the menu brought error messages.

The problem has been solved.

4.8 FCI - Unclear DSL mode description

(ID 14155)

On devices with differing DSL variants (e.g. **R3502** with ADSL1 + ADSL2 + ADSL2+ + VDSL), the name of the automatic mode for ADSL in the **Physical Interfaces**->**ADSL Modem**->**ADSL Configuration** menu was subject to error. *Automatic Mode* has been renamed to *ADSL Automode*.

4.9 FCI - Firewall filter rule configuration led to stacktrace and panic

(ID 14209)

If an entry was opened in the **Firewall**->**Policies**->**Filter Rules**->**New** menu and closed with **OK** or **Cancel** stacktrace and panic resulted.

The problem has been solved.

4.10 RTSP - RTSP data stream for video on demand not possible

(ID 14261)

Because of faulty NAT settings, no RTSP data for video on demand could be transmitted.

The problem has been solved.

4.11 FCI - Wrong timing for web filters

(ID 14324)

As the time for web filter entries was inconveniently based on UTC, real time for web filtering did not correspond to the values configured in **Schedule (Start / Stop Time)** in the **Local Services**->**Web Filter**->**Filter List**->**New** menu.

The problem has been solved.

4.12 FCI - Faulty ISDN login settings in administrative access

(ID 14357)

If, in menu **System Management**+**Administrative Access**->**Access** die Option *ISDN-Login* was disabled for a specific interface, ISDN login was no longer possible for any of the available interfaces on the device.

The problem has been solved.

4.13 FCI - Faulty deletion of RIP filters

(ID 14366)

If a single entry was deleted in the **Routing Protocols**->**RIP**->**RIP Filter** menu, all other table entries were also deleted.

The problem has been solved.

4.14 FCI - Wrong indication in statistics for load sharing-data traffic

(ID 14394)

In the **Networking**->**Load Balancing**->**Load Balancing Groups**->🔍menu faulty values were displayed for **Download Traffic** and **Upload Traffic** .

The problem has been solved.

4.15 FCI - Wrong interface selection for BRRP

(ID 14446)

In the **Local Services**->**BRRP**->**Virtual Routers**->**New** menu, ethoa interfaces were incorrectly also offered in selection for **Ethernet Interface**.

The problem has been solved.

4.16 FCI - Faulty interface mode switch

(ID 14449)

If the mode of an interface has first been set on bridging and then back to routing in menu **System Management**->**Interface Mode / Bridge Groups**->**Interfaces**, either the IP configuration of this interface was lost, or a stacktrace occurred.

The problem has been solved.

4.17 Certificates - Faulty certificate key length and DSA selection

(ID 14479)

If, in menu **System Management**->**Certificates**->**Certificate List**->**Certificate Request**, settings for **Generate Private Key** other than the standard value *RSA 1024* bits were specified, the default value was still always used.

The problem has been solved.

4.18 Hotspot - Missing table labelling

(ID 14492)

In menu **Local Services**->**HotSpot Gateway**->**HotSpot Gateway** the labelling of the table column in which the hotspot entries can be enabled or disabled was missing. This is now called **Status**.

The problem has been solved.

4.19 ATM - Wrong preset MAC Address

(ID 14519)

When selecting the option **Use built-in** for parameter **MAC Address** in menu **WAN**->**ATM**->**Profiles**->**New**, the wrong MAC address was entered in the system.

The problem has been solved.

4.20 Media Gateway - Too few possible call routing entries

(ID 14521)

In menu **VoIP**->**Media Gateway**->**Call Routing**, a maximum of only 100 entries was possible.

The problem has been solved.

4.21 Media Gateway - Faulty SRTP option for SIP accounts

(ID 14580)

In **VoIP**->**Media Gateway**->**SIP Accounts**->**New**->**Advanced Settings** the option *SRTP* for **Sort Order** was not properly set and didn't work.

The problem has been solved.

4.22 IPSec - Phase-2 profile not marked as standard profile

(ID 14581)

In menu **VPN**->**IPSec**->**IPSec Peers**->**New**->**Advanced Settings** the asterisk (*) was missing in the default **Phase-2 Profile**.

The problem has been solved.

4.23 IPSec - Fault phase-1 profile key length with AES

(ID 14584)

In the **VPN**->**IPSec**->**Phase-1 Profiles**->**New** menu, the key length for the **Encryption** of the **Proposals** with AES was incorrectly calculated. Now the fixed values *AES-128*, *AES-192* and *AES-256* are available.

4.24 SNMP-Browser - Stacktrace at entry in biboAdmUsrTrapTable

(ID 14588)

When making a new entry in biboAdmUsrTrapTable over the SNMP browser, stacktrace occurred.

The problem has been solved.

4.25 Webfilter - No Internet after disabling of web filters

(ID 14600)

If the web filter status was also disabled **Local Services**->**Web Filter**->**General**, Internet access over HTTP was no longer possible.

The problem has been solved.

