# RipEX2 - Release Notes

## Release 2.2.0.0

2024-08-30

- Main component versions:
  - CNF version: 24
  - Web client version: 1.70.0
- Warning:
  - FW Version 2.x is **not over the air compatible** with 1.x versions
- New features:
  - System
    - New NETCONF API supporting reading and modifying the Device > Configuration. This configuration data is defined by the YANG model.
  - Security
    - Unit configuration is fully validated. Validation is triggered at unit start-up and at any configuration change during operation.

      **Note**

      Until now, the configuration was fully verified only in the web interface. If the configuration was updated in another way, the current configuration may not be valid. In this case follow the instructions below in the Known Issues section to ensure a smooth FW upgrade.

    - For compatibility reasons, the OpenVPN tunnel now allows the use of legacy SHA1 ciphers
  - Serial protocol
    - IEC 101 supports RTU reset
    - PPP protocol supports TETRA terminal connection
  - Routing
    - DHCP server implemented. Up to 16 instances of DHCP servers can run simultaneously on different interfaces. The server can also assign static IP addresses.
    - DNS forwarding service implemented. DNSSEC is supported.
    - Link manager is extended by the possibility of switching back-up routes to PPP and PPPoE.
    - PPP protocol supports Masquerade.
- Fixed bugs:
  - Fixed occasional incorrect ICMP ping termination
  - Correction of Cellular connection registration if the cellular network supports only 4G technology
  - The PPP protocol now allows you to use an empty username and password
  - Web interface
    - Firmware activation when using Remote access may result in an error - fixed.
    - Unification of system log names (tools/logs)
    - Missing parameter added: Advanced > Interfaces > Radio > Encryption > Passphrase (secondary)
    - Fixed item access rights: Settings > Interfaces > Radio > Encryption > Passphrase (secondary)
- Known issues:
  - After installing FW version 2.2.0.0 and higher, a full configuration validation is now performed each time the unit is booted. After installing this newer FW version, when the station is started for the first time, a situation may occur that the saved configuration does not pass full validation (this situation can occur if the configuration was updated in a way other than using the web interface). Even in this case, **the unit starts correctly** and works as it did before installing the new FW version. An invalid configuration is indicated to the user by the system event "Boot configuration contains

errors" (SYS LED indicates Alarm). The notification area contains an error message with a detailed description of the configuration items that did not pass validation. These invalid entries must be manually corrected (changed to a value that passes validation). It is only possible to change the configuration of the unit (save the new configuration) when all invalid entries have been corrected.

## Release 2.1.7.0

2024-06-07

- Main component versions:
  - CNF version: 23
  - Web client version: 1.69.0
- Warning:
  - FW Version 2.x **is not over the air compatible** with 1.x versions
- New features:
  - Security
    - Radio channel encryption is extended to include periodic exchange of encryption keys during operation
    - IPSec is extended with modern AEAD ciphers providing encryption and integrity checking in one algorithm
    - IPsec is extended with the possibility of using a PPK key
    - The service (uftp) ensuring the distribution of firmware in the network is updated to a new version to improve security
    - Security components are updated (Dropbear, NTP, NetSnmp)
  - Routing
    - The Babel protocol is extended to include the ability to respond to degraded line quality (Radio filter). By continuously evaluating the strength (RSS) and quality (MSE) of the signal and proportionally discarding Hello packets, it prevents unwanted switching to a low-quality route.
    - The Babel protocol is extended with the ability to filter routing rules (Relay filter) in order to reduce the amount of Babel protocol overhead data transmitted over the radio channel.
  - Diagnostics
    - Detailed Hot-standby Status is implemented
    - Improved Remote access error message in case of remote station not reachable
    - The web interface now provides the possibility of directly viewing the system logs of individual services
  - Interfaces
    - SW support was added for the new RipEX2 models supporting 2 COM ports on the DSUB connector
  - Web interface
    - The GRE tunnel configuration is extended by the Tunnel Name
    - The console dump filtering setting on the Diagnostics > Tools page is now disabled when the command is running. The purpose is to ensure consistency between the filter settings and the listing currently in progress.
    - Implementation of new corporate graphics - logos and icons
    - Implementation of a new screen for PPPoE client settings: Settings > Interfaces > PPPoE client
- Fixed bugs:
  - Advanced Network interface name checking has been added, which will ensure checking the maximum length of the interface name even in the case of VLAN configuration
  - Configuration of Flow control (RTS/CTS) on the COM port is now disabled if the COM port is switched to RS485 mode
  - Fixed incorrect display of TCP header values in monitoring
  - Fixed FTP connection not working when using NAT

 

    - Web interface
        - Improved error message when remote device is unavailable
        - Modifying the names of some IPSec parameters
- Known issues:
    - Firmware activation when using Remote access may result in an error. The firmware is correctly activated, but the user is not correctly informed about it.
      Workaround: Reload the web page

## Release 2.1.6.0

2024-03-13

- Main component versions:
    - CNF version: 22
    - Web client version: 1.68.0
- Warning:
    - FW Version 2.x **is not over the air compatible** with 1.x versions
- New features:
    - Security
        - Added a config item to prevent FW downgrade
        - Radio channel encryption extended by a second key enabling secure distribution of the new key and seamless switching from the old to the new key throughout the network
        - OpenVPN is extended by the possibility of authentication using user name and password
        - L2 Firewall has been expanded with Forward rules, which now enables full filtering of L2 forwarded traffic
    - Serial protocols
        - IEC 101 now supports spontaneous mode
    - System
        - The time in the RTC is periodically synchronized with the system time to increase the accuracy of the time stored in the RTC
    - Interfaces
        - PPPoE client is now available
    - Web interface
        - The L2 Firewall screen is redesigned: renaming Blacklist and Whitelist to Blocklist and Allowlist, adding a new Forward table.
        - New "Device incompatible" error screen in case the web client is not compatible with the unit
        - Highlighting the Status field on configuration screens
        - Credentials configuration expanded to include Certificate Subject Alternate Names (SAN) settings
        - The password input component has been expanded to include the option to copy to the clipboard and the option to hide/show the password
        - If the unit is unavailable at the same IP address after activating the new FW, an error message is displayed with information about the IP address change
- Fixed bugs:
    - Fixed false occurrence of "USB overcurrent" event when booting the unit.
    - Cellular
        - Fix rewriting of APN profiles from cellular network
    - Status screen: fix "Primary link down" event link to point to Link management Status
    - Fixed creating a trusted CA in the unit
    - DNAT rule for the EXT interface cannot be created – fixed
    - Fixed incorrect SNMP functionality when using a space in the "Security user name" parameter (used in SNMP v3).
    - Web interface

    - Fixed a bug when disconnecting from a remote device with older firmware
    - Fixed OpenVPN tunnel nested table configuration duplication feature
    - Fixed showing preferred cellular service in card view when using LPWAN on Settings > Interface > Cellular page
    - Fixed validation of Note item in Credentials configuration

## Release 2.1.2.0

2023-12-15

- Main component versions:
  - CNF version: 21
  - Web client version: 1.66.0
- Warning:
  - FW Version 2.x **is not over the air compatible** with 1.x versions
  - Due to the implementation of Security certificates storage, the “Credentials lost” event is triggered and SYS LED shines red (to indicate serious system alarm) when upgrading from FW version older than 2.1.0.0. The reason is the Credentials storage is empty (because it could not be initialized yet) which is indicated as an alarm. The future FW upgrades will not trigger the alarm any more as the Credentials storage is initialized once the 2.1.0.0 or newer FW is installed. The alarm is cleared by subsequent unit reboot.
- New features:
  - Security
    - OpenVPN server and client are implemented. Every unit can act both as a server and/or client.
    - Radio channel AES-256-CCM encryption is extended by Replay attack protection
    - Any Special characters can now be used in IPsec passphrase
    - Several configuration parameters (Severity, SNMP and SMS notification, Threshold field for all Events) are updated to require higher level (security technician level) of access rights
    - New Settings > Security > Management access menu combining settings of Webserver, Remote access and Service USB
  - Serial protocols
    - IEC 101 extension providing time synchronization
  - Interfaces
    - New Cellular module supporting LTE Cat M1/NB1/NB2 (Global bands, incl. 450 MHz) is now available
  - Diagnostics
    - RSS ping output is extended to provide worst signal level records
    - Most Status info panels are revised to provide more information
  - Web interface
    - Settings > QoS card-view is extended to show “Flow rate” units
    - Settings > Device > Software keys screen is extended to provide basic System information
    - Settings > Security > Credentials > Sign CSR > Choose File selection dialog now provides filtering by file extension
    - Settings > VPN > OpenVPN tunnel configuration can now be easily duplicated to create a new tunnel
- Fixed bugs:
  - FW distribution occasional crash – fixed
  - OpenVPN Server status uses incorrect column labels - fixed
  - BGP – MD5 password length limit is now properly set to 80 characters
  - Fixed overflow of long filenames in some places in the web interface
  - Fix required credential type on Settings > Security > Management access > Remote access page
  - Security > Credentials download/upload buttons are hidden when using remote connection

