Firmware update release 1.2.2 for REX640 control and protection relay

Scope

This update release 1.2.2 concerns all REX640 protection relays and LHMIs delivered from the factory earlier than 27th of June 2022.

To verify whether the update applies to the protection relay at hand, there are two things to check:

1. Product Connectivity Level shall be three (PCL3). This information can be checked from LHMI, WHMI or from the product label. The PCL is a part of product composition code, as the example below shows.

   REX640B10Nx + xxxx + COMx + PSMx + BIOx + **PCL3**

2. Relay firmware version is 1.2 or 1.2.1 This can be checked from LHMI or from WHMI.

Following figures show how to locate the above-mentioned information from the LHMI Device Information page and from the WHMI Product Identifiers page. The LHMI Device Information page can be accessed by tapping the menu bar on upper part of the LHMI screen and locating the Device Information button from the lower left-hand corner of the screen. The relay Firmware version is referred as "SW version". The "PCL" part of the composition code is pointed out as well.
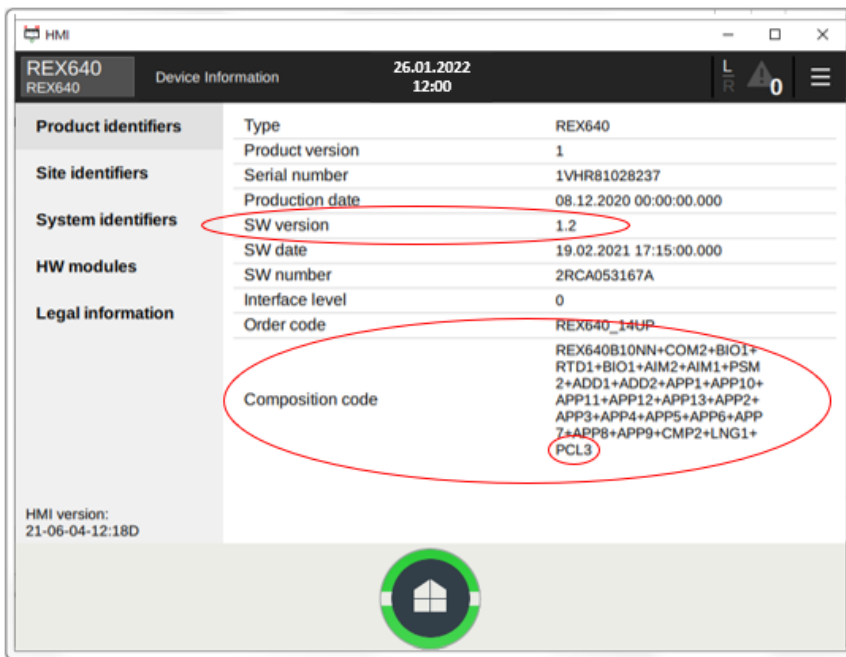
Fig 1. LHMI Device Information page
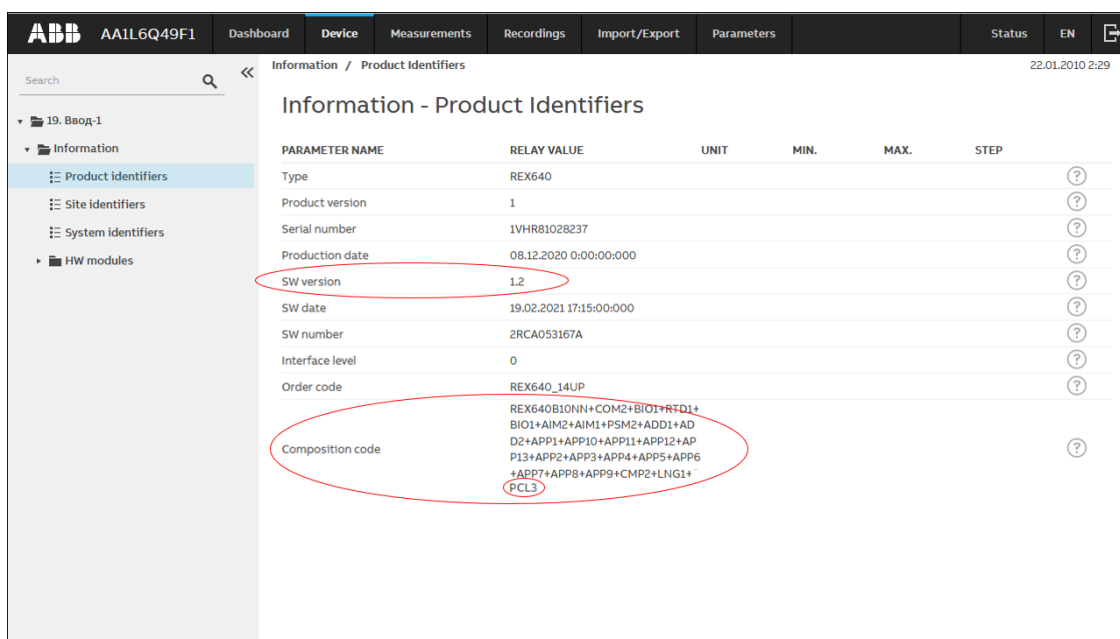
Fig 2. WHMI Product Identifiers page

Implemented usability improvements

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

Firmware update release 1.2.2 for relay

Protection

- *Autosynchronizer for generator breaker ASGCSYN* function operation has been improved to allow generator circuit breaker close command activation also in cases where the generator and the network are running in phase and with zero, or close to zero, frequency difference. This enhancement concerns cases where ASGSYN function parameter "Synchronization Dir" is having value "2=Both direction".

