Firmware update release 1.0.2 for SMU615 product version 1.0 Substation merging units

Scope

Firmware update release 1.0.2 is for the Substation merging unit SMU615

To verify that the firmware update applies to the merging unit version, ensure that the second and last two characters of the order code on the label on top of the human-machine interface (HMI) match the corresponding characters of the order code in Fig. 1.

SMU615xxxxxxxxxx1G

Fig 1. Order code of the SMU615 merging unit

To identify the current firmware revision of the SMU615 Substation merging unit, please refer to Fig. 2.

Parameter Name	IED Value
Type	SMU615
Product version	1.0
Serial number	1VHR91479539
Order code	SMU6151BBBBA1NN21G
Production date	2019.06.18 00:00:00:000
Configuration name	SE04
SW version	1.0
SW date	2017.08.25 16:42:00:000
SW number	2RCA039241A
HW revision	G

Fig. 2 Current firmware revision of the SMU615 Substation merging unit

Implemented usability improvements

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

Firmware update release 1.0.2:

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.

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

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

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).

- Improvement to time synchronization in IEEE1588 PTP systems - improved handling of PTP configuration parameters.

---

[1] The merging unit firmware update may also include some minor usability improvements not listed in this note.

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.

- Improvement enables generic control point SPCGAPC data preservation during a watchdog reset.

- Improvement to watchdog supervision by optimizing timer clearance during parallel tasks.

- Multiple improvements to relay self-supervision.
  - Improvements areas including, but not limited to
    - fault self-recovery improvements and harmonization
    - fast self-recoveries
    - HMI indications
    - RAM & EEPROM supervision improvements
    - composition detection improvement

  More information and details are found in the latest product Technical Manual under chapter Self-supervision.

Engineering

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

- Analog and sensor input Angle correction range change. Current and voltage angle correction factors setting range has been adjusted to -8.0000...8.0000 degrees.

Firmware update release 1.0.1:

Communication

- Improvement to the 1588 time synchronization master switch-over situation.
- 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.
- 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 merging unit's filesystem and then causing the Internal Fault "File system error" (Fault code 7).
- Merging unit moving from Application mode to Bootloader mode improved for Ethernet communication.

Supervision

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

Tools for updating the IED

Tools needed to update to SW version 1.0.2
- PCM600 2.8 or newer
- SMU615 Connectivity package 1.0.2 or newer
- SMU615 Update file version 1.0.2.
  - Example: **SMU615_IEC**_Config_615_Version_**A_1.0.2**_2RCA037411C.bin

    SMU615 refer to: Substation merging unit SMU615
    IEC   refer to: International Standard
    A   refer to: Application Configuration A
    1.0.2   refer to: Update file version 1.0.2

Update procedure

Firmware updates represent an integral part of ABB's life cycle management of distribution protection devices and merging units. The updates ensure optimized usability throughout the 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 SMU615 version 1.0 (1G) products manufactured later than 30th August, 2022 include the stated merging unit firmware update 1.0.2 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 devices.