 

  - Remote access dialog improved to wrap IP addresses correctly
  - Settings > Security > Credentials > Credentials Note is wrapped correctly to prevent text overflow
  - Fixed size of TLS protection shared key ID field on Settings > VPN > OpenVPN page
- Known issues:
  - FW distribution problems may arise in certain circumstances. Please contact technical support for the correct procedure if this happens to you.
  - DNAT rule for the EXT interface can not be created
    Workaround: Select PPP protocol for any COM port.

## Release 2.1.1.0

2023-10-31

- Main component versions:
  - CNF version: 20
  - Web client version: 1.65.0
- Warning:
  - FW Version 2.x **is not over the air compatible** with 1.x versions
  - Due to the implementation of Security certificates storage, the “Credentials lost” event is triggered and SYS LED shines red (to indicate serious system alarm) when upgrading from FW version older than 2.1.0.0. The reason is the Credentials storage is empty (because it could not be initialized yet) which is indicated as an alarm. The future FW upgrades will not trigger the alarm any more as the Credentials storage is initialized once the 2.1.0.0 or newer FW is installed. The alarm is cleared by subsequent unit reboot.
- New features:
  - Security
    - OpenVPN server and client are implemented. Every unit can act both as a server and/or client.
    - OpenVPN server related Events are implemented: OpenVPN client connected, OpenVPN client disconnected
    - OpenVPN client related Events are implemented: OpenVPN tunnel 1 down … OpenVPN tunnel 4 down
    - When generating a new key for the web interface, only keys supported by current web browsers (RSA or OC) are allowed. The key fingerprints for the website and the keys from the certificate for the website are checked to check if they belong to each other.
    - The labels on the credentials screen have been improved to better match the described functionality.
    - The IPsec configuration overview has been extended with a “Note” field and “Management mode” field was removed to improve screen readability.
    - Entering passphrases is unified across the web client.
  - Firmware
    - Settings > Device > Firmware > USB screen is now available to configure USB flash drive firmware upgrade option.
  - Interfaces
    - Default MTU for cellular interface was changed to 1500 bytes.
  - SNMP
    - Settings > Services > SNMP > Status info section is now available.
    - The complete Engine ID value is now displayed in the SNMP Status.
    - MIB description fields updated to use “Username” and “User” labels correctly
    - The System uptime information is now available.
  - Diagnostics
    - Syslog can now be used to log all unit Events. Syslog enables logging to a remote server. Settings > Services > Syslog screen provides Status info and configuration options.

Note: A full copy of all events replaces the previous function copying only user login and logout events. The “Login attempt” parameter is removed. It is fully replaced by “Web interface login” and “Web interface login rejected” events.
    - New “Routing” and “COM” sections were added to the Status screen.
    - Status info section design was improved: Auto refresh provides more compact design; Download button offers the option of downloading the content of the status to a file.
  - System
    - Linux kernel updated to LTS version 6.1.38
- Fixed bugs:
  - PPP protocol does not work properly after a configuration change when flow control is active – fixed
  - Monitoring parameter “Include reverse” for COM and TS interfaces does not work – fixed
  - Remote access key configuration items are not properly translated – fixed
  - Different formatting of MAC addresses in Zabbix and MIB Browser – fixed
  - RipEX2e: COM2 cannot be enabled if COM1 is disabled – fixed
  - The lowest possible value Cellular interface MTU was updated to work correctly for the Cinterion TX62W module
  - Fixed diagnostic package generation to not include warning in case of GNSS module disabled
  - When a new SW key is uploaded, the web interface does not display new available features correctly – fixed
  - The "Sign CSR" button was incorrectly placed on the individual certificate tab. It is now moved correctly to the global context of the Credentials screen.
  - Settings > Firewall > L3 and NAT screens were rearranged to be uniform with the rest of the web client.
  - Diagnostics > Tools – Start and Run buttons are enabled also if there is valid data in the web store.
- Known issues:
  - FW distribution problems may arise in certain circumstances. Please contact technical support for the correct procedure if this happens to you.
  - OpenVPN Server status uses incorrect column labels. “Client address” and “Client port” should be used instead of “Server address” and “Server port”.
  - In case of replacing the Remote access key with a different one the configuration update results in error message “Compatibility error …”. This is not a proper error message. The error is caused by the fact there is a different authentication key on both units at the moment of updating the authentication key on a remote unit and still having the old one on a local unit.
    Workaround – Replace the Remote access key also on a local unit with a new one. Remote access should work correctly again using the new authentication keys.
  - Cellular interface “AUX” was renamed to “EXT” in version 2.0.13.0.
    If you upgrade from version 2.0.13.0 or older to version 2.0.14.0 or newer, and:
    1) the “AUX” Cellular interface was selected in *Babel* > *Network* > *Interface* or *OSPF* > *Network* > *Interface*, or
    2) in Firewall configuration the Cellular interface ”AUX” was selected manually using “Other” item in a List box (instead of selecting it directly from the List box items) à the FW upgrade causes configuration to be reverted to factory defaults.
    Workaround – Change the respective configuration item to other selection prior to FW upgrade. Revert the change back to “EXT” after the firmware upgrade. Renaming “AUX” to “EXT” is the cause of this issue.
  - Direct firmware upgrade from version 2.0.3.0 or older is not possible.
    Workaround – Upgrade firmware to version 2.0.10.0 prior to upgrading to 2.0.13.0 or newer.
  - Direct firmware upgrade from version 2.0.18.0 or older is possible in one of two ways
    - Upgrade firmware to version 2.1.0.0 prior to upgrading to 2.1.1.0 or newer
    - Use special upgrade package including the FWD abbreviation in its name. See the Firmware archive for download options.

 

  - The rule in the DNAT table for the EXT interface cannot be enabled. FW from version 2.0.18.0 are affected.
    Workaround: Set PPP protocol on any COM port.

## Release 2.1.0.0

2023-07-28

- Main component versions:
  - CNF version: 19
  - Web client version: 1.62.0
- Warning:
  - FW Version 2.x **is not over the air compatible** with 1.x versions
  - Due to the implementation of Security certificates storage, the “Credentials lost” event is triggered and SYS LED shines red (to indicate serious system alarm) after the first FW upgrade to version 2.1.0.0. The reason is the Credentials storage is empty (because it could not be initialized yet) which is indicated as an alarm. The future FW upgrades will not trigger the alarm any more as the Credentials storage is initialized once the 2.1.0.0 FW is installed. The alarm is cleared by subsequent unit reboot.
- New features:
  - Firmware
    - Firmware package security against unauthorized modifications is improved by adding asymmetric encryption
    - Firmware can be upgraded using USB Flash drive
  - Interfaces
    - RipEX2e DSUB interface now provides 2 COM ports instead of 1 COM.
    - Serial ports COM1 and COM2 configuration was extended by the possibility to define 5 and 6 stop bits (in addition to the current 7 and 8 stop bits).
  - Routing
    - Link Management implemented – adding a simple way to implement backup routes and to backup IPsec tunnels
  - Diagnostics
    - Default severity of several events was increased to get a better default unit status overview on the Status screen
  - Security
    - Security credentials (keys and certificates) subsystem including safe credentials storage was implemented: Various types of security credentials can be generated providing also Upload, Download and Update option. Whole Security credential storage Download, Replace and Update option.
    - Various types of security credentials can be used in unit configuration: Radio channel encryption, IPsec tunnels, Remote access authentication, Firmware distribution authentication, Web pages traffic encryption
- Fixed bugs:
  - PPP protocol reconfiguration stops proper protocol operation occasionally – fixed
  - COM ports 2 and 3 disablers were fixed
  - GNSS detection in various system configuration fixed
  - Time zone “America/Port” parameters fixed
  - Logging to a remote Syslog server fixed
- Known issues:
  - RipEX2e: COM2 can not be enabled if COM1 is disabled.
    Workaround - Enable COM1 if COM2 needs to be enabled.
  - Remote access key configuration items are not properly translated yet. The missing translation is:

