

Document class Release Note
Document ID 2NGA001052
Business Unit ABB Oy, Distribution Solutions
Page 1/6
Date 12.08.2021

Firmware update release 2.0.4 for 611 series IEC product version G protection relays

Scope

Firmware update release 2.0.4 is for the following 611 series protection relays:

- REF611
- REM611
- REB611
- REU611

To verify that the firmware update applies to the protection relay version, ensure that the last character of the order code on the label on top of the human-machine interface (HMI) match the corresponding character of the order code in Fig. 1.

REx611xxxxxxxxxxxG

Fig 1. Order code of the 611 series protection relays

To identify the current firmware revision of the 611 series protection relay, please refer to Fig. 2.

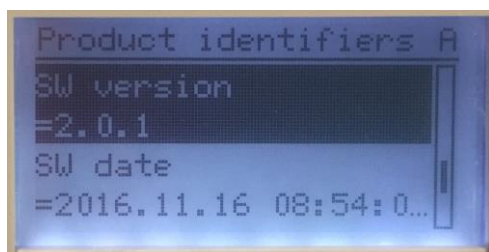


Fig. 2 Current firmware revision of the 611 series protection relay

Implemented usability improvements

The firmware update release includes usability and operational improvements. The following improvements have been implemented:¹

Firmware update release 2.0.4:

Cyber Security

- Cyber Security improvements to the "Ripple20" vulnerability in TCP/IP communication stack for normal product usage conditions. Following vulnerabilities has been identified in the product and fixed by the update:
 - CVE-2020-11907
 - CVE-2020-11909
 - CVE-2020-11910
 - CVE-2020-11911
 - CVE-2020-11912

Note! Some of the security scanners might still report existence of Ripple20 vulnerability after the update. This is a false positive, since the scanners indicate the presence of the IP stack, without being able to check the vulnerability and its fixes.

Supervision

- Improving Time counter rollover in relay's communication module that may have caused internal relay fault with error code *IRF116 COM card error* and relay to self-reboot after time interval(s) which is divisible by ~50 days from previous restart.
- Self-supervision recovery time improved in case of IRF Code 83 or 116 after 1 hour since previous.
- Improvement to watchdog supervision by optimizing timer clearance during parallel tasks.

Communication

- Improvement on GOOSE receiving. In a system where one relay is receiving GOOSE communication from multiple senders, it is possible that a communication break in one sender might impact handling of received values from other senders.
- Improvement to time synchronization in IEEE1588 PTP systems - improved handling of PTP configuration parameters.
- SNTP improvement to possible time synchronization interrupt alarms in HSR Ethernet topology.

¹ The relay firmware update may also include some minor usability improvements not listed in this note.

Date	12.08.2021
Page	3/6
Subject	Firmware update release

- Improving IEEE 1588 (PTPv2) Time synchronization when using non-zero (ID>0) PTP Domain ID. Enhancement at transparent clock peer-to-peer measurement and improving Path delay compensation. (Compensating delay for long communication cables).
- Internal time synchronization startup improvement.

HMI

- Improvements to LHMI firmware updating to prevent unwanted downgrade. Earlier it was possible that LHMI firmware updated in SW patch by FUT got downgraded when factory restore was done.

Firmware update release 2.0.3:

Communication

- Modbus communication bit SSR3 Bit 6 indicating device startup behavior improved.
- Limitation to the maximum number of files that can be opened by the MMS client. This improves the situation with certain types of MMS clients stressing the relay's filesystem and then causing the Internal Fault "File system error" (Fault code 7).
- Relay moving from Application mode to Bootloader mode improved for Ethernet communication.
- Improvement to the 1588 transparent clock message handling when the 1588 time synch source is not being selected but the Switch or HSR Ethernet topology is being used.
- Improved the SNTP time synchronization tolerance that is avoiding unwanted switching between primary and secondary time sync masters with less accurate time sync masters.
- Time synchronization performance improvement for less accurate time master setups causing unwanted Synch status up/down events.
- Improvement to the 1588 time synchronization master switch-over situation.
- Correction to the Modbus protocol initialization in cases where the Modbus is used together with the Profibus/SPA-ZC302. Correction prevents unexpected self-restarting of the relay in the situations where the Modbus is not first manually initialized by restarting the relay after Modbus is enabled.

Engineering

- Improved currents and voltages IEC 61850 data objects mapping to different data object levels

Protection

- Relay setting group change via SPCGGIO outputs control improved.

Protection

- Self-supervision recovery time improved in case of IRF Code 83 or 116.
- Self-supervision recovery handling improved in case of IRF Code 79.
- Internal diagnostic improvement for the self-supervision.

Firmware update release 2.0.2:

Control

- Improvement to autorecloser (DARREC) function operation with second autoreclosing sequence.

Communication

- Improvement to relay communication stack software to handle if IEC 61850 Edition 2 fixed length GOOSE messages is wrongly configured to the relay.
- Improved reporting of accumulated energy values from power and energy measurement function (PEMMXU).
- Improved status change event reporting of the Beh.stVal and Mod.stVal attributes.

Engineering

- It is now possible to set IP settings in IEC61850 Edition 1 mode with Parameter Setting Tool of PCM600.
- Improvement has been done in composition change indication function.

Protection

- Improvement to Intermittent earth-fault protection function (INTRPTEF) in "Intermittent EF" mode in case of very small earth fault current I_0 and high earth fault voltage U_0 .

HMI

- Improvement to WebHMI behaviour with continuous disturbance triggering condition.

Known limitations

If the PCM600 project is created by using 611 series Connectivity Package 2.0 then you must create a new PCM600 project with the (2.0.1 or later) Connectivity Package version. (latest version recommended) Please note that in this case GOOSE configuration has to be re-configured after the firmware update. The detailed instructions are available in the 611 series Firmware Update Guideline.

Date	12.08.2021
Page	6/6
Subject	Firmware update release

Update procedure

Firmware updates represent an integral part of ABB's life cycle management of distribution protection and control relays. The updates ensure optimized usability throughout the relay's entire life cycle by offering the latest improvements. The ideal time for a firmware update would be at device commissioning, during periodical testing or a maintenance break.

All 611 series IEC/CN version 2.0 (G) product deliveries manufactured later than August 12th 2021, include the stated relay firmware update 2.0.4. or newer.

Please note that ABB will not be liable for any direct or indirect costs related to the firmware update procedure. The update procedure shall be performed at the sole responsibility of the possessor of the installed base.