

Implemented usability improvements

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

Firmware update release 5.0.17:

Cyber Security

- Cyber security improvement
The following vulnerability (CVE, Common Vulnerabilities and Exposures) has been identified in the product and fixed by the update:
 - CVE-2021-22283: MMS file transfer vulnerability.

Additional details and mitigation methods can be found from mentioned (CVE, Common Vulnerabilities and Exposures) advisory.

- Cyber Security related update to webserver.

Supervision

- Improvements to *Load profile record LDPRLRC* function stability. Previously when using Load Profile Recorder it might have caused occasionally some self-supervision IRF indications (e.g. IRF2 & IRF82 seen).
- Improvement to self-supervision watchdog function, by enhanced task scheduling.
- Self-supervision indication adjustment. IRF Code 80 (RAM error) visible from HMI also after successful recovery reboot.
- RED615: Line Differential log file improvements.

Protection

- The improvement for the *Wattmetric-based earth-fault protection WPWDE* increases the function sensitivity in intermittent earth-faults when the fault has fault resistance > 100 Ohm.
- RED615: *Line differential protection with in-zone power transformer LNPLDF* weighted average 2nd harmonic calculation improvement.

Communication

- Improving MMS (IEC 61850) dual COTP connection requests handling.
- Improvements to status and quality reporting when binary input is oscillating.

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



Date 23.10.2023
Page 3/8
Subject Firmware update release

Firmware update release 5.0.16:

Protection

- RED615: *Line differential protection with in-zone power transformer LNPLDF* function sensitivity and stability improvement.

Firmware update release 5.0.15:

Cyber Security

- Cyber Security improvements to the "Ripple20" vulnerability in TCP/IP communication stack for normal product usage conditions. The following vulnerabilities have 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 improvement for composition detection.

Protection

- RED615: 2nd harmonic de-blocking condition improved in *Line differential protection with in-zone power transformer LNPLDF* function to use vector group matched, CT ratio corrected currents instead of directly measured primary currents. Using the directly measured primary currents may have caused the 2nd harmonic blocking to be deactivated too soon.

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.
- 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).

Firmware update release 5.0.14:

Communication

- Improvement to the Frequency measurement FMMXU avoids unnecessary reporting during momentary vector shift situations.
- Internal time synchronization startup improvement.
- SNTP improvement to possible time synchronization interrupt alarms in HSR Ethernet topology.
- Improvement enables the cyclic reporting of the unbalance currents from the Capacitor bank protection CUBPTOC and HCUBPTOC.

Engineering

- Minor correction on Bay name and Tooltip shown on WHMI

HMI

- Improvement to LHMI module firmware to avoid firmware downgrading in case of LHMI module change or factory restore.

Supervision

- Self-supervision performance improvement to the internal CPU memory supervision.
- Self-supervision recovery handling improved in case of LHMI, IRF Code 79.
- Self-supervision reset handling improvement.

Firmware update release 5.0.13:

Communication

- SNTP time synchronization performance improvement with time masters those are drifting approx. more than 200 ppm from the GPS time which could cause unwanted Synch status up/down events.
- Internal GOOSE performance improvement.
- Performance improvement for MMS file reading of certain file types.

Supervision

- Handling of the RTD card internal fault situation improved.
- Correction that avoids unexpected self-restarting of the relay during specific start-up situations.

Firmware update release 5.0.12:

Communication

- Improvement to the 1588 time synchronization master switch-over situation.
- Time synchronization performance improvement for less accurate time master setups causing unwanted Synch status up/down events.
- Improvement to DNP3, Modbus, IEC 103 protocols data value updating functionality regardless of the IEC 61850 dataset/report control block configuration in the relay.
- 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).
- 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.
- Time synchronization accuracy over the line differential communication improved.

Supervision

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

Firmware update release 5.0.11:

Control

- Improvement to the synchrocheck function for preventing unexpected short-period reset of SYNC_OK output. The reset could have been seen in vector shift situations earlier.

HMI

- Improvement to the local HMI reaction to very short and repetitive auxiliary power interruptions.
- Differential current values from the line differential protection LNPLDF are now recorded properly by the fault recorder.

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 communication performance in very rare and high communication load conditions.
- Improvement to IEC 61850 modelling of Open and Close command syntax to support substation automation systems giving these value with different syntax.
- Modbus event handling improved so that events are generated even if not present in any IEC 61850 data set.
- Improvement to the PhyHealth status value timestamp handling in the relay start-up situations.
- Improvement to current and voltage harmonics demand value reporting for IEC 61850 communication.

Protection

- The 2nd harmonic blocking takes into account the “CT ratio correction” setting in line differential protection LNPLDF.
- Improvement to the alarm output activation of the current total demand distortion CMHAI and voltage total harmonic distortion VMHAI in case of short duration disturbances.

Firmware update release 5.0.10:

Protection

- The angle accuracy has been corrected when the Rogowski current sensors are used.

Tools for updating the IED

Tools needed to update to SW version 5.0.17:

- PCM600 2.8 or later
- 615 Series Connectivity package 5.1.11 or later
- Relay Update file version 5.0.17
 - Example: REF**615**_IEC_Config_**A**_Version_**5.0.17**_2RCA032519S.bin
 - F refer to: Feeder protection and control REF615
 - 615 refer to: 615 product series
 - IEC refer to: International Standard
 - A refer to: Standard Configuration A
 - 5.0.17 refer to: Update file version 5.0.17

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.

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 devices.