    - UsAcc_RmtAccessClientKeySource … "Source of Remote access client key"
    - UsAccRmtA_ClientPrivKeyId … "Client private key ID"
  - In case of replacing the Remote access key with a different one the configuration update results in error message “Compatibility error …”. This is not a proper error message. The error is caused by the fact there is a different authentication key on both units at the moment of updating the authentication key on a remote unit and still having the old one on a local unit.
    Workaround – Replace the Remote access key also on a local unit with a new one. Remote access should work correctly again using the new authentication keys.
  - In case of replacing the Web server authentication certificate, the private key has to be generated using “RSA” or “EC” algorithms. Current web browsers do not support new "ED25519" and "ED448" algorithms. Validation of this configuration item is missing.
    Workaround – use only “RSA” or “EC” algorithms when generating a new Web server private key.
  - When a new SW key is uploaded, the web interface does not display new available features correctly.
    Workaround – logout and login again after SW key installation.
  - Cellular interface “AUX” was renamed to “EXT” in version 2.0.13.0.
    If you upgrade from version 2.0.13.0 or older to version 2.0.14.0 or newer, and:
    1) the “AUX” Cellular interface was selected in *Babel* > *Network* > *Interface* or *OSPF* > *Network* > *Interface*, or
    2) in Firewall configuration the Cellular interface ”AUX” was selected manually using “Other” item in a List box (instead of selecting it directly from the List box items) → the FW upgrade causes configuration to be reverted to factory defaults.
    Workaround – Change the respective configuration item to other selection prior to FW upgrade. Revert the change back to “EXT” after the firmware upgrade. Renaming “AUX” to “EXT” is the cause of this issue.
  - Direct firmware upgrade from the version 2.0.3.0 or lower is not possible.
    Workaround – Upgrade firmware version 2.0.10.0 prior to upgrading to 2.0.13.0 or higher.
  - An existing configuration of Babel interfaces needs to be updated manually by adding interface(s) Password(s). Standard configuration page *Settings* > *Routing* > *Babel* > *Network* > *Interfaces* cannot be used for this initial update. Subsequent updates work correctly on this configuration page.
    Workaround - Use *Advanced* > *Routing* > *Babel* > *Interfaces* > *Babel interface passwords* configuration page for this initial update.

## Release 2.0.18.0

2023-05-12

- Main component versions:
  - CNF version: 18
  - Web client version: 1.61.0
- Warning:
  - FW Version 2.x **is not over the air compatible** with 1.x versions
- New features:
  - SNMP
    - Several configuration items are now available (Enable/Disable status of: ETHx, COMx, TSx, Service USB, IPsec, GRE, QoS, FW, NAT, BGP, OSPF, BABEL, HS, Cellular, Monitoring; ETHx link speed; HS Radio MAC address; HS ETH MAC address), read-only.
    - HW dependent configuration items are returned as “no such instance” in case they are queried
    - Time stamp items data type “Counter32” changed to “Unsigned32”
  - Serial protocols
    - PPP protocol implemented

 

  - Security
    - SSH server updated to version 2022.83
- Fixed bugs:
  - Transparent protocol duplex operation occasional bug fixed
  - SNMP
    - “System boot completed” notification is now generated properly
    - “Radio signal statistics” table is now accessible without issues
    - “Radio signal non-addressable statistics” minimum and maximum values of RSS and MSE are now correct (minimum and maximum values were swapped)
  - Sleep mode “Waking period” is now measured properly
- Known issues:
  - Cellular interface “AUX” was renamed to “EXT” in version 2.0.13.0.
    If you upgrade from version 2.0.13.0 or older to version 2.0.14.0 or newer, and:
    1) the “AUX” Cellular interface was selected in *Babel* > *Network* > *Interface* or *OSPF* > *Network* > *Interface*, or
    2) in Firewall configuration the Cellular interface ”AUX” was selected manually using “Other” item in a List box (instead of selecting it directly from the List box items) → the FW upgrade causes configuration to be reverted to factory defaults.
    Workaround – Change the respective configuration item to other selection prior to FW upgrade. Revert the change back to “EXT” after the firmware upgrade. Renaming “AUX” to “EXT” is the cause of this issue.
  - Direct firmware upgrade from the version 2.0.3.0 or lower is not possible.
    Workaround – Upgrade firmware version 2.0.10.0 prior to upgrading to 2.0.13.0 or higher.
  - An existing configuration of Babel interfaces needs to be updated manually by adding interface(s) Password(s). Standard configuration page *Settings* > *Routing* > *Babel* > *Network* > *Interfaces* cannot be used for this initial update. Subsequent updates work correctly on this configuration page.
    Workaround - Use *Advanced* > *Routing* > *Babel* > *Interfaces* > *Babel interface passwords* configuration page for this initial update.
  - PPP protocol reconfiguration stops proper protocol operation occasionally.
    Workaround – Restart the unit or make any serial protocol configuration change (causing serial protocol restart).

## Release 2.0.17.0

2023-03-24

- Main component versions:
  - CNF version: 17
  - Web client version: 1.59.2
- Warning:
  - FW Version 2.x **is not over the air compatible** with 1.x versions
- New features:
  - RipEX2-9A extended frequency range 860-960 MHz supported
- Known issues:
  - Cellular interface “AUX” was renamed to “EXT” in version 2.0.13.0. If you upgrade from version 2.0.13.0 or older to version 2.0.14.0 or newer, and:
    1) the “AUX” Cellular interface was selected in *Babel* > *Network* > *Interface* or *OSPF* > *Network* > *Interface*, or
    2) in Firewall configuration the Cellular interface ”AUX” was selected manually using “Other” item in a List box (instead of selecting it directly from the List box items) → the FW upgrade causes configuration to be reverted to factory defaults.

Workaround – Change the respective configuration item to other selection prior to FW upgrade. Revert the change back to “EXT” after the firmware upgrade. Renaming “AUX” to “EXT” is the cause of this issue.
  - Direct firmware upgrade from the version 2.0.3.0 or lower is not possible.
    Workaround – Upgrade firmware version 2.0.10.0 prior to upgrading to 2.0.13.0 or higher.
  - An existing configuration of Babel interfaces needs to be updated manually by adding interface(s) Password(s). Standard configuration page *Settings* > *Routing* > *Babel* > *Network* > *Interfaces* cannot be used for this initial update. Subsequent updates work correctly on this configuration page.
    Workaround - Use *Advanced* > *Routing* > *Babel* > *Interfaces* > *Babel interface passwords* configuration page for this initial update.