---

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

Firmware update release 1.2.1 for relay

Cyber Security

- Cyber security improvements
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.

- Also other Cyber Security related updates.Improvement areas including, but not limited to
  - Cryptography library
  - Webserver

Communication

- Improvement in IEC104 secure authentication mode. IEC104 spontaneous event sending does not get interrupted by erroneous SCADA control+key exchange sequence.

- Improving communication error handling in case of SFP transceiver is unplugged while Line Differential communication is in use.

- Improvement to IEEE 1588 PTPv2 Time synchronization Timesource field indications fixed. Before relay announced PTPv2 TimeSource=GPS if the relay was previously synced to a GNSS/GPS grandmaster, even GPS connection was lost. Now the REX640 ordinary clock was modified to announce TimeSource=Internal Oscillator accordingly regardless of previous state.

- Enhancements to IEEE 1588 PTPv2 Time synchronization to expedite master negotiation process.

Supervision

- Improving supervision and handling of PKI certificate renewal.

- User Account Management (UAM) enhancements.
- Custom UAM Roles and Rights changes from PCM600 does not require relay restart anymore to become activated.
- Preventing firmware updates with operator credentials from PCM600 Firmware Update Tool.
- Improvements to password change via LHMI & WHMI.

- Improvement to relay self-supervision to mitigate rare occurrence of Card error, slot A2 (IRF code -42) during relay startup situation. Possible occurrence has been limited to certain communication card types only (listed below).

  Communication card type and revision in use can be verified e.g., from REX640 LHMI or WHMI. Menu --> Device/Information/HW modules/x000 (COM)
          Check Article number and HW revision

  List of COM cards that can be updated by normal FUT update process:
Article number	HW revision
2RCA034478A0001	F, G
2RCA034478A0901	F, G
2RCA034483A0001	F, G
2RCA034483A0901	F, G
2RCA034488A0001	F, G
2RCA034488A0901	F, G
2RCA034493A0001	E, F
2RCA034493A0901	E, F
2RCA034497A0001	E, F
2RCA034497A0901	E, F

  List of COM cards that need update by process requiring factory support and tools: Please contact your local ABB representative for further guidance. Technical support is available for all ABB employees at: https://abb.custhelp.com
Article number	HW revision
2RCA034478A0001	H, J
2RCA034478A0901	H, J
2RCA034483A0001	H, J
2RCA034483A0901	H, J
2RCA034488A0001	H, J
2RCA034488A0901	H, J
2RCA034493A0001	G, H
2RCA034493A0901	G, H
2RCA034497A0001	G, H
2RCA034497A0901	G, H

  All other types of communication cards and revisions are not affected by this issue.

HMI

- Enhancing Web Human-Machine interface (WHMI) stability. WHMI server stability improvement by limiting parallel web server sessions.

- Language fallback support for WHMI. When any other languge than English in use and translation for certain word(s) is missing, WHMI utilize english default text instead of indicating "String Not Found".

Protection

- *Line differential protection with in-zone power transformer LNPLDF*, improving CT connection type 2 measurement buffer handling and such stabilizing LNPLDF operation.

- *Three-phase underexcitation protection UEXPDIS* function timer reset improvement. In switch onto fault situation, it could been possible that operate delay time not fully waited, when Definite Time (DT) mode selected.

- Enhancement to *Three-phase voltage-dependent overcurrent protection PHPVOC*. Earlier there has been narrow current range where PHPVOC start could have resetted incorrectly and such affecting function operation.

- *Autosynchronizer for generator breaker ASGCSYN*. Interaction between bypass and GCB_TEST inputs has been aligned with the description in the technical manual.

- *High-impedance fault detection PHIZ* function operation and stability has been enhanced.

- *Stabilized and instantaneous differential protection for two winding transformers TR2PTDF* function Improvement to waveform and 2nd harmonics blocking/de-blocking.

- Improvements on *Stabilized and instantaneous differential protection for two or three-winding transformers TR3PTDF* function CT ratio correction in current group 3.

- *Stabilized and instantaneous differential protection for machines MPDIF* improvement to CT ratio correction handling. Now also Sample Based MPDIF calulation can take account CT ratio correction.

- Improvement to all overcurrent and earth fault protection functions with user programmable or UK rectifier operating curve types. (IDMT operating curve types.) There has been very narrow operate range where very low overshoot above the protection functions set starting value, which could cause immediate operation, instead of delayed operation as per mentioned user programmable or UK rectifier curves delay times.

Tools for updating the REX640 (PCL3) relay

Tools needed to update to SW version 1.2.2:
- PCM600 2.10 (Hotfix 20201215) or later
- REX640 Connectivity package 1.2.1 or later
- Relay Update file version 1.2.2 (REX640_ALL_Config_640_Version_1.2.2_2RCA053167C.cab)

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 during a maintenance break.

All REX640 (PCL3) relays and LHMI product deliveries manufactured later than 27th of June 2022, include the stated relay firmware update 1.2.2 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.

Glossary

Abbreviations and acronyms are spelled out in the glossary. The glossary also contains definitions of important terms.

CT	Current transformer
CVE	Common Vulnerabilities and Exposures
FW	Firmware
HMI	Human-machine interface
HW	Hardware
IEC103	1. Communication standard for protective equipment
	2. A serial master/slave protocol for point-to-point communication
IDMT	Inverse definite minimum time
LHMI	Local human-machine interface
MMS	Manufacturing message specification
PCL	Product Connectivity Level
PCM600	Protection and Control IED Manager – Software
PKI	Public Key Infrastructure
SCADA	Supervision, control and data acquisition
SFP	Small Form-factor Pluggable - transceiver
SW	Software
UAM	User Account Management
WHMI	Web human-machine interface