4.26 Media Gateway - Faulty fax identification with outgoing fax

(ID 14646)

When the media gateway was used as a Remote CAPI Fax Gateway, it sometimes occurred that the fax tone for outgoing faxes was not recognised.

The problem has been solved.

4.27 UMTS - Problems at connection setup to UMTS/ GPRS networks

(ID 14652)

With poor signal quality, it might occur that no connection could be established to some UMTS/GPRS networks.

The problem has been solved.

4.28 FCI - Access and QoS filters: TCP/UDP missing

(ID 14665)

Parallel selection of TCP and UDP for **Protocol** in menu **Routing**->**QoS**->**QoS Filter**->**New** was not possible. Now a *tcp/udp* option is available. Because of the reorganised routing menu, this option can now be found in the **Networking** menu.

4.29 FCI - DSP module info missing on status page

(ID 14689)

Inserted DSP modules were not displayed in **System Management**->**Status**->**Modules**.

The problem has been solved.

4.30 PPTP - Superfluous numbers with disabled callback

(ID 14691)

If a previously used callback function for PPTP connections was deactivated, the entered callback number was not deleted. Manual deletion also failed.

The problem has been solved.

4.31 FCI - No Internet Explorer 9 support

(ID 14714)

The **Funkwerk Configuration Interface** can now also be used correctly with Microsoft Internet Exploreer 9.

4.32 Wireless LAN Controller - WTP reboot with multiple SSID's

(ID 15138)

If several SSID's were operated in a wireless scenario with multiple WTP's managed by the wireless LAN controller, it sometimes might happen that WTP's in the network sporadically restarted.

The problem has been solved.

4.33 FCI - Wrong protocol for manual routing entries

(ID 15127)

If a routing entry was generated in the **Routing**->**Routes**->**IP Routes**->**New** menu, the protocol was set by default to *netmgmt*. This value was modified to *local* and can be viewed in the route overview in the new, modified routing menu under **Networking**->**Routes**->**IP Routes** under **Protocol**.

The problem has been solved.

4.34 FCI - Faulty display for ISDN usage external

(ID 15054)

In menu **System Management**->**Status** the PRI channels might not be displayed under **ISDN Usage External**.

The problem has been solved.

4.35 FCI - PPP passwords incorrectly included at configuration export

(ID 15044)

If, in the **Maintenance**->**Software &Configuration**->**Options** menu,a configuration file with status information (**Action** = *`Export configuration with state information`*) was exported, all PPP passwords were included unencrypted. As a configuration file with status information is used for support purposes, however, and no passwords may be included without encryption, these were removed.

4.36 IPSec - Bad connection setup

(ID 14985)

Connection setup to IPSec peers was slow, if many peers were configured. The device might also be completely blocked.

The problem has been solved.

4.37 Wireless LAN Controller - New channel designation

(ID 14980)

In the **Wireless LAN Controller**->**Controller Configuration**->**Slave Access Points** menu, the **Channel reallocation** button was displayed, even if the wireless module was unconfigured and no wireless profile was assigned.

The problem has been solved.

4.38 Wireless LAN Controller - Faulty IP address handling

(ID 14794)

If the wireless LAN controller was operated with static IP addresses, and in the **System Management**->**Global Settings**->**System** menu an IP address given under **Manual WLAN Controller IP Address**, still no communication could be established between controller and WTP's.

The problem has been solved.

4.39 IPSec - Malfunction and stacktrace with IPhone as dynamic IPSec client with XAUTH

(ID 14194)

When IPhones were connected to XAUTH using IPSec, connection setup failed and stacktrace occurred.

The problem has been solved.

4.40 WLAN - Frequent stacktraces and reboot at access points

(ID 14137)

At access points, especially **bintec Wx002**, there were frequent unexpected reboots.

The problem has been solved.

4.41 Media Gateway - Frequent stacktraces and reboots

(ID 14082)

When the media gateway was connected to an exchange VoIP server, there were frequent stacktraces and reboots.

The problem has been solved.

4.42 FCI - Dynamic DNS server not possible in the assistant

(ID 14728)

In assistant **First steps** it was not possible to configure the device in such a way that it dynamically accessed a DNS server from the ISP, and entry of a fixed IP address for a DNS server was required. This has been modified. It is now possible to activate the **Fixed DNS Server Address** option and to enter two alternate DNS server addresses (**DNS Server** 1 and **DNS Server** 2). By default, the option is not enabled, i.e. a DNS server of the ISP is dynamically employed.

4.43 FCI - Incorrectly preconfigured options in the assistant

(ID 14844)

In assistant **Internet Access** incorrectly predefined values were offered for the respective modem type (ADSL, VDSL) for **Internet Service Provider**.

The problem has been solved.

4.44 Wireless LAN Controller - Monitoring shows inactive SSID's

(ID 14897)

Inactive SSID's were incorrectly displayed in the **Wireless LAN Controller**->**Monitoring**->**Wireless Networks** menu.

The problem has been solved.