## Release 2.0.16.0

2023-02-24

- Main component versions:
  - CNF version: 17
  - Web client version: 1.59.2
- Warning:
  - FW Version 2.x **is not over the air compatible** with 1.x versions
- New features:
  - System
    - GNSS implemented – time synchronization, position
    - Sleep mode – wake on Sleep input implemented
  - Interfaces
    - Network interface (Ethernet bridge) can be configured without any Ethernet port attached
  - Diagnostics
    - Invalid radio packets monitoring unified
    - NTP status extended
- Fixed bugs:
  - Cellular interface
    - Cellular interface naming in Statistics fixed
  - Monitoring
    - Ethernet interface monitoring did not work correctly in case only one direction (Tx or Rx) was enabled. Fixed: it is now possible to monitor either both direction or one direction only.
- Known issues:
  - Cellular interface “AUX” was renamed to “EXT” in version 2.0.13.0.
    If you upgrade from version 2.0.13.0 or older to version 2.0.14.0 or newer, and:
    1) the “AUX” Cellular interface was selected in *Babel* > *Network* > *Interface* or *OSPF* > *Network* > *Interface*, or
    2) in Firewall configuration the Cellular interface ”AUX” was selected manually using “Other” item in a List box (instead of selecting it directly from the List box items) → the FW upgrade causes configuration to be reverted to factory defaults.
    Workaround – Change the respective configuration item to other selection prior to FW upgrade. Revert the change back to “EXT” after the firmware upgrade. Renaming “AUX” to “EXT” is the cause of this issue.
  - Direct firmware upgrade from the version 2.0.3.0 or lower is not possible.
    Workaround – Upgrade firmware version 2.0.10.0 prior to upgrading to 2.0.13.0.
  - An existing configuration of Babel interfaces needs to be updated manually by adding interface(s) Password(s). Standard configuration page *Settings* > *Routing* > *Babel* > *Network* > *Interfaces*

 

cannot be used for this initial update. Subsequent updates work correctly on this configuration page.
Workaround - Use *Advanced* > *Routing* > *Babel* > *Interfaces* > *Babel interface passwords* configuration page for this initial update.

## Release 2.0.14.0

2022-12-16

- Main component versions:
  - CNF version: 16
  - Web client version: 1.58.0
- Warning:
  - FW Version 2.x **is not over the air compatible** with 1.x versions
- New features:
  - System
    - Sleep low power mode implemented
    - Sleep mode related event implemented
    - Firmware distribution – robust, configurable firmware update over the slow radio links
    - Firmware distribution events implemented
    - OTH-W3-WIFI adapter driver implemented
    - Several Events were updated to provide a possibility of sending SNMP and SMS notification
  - Routing
    - Routing option to set Metric for each routing rule implemented
    - Babel – Network neighbor authentication implemented
    - IPsec – List of active IPsec associations and Traffic selectors in the Status field now provides better formatting
    - IPsec – Traffic selectors filtering rules are now extended by IP protocol option
  - Interfaces – Cellular interface
    - Default MTU changed to 1430 Bytes
    - Cellular connection down event implemented
  - Security
    - Security subsystem updated (StrongSwan)
  - Firewall
    - L3 Firewall Input – Block list implemented
  - Diagnostics
    - Monitoring now provides RSS measurement of the Radio in the moments without active communication (background noise measurement)
    - Monitoring output enriched by translation of several EtherTypes
    - List of *Diagnostics* > *Information* > *SMS* messages is now sorted to show newest records first
    - Firmware upgrade screen now provides more information about installed FW and version of FW in archive in order to find out which update files can be used for the unit FW upgrade
  - Web interface
    - Radio Interface Status provides value of RF power in mW
    - Input field component size was optimized
    - All input fields are now validated on blur (after the input is completed)
    - *Diagnostic* > *Event* page Severity filter groups were updated
    - Monitoring File output is refreshed automatically
    - Notifications from Remote device are now identified by the Remote unit's name and/or address
    - User interface is redirected to Status page after successful firmware upgrade
    - Notification messages are sorted in descendent order in order to provide newest messages on top of the previous
    - *Diagnostics* > *Information* > *Static tab* renamed to *System* to better reflect its content
    - All dialog and modal windows updated to a new version of modal component
    - Activating firmware over Remote access is now supported. Firmware file to a Remote unit needs to be transferred using Firmware distribution service
    - New menu *Settings* > *Services*

 

        - Firmware distribution – configuration of distributing firmware across the radio network
        - SNMP, SMS and Hot standby configurations moved here
    - New screen *Settings* > *Device* > *Firmware* > *Distributed* providing receiver configuration of the firmware distribution service
    - Timeout of all requests from web interface to a unit is now 120 seconds
- Fixed bugs:
  - Serial interface
    - SAIA S-BUS: The first answer was not transmitted if operating in a SavePlus mode – fixed
  - Monitoring
    - Known issue “Monitoring of the IPsec encrypted packets on the Cellular interface does not work correctly” – fixed
    - Monitoring activated on disabled ETH port led to recovery mode – fixed
    - Monitored values of wideband RSS (in_pck_bbp) were incorrect in case of “Strange” packet reception – fixed
  - Web interface
    - Various layout and disable field fixes (Attach to network interface, ETH ports)
    - Update of Web inactivity timeout parameter fixed
    - *Diagnostics* > *Tools* > *ICMP ping* Source address does not offer WWAN interface address as it was not correct in all circumstances
    - Status info fields extra refresh suppressed
    - Sharing configuration files between RipEX2 and M!DGE3 minor fixes
    - Return to *Settings* > *Firewall* > *SNAT* and *DNAT* screens from Notification area – fixed
    - Web inactivity timeout calculation improved
  - System
    - Unit RTC update is now blocked when Tamper is active
    - Known issue “Disabling HTTP protocol together with Ethernet configuration changes can lead to unit recovery restart” – fixed
- Known issues:
  - If 1) the “AUX” Cellular interface was selected in Babel > Network > Interface or OSPF > Network > Interface, or
    2) in Firewall configuration the Cellular interface ”AUX” was selected manually using “Other” item in a List box (instead of selecting it directly from the List box items) → the FW upgrade causes configuration to be reverted to factory defaults.
    Workaround – Change the respective configuration item to other selection prior to FW upgrade. Revert the change back to “EXT” after the firmware upgrade. Renaming “AUX” to “EXT” is the cause of this issue.
  - Direct firmware upgrade from the version 2.0.3.0 or lower is not possible.
    Workaround – Upgrade firmware to any version between 2.0.5.0. and 2.0.10.0 prior to upgrading to 2.0.14.0.
  - Firmware upgrade using Patch files is possible only from version 2.0.13.0. Upgrade from older version is possible using full firmware file.
  - An existing configuration of Babel interfaces needs to be updated manually by adding interface(s) Password(s). Standard configuration page Settings > Routing > Babel > Network > Interfaces cannot be used for this initial update. Subsequent updates work correctly on this configuration page.
    Workaround - Use Advanced > Routing > Babel > Interfaces > Babel interface passwords configuration page for this initial update. Set an empty password for each Babel interface – 1 st Babel interface has Parent ID = 0, others follow (1, 2, …).

## Release 2.0.13.0

2022-08-26

- Main component versions:
  - CNF version: 15
  - Web client version: 1.57.2
- Warning:
  - FW Version 2.x **is not over the air compatible** with the 1.x versions
  - ”LastPass” web browser extension can cause problems while uploading new firmware. Disabling (temporary) this extension is recommended to ensure smooth firmware upgrade.
- New features:
  - Firewall:
    - Input and Output rules for L3 firewall implemented (Settings > Firewall > L3 > Input, Output)
  - Security:
    - Security components updated (dropbear, StrongSwan)
    - Tamper reset implemented (Settings > Security > Tamper reset)
  - SNMP
    - EngineID available
  - Diagnostics:
    - Cellular interface monitoring implemented
  - Web interface:
    - Cellular interface “AUX” renamed to “EXT”
    - Auto refresh option enabling periodic refresh of the Status fields added
    - Status screen section Alarms in last 7 days is now more condensed; Inactive alarms are displayed in different color scheme.
- Fixed bugs:
  - Cellular interface:
    - Status refresh issues fixed
    - Status PLMN readout fixed
  - Serial interface:
    - RS485 interface interrupt handling improved
  - Monitoring:
    - Management traffic monitoring issue fixed
    - Ethernet interface Rx/Tx indication fixed
    - Configuration of ETH ports monitoring fixed to handle Disabled ETH ports properly
  - Diagnostics:
    - Incorrect behavior of Statistic screen in specific occasions fixed
  - Web interface:
    - Web client behavior after receiving error responses improved
    - Order of data tables on Diagnostics > Statistics page fixed to be the same as their Enablers (on the upper part of the screen)
    - Diagnostic tools polling fixed (e.g. Monitoring, ICMP ping). Only first refresh was handled.
    - Remote access error response handling improved
    - Device > Unit > Time screen > Status info flickering fixed
    - Settings > Firewall > L3 > Input and Output – fixed Port value display when Other option is selected
    - Various layout fixes: button size, overflowing texts
  - System:
    - Boot sequence stability improved
- Known issues:

 

- If 1) the “AUX” Cellular interface was selected in *Babel* > *Network* > *Interface* or *OSPF* > *Network* > *Interface*, or
  2) in Firewall configuration the Cellular interface ”AUX” was selected manually using “Other” item in a List box (instead of selecting it directly from the List box items) → the FW upgrade causes configuration to be reverted to factory defaults.
  Workaround – Change the respective configuration item to other selection prior to FW upgrade. Revert the change back to “EXT” after the firmware upgrade. Renaming “AUX” to “EXT” is the cause of this issue.
- Direct firmware upgrade from the version 2.0.3.0 or lower is not possible.
  Workaround – Upgrade firmware to any version between 2.0.5.0. and 2.0.10.0 prior to upgrading to 2.0.13.0.
- Disabling HTTP protocol together with Ethernet configuration changes can lead to unit recovery restart
  Workaround - Split the configuration changes into 2 steps: First – disable the HTTP protocol and Commit changes. Second – make other requested configuration changes and Commit changes.
- Monitoring of the IPsec encrypted packets on the Cellular interface does not work correctly.
- Activating monitoring on a disabled ETH port leads to unit recovery restart.

## Release 2.0.10.0

2022-06-03

- Main component versions:
  - CNF version: 14
  - Web client version: 1.56.1
- Warning:
  - FW Version 2.x **is not over the air compatible** with the 1.x versions
- New features:
  - Interfaces - Cellular interface:
    - Link testing implemented
    - Profile switching implemented
    - SMS – Event notifications implemented
    - SMS – Read of Cellular status implemented
    - SMS – Statistics implemented
  - Security:
    - HTTP server configuration updated to increase security
    - TCP port numbers for management access (SSH, HTTP, HTTPS) can be altered to a non-standard port number
    - SSH and HTTP Management access services can be disabled
  - Default SSID of WiFi management access was modified
  - Unit overheated Event can now be used as a trigger for Hot standby to switch to a backup unit
  - Diagnostics:
    - Creation and download of configurable Diagnostics package to support advanced unit diagnostics implemented
  - Web interface:
    - Cellular interface screen – Link testing and Profile switching configuration implemented
    - Cellular interface AUX is renamed to EXT
    - SMS configuration and diagnostic screens implemented
    - Help files updated
    - Several card-type lists updated (e.g. QoS)
    - Ethernet configuration page was redesigned completely in order to better reflect the Network interfaces configuration hierarchy

        - Major error messages splash screens redesigned
        - Changes to commit screens visually improved
        - Table type lists including drag-and-drop sorting improved
        - Events on *Settings* > *Device* > *Events* screen are now sorted into groups. Advanced filtering to show only selected events was implemented.
        - Configuration of Hot standby switch Events moved to *Settings* > *Device* > *Events* screen
- Fixed bugs:
    - Serial protocols: Fine tuning of memory management
    - Cellular interface: Counter of failed PIN input attempts fixed
    - Hot standby
        - Range for virtual addresses parameter fixed
        - Occasional incorrect boot behavior fixed
    - Web interface:
        - Missing PSK key parameter was added to the IPsec configuration modal screen
        - File input field on *Settings* > *Device* > *Configuration* screen is reset after the file upload to give a better indication the file is uploaded
        - Various minor layout fixes
        - Various text label fixes
- Known issues:
    - Cellular interface statistics are deleted after FW upgrade
    - *Settings* > *Device* > *Unit* > *Hot standby* screen is not available via Remote access when accessing unit with an older FW version.
      Workaround: Use *Advanced* > *Device* > *Unit* > *Hot standby* screen
    - If the Management access ports are changed to non-default value, the Monitoring of ETH interface does not include Management traffic frames

## Release 2.0.8.0

2022-03-04

- Main component versions:
    - CNF version: 13
    - Web client version: 1.55.1
- Warning:
    - FW Version 2.x **is not over the air compatible** with the 1.x versions
    - Cellular interface configuration will be changed to default values after upgrade to this FW version
    - It is not possible to setup monitoring via Remote access when accessing unit with an older FW version
- New features:
    - Interfaces - Cellular interface:
        - Cellular module mPCIe-W support implemented
        - Configuration screen improvements
        - Statistics implemented
        - Signal strength indication implemented
    - Router: QoS is implemented
    - Routing: “Local preferred source” address option added to Static routing
    - Serial protocols - RDS protocol
        - No more bound to Radio address only
        - “Local response address” configuration option added
    - Radio channel: Radio interface is blocked when the extreme temperature is reached
    - SNMP:
        - All statistics data are now available via SNMP

 

        - Several unit information added (Unit note, configuration version, web client version, region id)
    - Diagnostics - additional Status information fields implemented
        - NAT status
        - Firewall L3 status
        - Firewall L2 status
    - Diagnostics: ETH interface monitoring extended to show L2 headers
    - Diagnostics: Enhanced export of statistics data to csv files – first line giving the column names is updated to provide more robust import to a spreadsheet
    - Monitoring: Enhanced export to an external file – missing records are indicated
    - Web interface: Unit “Mode” (Bridge/Router) parameter was moved from the Settings > Device > Unit menu to the Settings > Interfaces > Radio menu
    - Web interface - Status screen
        - Updated to show Events of severity Notice or higher
        - Disabled interfaces are not listed
        - Last refresh timestamp is available
    - Web interface: “Reset monitoring to defaults” implemented
    - Web interface: If the Sending new configuration fails due to an invalid configuration, the link to affected configuration page is given within the notification area error message
    - Web interface: Diagnostic > Information section providing detailed status information implemented
    - Web interface: Changes to commit records are sorted alphabetically
    - Web interface: Firmware Activate dialog improved with an Alert message
    - General: “System boot completed” Event can control “AO” output
    - General: It is now possible to restore unit configuration with the configuration backup of a different configuration version. Warning message is given in case the configuration file does not contain configuration version information.
- Fixed bugs:
    - SNMP: Incorrect read of the user role – fixed
    - Serial protocols: PR2000 memory leak – fixed
    - Cellular interface: Masquerade option fixed to work correctly with IPsec
    - Interfaces: COM1 port unwanted voltage level – fixed
    - Security: IPsec deadlock in certain circumstances when configured with IKEv2 – fixed
    - Diagnostics: Monitoring of Serial protocol Transparent – fixed
    - Diagnostics: Temporary lock of frequently called ICMP ping and RSS ping commands – fixed
    - Web interface: Missing IPsec configuration parameters on Settings > VPN > IPsec screen added
    - Web interface: Remove extra 0 shown when Radio Encryption is off
    - Web interface: Various minor layout fixes
- Known issues:
    - When upgrading from an older FW version the "Unrecoverable Error" message is raised at the end of the upgrade process.
      Workaround - Press the "Retry" button on the error message dialog. The firmware upgrade was finished correctly.