4.45 FCI - Route modification for IPSec peer not possible

(ID 14900)

Modification of **Route Type** of a IPSec peer route from *`Network Route`* to *`Default Route`* in menu **Networking**->**Routes**->**IP Routes** (previously **Routing**->**Routes**->**IP Routes**) was performed incorrectly.

The problem has been solved.

4.46 FCI - Default user password for RADIUS in wrong position

(ID 14903)

Configuration of **Default User Password** in menu **System Management**->**Remote Authentication**->**RADIUS**->**New** was up to now erroneously configurable only in RADIUS dialout context **Advanced Settings**. As this, however, can have more general uses, the parameter can now be found under **Basic Parameters**.

4.47 FCI - Superfluous number in ISDN port configuration

(ID 14915)

The field **P-P Base Number** in menu **Physical Interfaces**->**ISDN Ports**->**ISDN Configuration**->🔧 (with **Autoconfiguration on Bootup** disabled, **Port Usage** = *Dialup (Euro ISDN)* and **ISDN Configuration Type** *Point-to-Point* is only required for devices with media gateway.

The problem has been solved.

4.48 PPP - CHAP authentication failed

(ID 14947)

Because of a too narrow value range for the "Challenge Length" field in a CHAP authentication packet, CHAP authentication failed for remote terminals with higher values.

The problem has been solved.

4.49 FCI - Faulty description at certificate import

(ID 14963)

When importing a certificate with **System Management**->**Certificates**->**Certificate List**->**Import** with empty field **Local Certificate Description** the automatically generated certificate name was not saved in certificate entry under **Description**. Hence, an entry in **Local Certificate Description** has now been forced.

The problem has been solved.

4.50 FCI - Local GRE IP address without entry not possible

(ID 14969)

In menu **VPN**->**GRE**->**GRE Tunnels**->**New** an unnecessary entry was forced in **Local GRE IP Address**.

The problem has been solved.

4.51 IPSec - Wrong maximum number IPSec phase-1

SA's

(ID 14987)

As the maximum number for Phase-1 SA's was overly restricted, older SA's were automatically deleted when further negotiation was required.

The problem has been solved.

4.52 UMTS - ISDN login with GSM was not operating

(ID 14996)

If a device was configured with **Preferred Network Type** *GPRS only* and **Incoming Service Type** *ISDN Login* (Menu **Physical Interfaces**->**UMTS/HSDPA**->**UMTS/HSDPA/HSUPA** ->🔧), though the incoming ISDN data call was visible in debug messages, no connection could be established.

The problem has been solved.

4.53 FCI - Configuration of the SHDSL 4 wire mode not possible

(ID 14790)

Configuration of the SHDSL 4 wire mode (**Wire Mode** *4 wire*) in menu **Physical Interfaces**->**SHDSL**->**Modem**->**SHDSL Configuration** led to errors.

The problem has been solved.

Chapter 5 Known Issues

The following problems have been identified in **Systemsoftware 7.10.1** :

5.1 Wireless LAN Controller - WTP Software update is not operating

In a wireless LAN controller installation with an AC on software release 7.10.1 and an WTP with software release 7.9.6, though updating does occur with software update to 7.10.1 on the WTP, the system does not automatically reboot, preventing the new system software being activated on the WTP.

In this case, perform one of the following actions:

(a) Restart the WTP manually by removing the power cord from the power supply, then reconnecting it. Systemsoftware 7.10.1 is activated on the WTP.

(b) Deactivate the WTP over the AC, thus also triggering a WTP reboot. For this, de-select the value **Administration Status** in menu **Wireless LAN Controller**->**Slave AP configuration**->**Slave Access Points** and click on **OK**.

5.2 Wireless LAN Controller - No support for a second IP address

If a second IP address is configured on the ethernet interface over which the WTP's of a wireless LAN controller installation are managed, connection to all WTP's is lost. Hence, it is not possible in wireless controller installations to link a second IP address on the corresponding ethernet interface.

5.3 IPSec Callback via UMTS - No configuration for connection to ISDN partner

(ID 15038)

For IPSec Callback via a UMTS connection the IP address exchange cannot be done via the D channel, but via the B channel. The ISDN partner must support V.110 (9600) or ISDN voice services for this purpose (depending on the provider and the SIM card and modem capabilities). The connection from the GSM modem to an ISDN partner, however, cannot be configured yet.

5.4 IPSec - Panic with IKEv2 Tunnel

(ID 15079)

With an active IPSec tunnel using IKEv2 for phase 1, a panic can happen when a Delete message for a Child SA is received.

5.5 IPSec - Endless loop with IKEv2 tunnel

(ID 15318)

Deactivating the IPSec subsystem when having an active IPSec peer with IKEv2 results in an endless loop.

5.6 IPSec - Sporadic Panic and Stacktrace

(ID 15359 und ID 15298)

Under the following circumstances panic and stacktrace may occur:

- Dynamic IPSec peers with RADIUS authentication.
- Phase 2 ran through rekeying at least once for a peer.
- High system load because of numerous connects and disconnects of phase 1 and phase 2.