## Release 2.0.7.0

2021-11-26

- Main component versions:
    - CNF version: 12
    - Web client version: 1.54.0
- Warning:
    - FW Version 2.x **is not over the air compatible** with the 1.x versions
- New features:

  - Firewall: Source and Destination NAT (NAPT) is implemented offering rich possibilities of packet filtering and modification
  - Radio channel: Resiliency mode can now be configured also to manually selected value
  - Ethernet: ETH1-ETH4 disable option implemented
  - Ethernet: ETH1-ETH4 link speed and duplex configuration implemented
  - Ethernet: SFP port (ETH5) is disabled when not assigned to any Network interface
  - Ethernet: Ethernet link down event is blocked in case the Ethernet port is disabled
  - Ethernet: Detailed Ethernet Status is implemented
  - Ethernet: SFP module advanced information
  - Serial protocols: RDS protocol – Reverse mode was deprecated
  - Diagnostics: Realtime section of Status page was implemented
  - Diagnostics: Some of the RF Monitoring values are updated to show PEP values
  - Diagnostics: Unit HW status measurement implemented:
    - Input voltage; CPU, Modem board and Radio board temperature
    - Statistics extended to provide minimum, maximum and average values
    - Every value is monitored by a new system Event for Low and High threshold (i.e. 8 new Events)
  - Security: Password complexity check added – fully configurable to check: Min. length; Min. number of lowercase letters; Min. number of uppercase letters; Min. number of numbers; Min. number of special characters
  - Security: Password lockout implemented – login operations are progressively delayed after unsuccessful attempt to login
  - Web interface: Hot standby configuration screen hides events which cannot be used as a switch-over trigger because they are disabled (e.g. Eth port, Antenna detector)
  - Web interface: Configuration restore from file dialog check the backup configuration if it contains proper version of configuration data
  - Web interface: Improvements for better accessibility on small screens
  - Web interface: ICMP ping diagnostic tool extended by possibility to define a Source address
  - Web interface: L3 firewall extended by possibility to define interface name manually as an addition to pre-configured Input/Output interface names
  - Web interface: Firmware upgrade page was redesigned to provide better user experience especially when working with firmware patches
  - Web interface: Several group of Severity levels added to the Events screen to provide better filtering
- Fixed bugs:
  - Interfaces: Cellular module authentication failure leading to occasionally module deadlock – fixed
  - Serial protocols: Transparent protocol causing in special circumstances packet looping - fixed
  - Web interface: Impossibility to upgrade FW in a brand-new unit having FW 2.0.5.0 – fixed
  - Web interface: Monitoring – several minor issues fixed
  - Web interface: Maximum length of the user name was fixed to be the same for both user creation and for login
  - Web interface: If the Ethernet port is disabled, it is also detached from a Network interface now
  - Web interface: Device Menu is updated after connecting to another unit to reflect eventual HW configuration or SW key differences
  - Web interface: In the case the FW activation was not successful and the application was reconnected, the user is log out
  - Web interface: Notification center large screens issues fixed
  - Web interface: Static routing configuration page – Default gateway records behavior fixed
  - When the unit time is changed by 1 hour or more, the web server is blocked – fixed
  - Antenna detector minor fixes
- Known issues:
  - Firmware upgrade from the version 2.0.5.0 (or lower) to version 2.0.7.0 (or higher) can revert the unit configuration to Factory defaults. It might happen in case when some of the ETH ports (ETH1-5) are not assigned to any Network interface.

 

Workaround: Add all ETH ports to a Network interface prior to FW upgrade (ETH5 does not have to be added in case it is disabled). The configuration can be restored back to original status after the successful FW upgrade.

## Release 2.0.5.0

2021-08-27

- Main component versions:
  - CNF version: 11
  - Web client version: 1.53.1
- Warning:
  - FW Version 2.x **is not over the air compatible** with the 1.x versions
- New features:
  - Radio channel: Radio resilience extended by High sensitivity mode to improve operation with duplexer
  - Radio channel: Rx status LED operation mode is now configurable for better operation with duplexer
  - Routing: Default value of Destination mask changed to more convenient value (32)
  - Routing: Any routing rule can be configured as Persistent to prevent routing changes in case of disconnected Cellular interface
  - Serial protocols: COMLI protocol implemented for both COM and Terminal server interfaces
  - Serial protocols: Buffer flush timeout implemented to protect communication deadlock when a message is lost
  - Diagnostics: RSS ping, tool for radio link analysis, implemented
  - Diagnostics: Monitoring menu extended by Overview section to enable faster interaction
  - Diagnostics: Monitoring output can be stored as a file
  - Diagnostics: Monitoring output can be recorded to a file to provide reliable monitoring of Remote units connected over slow connection
  - Diagnostics: Amount of transferred monitoring data optimized to spare over the air bandwidth
  - Web interface: Changes to commit dialog major update:
    - Configuration changes are now grouped by configuration screens to provide better overview of configured changes
    - Links to a specific screen or screen-section are provided for each group of configured changes for faster access
    - Deleted records of configuration tables (e.g. deleted Static route) are displayed as a configuration change
  - Web interface: Communication between the unit web server and client web interface is now compressed to limit amount of transferred data
  - Web interface: Individual VLAN can now be configured as an input port of any Network interface (Ethernet bridge)
  - Web interface: VLAN configuration extended by a Note parameter
  - Web interface: Antenna detection status now displayed in better human readable format
  - Web interface: Firmware upload service updated to improve upload over slow connection and to improve FW patches upload
  - Web interface: “Enable SNMP trap for all” events button added
  - Web interface: Every tab on a specific screen can have individual Help file
  - Web interface: Configuration backup file now contains only raw configuration data to reduce the backup file size
  - Web interface: Several “card views” were updated to contain better set of displayed data (e.g. L3 firewall)
  - Web interface: Antenna detection and RF transmission test tools were moved to Diagnostics – Tools section

  - Web interface: Antenna detection layout and messages were improved
  - Web interface: Several compatibility specific messages improved and added for better user notification
  - Web interface: "… We recommend downloading current configuration file backup …" notification after FW upgrade was added
  - Web interface: Diagnostic tools ICMP ping and Routing provide a possibility to save their output to a text file
  - Web interface: File naming convention of the files downloaded from the web interface was updated to provide better readability
  - Web interface: Diagnostics – Events provide a pre-configured Severity filters to enable filtering by Info, Warning and Alarm groups of events
  - Web interface: Status page "Alarm in last 7 days" label and "Latest alarms" label were updated. "View more" buttons show all Events with Alarm severities.
  - Web interface: Remote access dialog provides a button to copy Remote unit connection URL to clipboard for user convenience (e.g. creating bookmark)
  - Web interface: Firmware update screen provides information of stored FW versions which can be used as a base for applying firmware patches (patches are of smaller file size compared to full FW file)
  - Web interface: Hot standby configuration extended by "Virtual radio MAC" parameter
  - General: New Regions added
- Fixed bugs:
  - Routing: OSPF protocol parameter Interface – Password: check of its presence fixed
  - VPN: Configuration of GRE L3 tunnel with MTU smaller than 1280 Bytes fixed
  - Serial protocols: UNI protocol parameter "Address translation" incorrect behavior during the protocol configuration fixed
  - Diagnostics: Several monitoring issues fixed
  - Diagnostics: ICMP ping tool minor fixes
  - Diagnostics: "Configuration lost" event is now cleared in a new unit
  - Web interface: Long User account names issues while connected via Remote access fixed
  - Web interface: Ethernet settings screen minor layout fixes
  - Web interface: "Status" component fixed to show loading state correctly
  - Web interface: Several "card views" layouts fixed
  - Web interface: Remote unit information is reloaded after FW upgrade to prevent a false Incompatible FW message
  - Web interface: Diagnostics – statistic multiple files download malfunction in case there are some empty tables fixed
  - Web interface: SW key related error messages fixed which appeared when a locked page (e.g. IPsec) was accessed before the Remote unit configuration was loaded
- Known issues:
  - Firmware downgrade to the version 1.3.4.0 will cause the station to malfunction.
    Workaround - downgrade to a different version first (e.g. 1.4.8.0) and to the 1.3.4.0 version afterwards. Note: firmware downgrade is NOT recommended.
  - When upgrading from a version 1.x the "Unrecoverable Error" message is raised at the end of the upgrade process.
    Workaround - Press the "Retry" button on the error message dialog. The firmware upgrade was finished correctly, there is only issue with the final success message delivery.
  - When upgrading from a version 2.0.3.0 or older, the error message is raised at the end of the upgrade process.
    Workaround – Reload the web page. The firmware upgrade was finished correctly, there is only issue with the final success message delivery.

 

- When the unit time is changed by 1 hour or more, the web server is blocked (management web interface is not operating). The time zone shift does not raise this problem. No other services of the unit are affected.
  Workaround – Restart the unit.

## Release 2.0.3.0

2021-05-28

- Main component versions:
  - CNF version: 10
  - Web client version: 1.45.1
- Warning:
  - FW Version 2.x **is not over the air compatible** with the 1.x versions
- New features:
  - Routing: Babel dynamic routing protocol (OSPF based) implemented
  - Routing: Dynamic routing rule capturing the cellular interface traffic can be set as persistent
  - Cellular interface: Status information extended
  - Cellular interface: Statistic counters implemented
  - Serial protocols: Mars-A protocol implemented for both COM and Terminal server interfaces
  - Serial protocols: SAIA S-BUS protocol implemented for both COM and Terminal server interfaces
  - Serial protocols: RDS protocol address translation extended to enable reverse protocol address to IP:port translation
  - Serial protocols: Protocol drivers improved to prevent unwanted frames concatenating or splitting
  - SNMP: User identification added to selected notifications
  - Diagnostics: Multicast frames counters are now also based on ETH type and IP protocol type
  - Diagnostics: Routing diagnostic tool available – returning the next hop interface for the given IP address
  - Diagnostics: Dynamic and Static routing - comprehensive status information available
  - Web interface: Allow unit management parameter added to Ethernet and Radio interface configuration screens
  - Web interface: VLAN configuration screen implemented
  - Web interface: Consistently display "–" for unavailable data in diagnostics and status display contexts
  - Web interface: URL extended to enable direct access to a Remote device
  - Web interface: RADIUS configuration screen implemented
  - Web interface: Messages having the severity level “Warning” are colored (blue) in Monitoring output
  - Web interface: Help files updated
  - General: New Regions added
- Fixed bugs:
  - Serial protocols: Short idle causing frames split - fixed
  - Diagnostics: Statistics standard deviation calculation - fixed
  - Web interface: Several Responsive design fixes (small screen resolution issues)
  - Web interface: Help files fonts loading - fixed
  - Web interface: Disable Interface field on GRE L2 page when the rest of the table is disabled
  - Web interface: Long file name input field overflow - fixed
  - Web interface: Long config tree items wrapping improved
- Known issues:
  - Firmware downgrade to the version 1.3.4.0 will cause the station to malfunction.
    Workaround - downgrade to a different version first (e.g. 1.4.8.0) and to the 1.3.4.0 version afterwards. Note: firmware downgrade is NOT recommended.

  - When upgrading from a version 1.x the "Unrecoverable Error" message is raised at the end of the upgrade process.
    Workaround - Press the "Retry" button on the error message dialog. The firmware upgrade was finished correctly, there is only issue with the final success message delivery.

## Release 2.0.1.0

2021-03-26

- Warning:
  - FW Version 2.0.1.0 is **not over the air** compatible with the previous versions (1.x)
- New features:
  - Radio channel: Flexible protocol implemented
  - SW keys: Implemented
  - Security: Embedded libraries updated
  - Security: IPsec IKE protocol's Diffie-Hellman group (PFS) was extended by new "X25519" and "X448" elliptic curves
  - Serial protocols: Additional protocols implemented: PR2000, S3964R
  - Serial protocols: RDS protocol was extended by Reverse protocol address translation option
  - Serial protocols: DF1 protocol was extended by Local acknowledge option
  - Serial protocols: UNI protocol was extended by "ASCII (2B)" address mode option
  - Serial protocols: Minor improvements (Broadcast address processing when Broadcasts are disabled; Corrupted frames processing; Protocol timeout safeguard when processing torn frames)
  - Events: HW outputs 'DO1' and 'DO2' can be triggered by unit Events
  - Events: Digital inputs 'DI1', 'DI2' and 'DI3' can trigger unit Event
  - Diagnostics: Statistics subsystem updated to keep stored data with all FW upgrades
  - Web interface: Modbus TCP and Modbus RTU protocols available in Settings menu
  - Web interface: Web page header Keyboard shortcuts implemented (Remote access, Changes to commit, Notification center)
  - Web interface: Establishing a connection to Remote unit is now indicated
  - Web interface: Warning sign occurs, when performing an action which leads to Remote access disconnection
  - Web interface: Reset button on the Events screen pre-fills the "Time until" field with the current time
  - Web interface: ETH5 (SFP) port "Active" configuration item was implemented
  - Web interface: Terminal server and COM ports Protocol address translation – Destination UDP port and name of the destination interface is now displayed
  - General: Region specific limitations are available (when ordering new units)
- Fixed bugs:
  - Radio channel: FEC algorithm was updated to suppress corruption of certain types of packet (this update leads to over the air incompatibility with the previous FW versions).
  - Serial protocols: IEC101 TELEGYR mode Broadcast processing – fixed
  - Serial protocols: Protocol address translation table – an inactive rule caused the subsequent rules not to be processed – fixed
  - SNMP: Data type of "sysApiLoginId" modified to correspond with MIB data type
  - Web interface: Several Responsive design fixes (small screen resolution issues)
  - Web interface: If the FW update failed, the Firmware web page did not work correctly
  - Web interface: Messages announcing a failed FW update were modified to be more informative
  - Web interface: Remote access "Local authentication" screen – remotely inactive actions are now disabled
  - Web interface: Long notification messages – delete button position fixed
  - Web interface: COM port Protocol address translation – "Note" printout fixed

 

## Release 1.4.8.0

2020-12-11

- New features:
  - Modbus RTU implemented for both COM and Terminal server interfaces
  - Modbus TCP implemented for Terminal server interface
  - Hot-standby operation extended by possibility to set up shared MAC address of the Radio interface
  - Ethernet Link down events implemented
  - SNMP provides information about Events status. MIB was updated
  - Web interface: Status page, providing overview of Major and Critical events in last 7 days, was implemented
  - Web interface: Remote access is indicated by a specific web browser tab icon (favicon)
  - Web interface: USB service access configuration screen implemented
  - Web interface: Radio channel encryption configuration added to Radio interface configuration screen
  - Web interface: Monitoring provides localized time stamps (….as well as the rest of the web interface)
  - Web interface: Old firmware version warning message is provided after establishing Remote access connection to a unit equipped with an older FW version
  - Web interface: Automatic logout is performed when the “Web inactivity timeout” expires
  - Web interface: Logged in user Role (access level) is displayed
- Fixed bugs:
  - If the unit is not equipped with a cellular module, Cellular interface is no more listed in the main menu
  - Event log notifications minor fixes
  - ETH5 (false) statistics count, when cable is disconnected (but the port remains connected to an eth bridge) - fixed
  - Common SNMP notification enable/disable configuration fixed
  - Ability to turn on SNMP “Inform” notification fixed
  - Monitoring minor fixes (fixed scrolling when longer period of signal is monitored; configuration window layout fixed; RDS protocol monitoring fixed)
  - BDP base station: FEC setting for the individual Remote stations fixed
- Known issues:
  - In some versions of web browser Vertical scrollbar fails to operate correctly from time to time
  - SNMP trap “Web interface login” has an incorrect data type

## Release 1.4.6.0

2020-10-23

- New features:
  - New event added: “Radio TX or antenna degraded” supervising radio part malfunction
  - Hot standby switchover also based on test “Radio TX or antenna degraded” event
  - Transmitter attack times for power up and down were shortened for the following channel spacings: 50, 100, 150, 200, 250, and 300 kHz
  - Radio interface monitoring: wider set of monitored values
  - Web interface: Status information added for the following modules – System information; Ethernet interfaces; Radio interface; Cellular interface; Static routing; IPsec
  - Web interface: Russian language support added
  - Web interface: Advanced menu UI improved
  - Web interface: Monitoring UI improved – ability to modify monitoring parameters when running; better readability of monitoring output

  - Web interface: Title bar indicates menu position and active Remote access connection
  - Web interface: Return to previous configuration page fast link added to the Changes to commit screen
  - Web interface: Hot standby configuration screen is now available
- Fixed bugs:
  - Radio interface Transparent protocol setup of Link address fixed. Monitoring and Statistics output are now correct
  - Several SNMP malfunctional settings fixed
  - Hot standby operation with unplugged ETH cable(s) fixed
  - Remote access connection minor fixes
- Known issues:
  - Cellular interface configuration is visible even if the HW module is not present
  - BDP base station: FEC setting for the individual Remote stations makes it possible to set unallowed values.
    Workaround – set up permitted values only (as listed in the User manual)
  - Shortening the transmitter attack time can cause protocol timing to be incompatible with the previous firmware versions

## Release 1.4.5.0

2020-08-28

- New features:
  - Multiple user accounts (4 levels of user privileges)
  - Factory settings and Total purge: delete all user accounts
  - RADIUS authentication
  - SNMP notifications (system Events)
  - SNMP: "System Group" MIB-II support enhancements
  - Differential statistics - based on counters custom reset
  - Expansion board ‘C’ providing 2×RS232 ports supported
  - Web interface: System events configuration screen
  - Web interface: Cellular interface configuration screen
  - Web interface: Tab header contains IP address of managed unit and menu position
  - Web interface: More Help screens available
- Fixed bugs:
  - RDS protocol memory allocation fixed
  - Ethernet interface monitoring - minor fixes
  - Statistics - Radio signal non-addressable statistics - Att2 value fixed
  - Web interface: SNMP notifications of Inform type are now blocked for SNMPv1
  - Web interface: input fields of ‘range of values’ type - validation fixed
  - Web interface: unit time input - validation of upper limit fixed
- Known issues:
  - Cellular interface configuration is visible even if the HW module is not present.
  - When upgrading from FW 1.4.1.0 or 1.4.3.0 - it is necessary to logout and login again to get a proper translation of web interface.

## Release 1.4.3.0

2020-06-26

- New features:
  - Time synchronization - NTP Server and Client

 

  - Service access via the USB port: USB/WiFi and USB/ETH adapters available; service address and DHCP range configurable
  - Serial protocols implemented: UNI and RDS
  - Diagnostics - Statistics: possibility to read the latest data
  - Monitoring: "ESP" protocol (used by IPsec) is now detected and listed
  - All the displays and inputs of time are now localized according to a configured Time zone
  - Web interface shows internal time of the connected RipEX unit
  - Web interface provides more detailed information after the Factory reset operation
  - COM and Terminal server interfaces configuration pages provide more detailed information (interface specific UDP port)
  - ETH interface configuration page provides status indicator (if the interface is enabled/disabled and attached/detached to a Network interface)
- Fixed bugs:
  - IEC101 protocol: proper handling of different configuration parameters respecting the usage of 8 bit or 16 bit addresses
  - COM interface: MRU settings fixed
  - Hot-standby: shared IP address proper handling after the ETH configuration changes
  - Hot-standby: active and passive units switch over fixed
  - Radio channel: fixed error multiplication when FEC is ON
  - Radio channel: proper operation, even when there is a very high level of signal strength (stronger than - 30 dBm)
  - Radio channel: Pre-frame signal measurement fixed
  - Web interface: Remote access IP address now displayed correctly
  - Web interface: When DF1 serial protocol is configured, the Table type of Address translation can be used
  - Web interface: Fixed behavior of time input fields on the Diagnostics - Statistics screen
  - Web interface: minor bug fixes
- Known issues:
  - When connected via Remote access: It is impossible to set up unit time if the remote FW version is 1.3.4.0 or older. It is impossible to display, but it is possible to set up unit time if the remote FW version is 1.3.6.0 or 1.4.1.0. There is not such an issue if the Remote unit FW is 1.4.2.0 (or newer).

## Release 1.4.1.0

2020-04-30

- Major features:
  - BGP dynamic routing protocol
  - OSPF dynamic routing protocol
  - ICMP ping via web interface
  - Longer history of statistics data
  - Hot standby improvements: HS virtual IP address can be set up as a source address; more types of Event log messages
  - Terminal server - persistent TCP connection option
  - Event log - export to external file option
  - Statistics data - export to external file option
  - Statistics data display - multiple improvements
  - Ethernet port monitoring extended by fragmented data monitoring option
  - Embedded security libraries updated
- Fixed bugs:
  - More Terminal servers can run simultaneously since this FW
  - ICMP messages generation on Ethernet bridge interfaces fixed (Linux kernel bug)

  - Several Diagnostics-Monitoring fixes
  - IEC101 protocol 'mask' type of address translation for 16 bit addresses fixed
  - DF1 protocol setup limited to 8 bit addresses (because DF1 protocol itself supports only 8 bit addresses)
  - IEC101 and DNP3: when using 'table' type of address translation, it is now possible to setup range of IP addresses
  - Event log display via Remote connection fixed
  - Manual setup of unit time fixed
  - Several web interface fixes
- Known issues:
  - Radio interface protocol timing was updated. There can be a problem with the backward compatibility in certain circumstances. If it happens, increasing the Maximal distance parameter (Advanced - Radio - Radio parameters - Maximal distance) in the whole network solves the problem.
  - Event log does not display correct Remote IP addresses in the case of remotely initiated events
  - If the COM port parameter MRU is setup to number 30 Bytes or lower, the unit might switch to Recovery mode
  - If the unit is operated in Hot standby mode and the Hot standby "Guard mode" is not used: in such a situation changing any of the Ethernet interface parameters leads to Hot standby Virtual address deactivation.
    Workaround: Enable the "Guard mode" protection

## Release 1.3.6.0

2019-12-20

- Major features:
  - GRE L2 and L3 tunnels
  - Diagnostics - ETH and Radio counters are also available
  - Diagnostics - detailed statistics for all interfaces
  - Manual setup and display of system time
  - Radio interface monitoring extended by advanced Receive signal quality and Transmit parameters information
  - IEC 101 protocol available on standard configuration screen
- Fixed bugs:
  - Router type of interfaces monitoring (Radio, COM, TS) has now correct (swapped) Rx/Tx labels
  - Hot-Standby operation fixed
- Known issues:
  - Unit statistics data are rather short (hours or days - depends on traffic load)
  - The ETH5 statistic counters are updated incorrectly in certain circumstances - counting up interconnected Network interface traffic, even if there is no active link in the ETH5 port

## Release 1.3.4.0

2019-12-20

- Warning:
  - Event system implementation causes partial incompatibility issues with the older FW versions. When upgrading to the new FW - it is necessary to start the upgrade process from the "distant" units first. The Base unit(s) needs to be upgraded last.
- Major features:
  - Event system implemented - handling internal unit events
  - HW output 'AO' can be triggered by unit events

 

  - Diagnostic system implemented - COM port and TS counters are available for now
  - Notification center implemented - handling user-unit interaction events
  - IEC 101 protocol implemented (Advanced menu configuration available only for now)
  - Remote access dialogues improved
  - Long parameters lists enhanced - card / table view switch implemented
  - Changes to commit icon enhanced - number of changes indicated
  - Default configuration can be loaded to GUI
  - ... and many minor improvements
- Fixed bugs:
  - Fix detach network interface function to remove all its descendants
  - Fix remote access dialog behaviour and appearance
  - ... and many minor fixes
- Known issues:
  - There may be some compatibility issues when communicating with the units having older FW and using BDP Radio protocol at very low speeds or over very long distances. Increasing the Maximal distance parameter (Advanced - Generic - Radio Channel - Maximal distance) might help in such a situation.
  - Should the unit be downgraded to this FW version, it is switched to Recovery status and needs to be re-configured manually

## Release 1.3.2.0

2019-11-13

- Major features:
  - Radio channel - Transparent protocol
  - Full duplex mode available (RF interface, Transparent protocol)
  - Ethernet traffic bridged to the RF interface (Bridge mode)
  - COM port - Transparent protocol
  - Default settings
  - Factory settings - available both from the web interface and the HW button
  - Total purge
  - Unit reboots when the HW button is pressed
  - Web interface configuration changes are validated to protect correct combinations of parameters
  - Firewall L2 configuration screen
- Fixed bugs:
  - Cellular module power supply fix
  - COM ports and Terminal servers: Protocol translation table displayed only if selected; Possibility to use interval of protocol addresses also via regular configuration screen
- Known issues:
  - When connected via Remote access the web interface seems to be disconnected from the Remote unit after applying the configuration changes or after Refresh settings.
    Workaround: connect to the Remote unit again to get clear connection status.

## Release 1.3.1.0

2019-10-04

- Major features:
  - Router mode
  - Base Driven Protocol
  - COM port and Terminal Server protocols: Async Link, DNP3, DF1

- Firewall L2 and L3
- Static routing
- Hot standby - basic support
- IPsec
- AES256 Encryption (Radio Channel)
- SNMPv2c, v3
- RF transmission test
- Monitoring
- Remote access (fast remote configuration)
- Cellular expansion board (2G/3G/4G available)