Document class	Release Note
Document ID	2NGA001406
Business Unit	ABB Oy, Distribution Solutions
Page	1/10
Date	30.05.2022

Firmware update release 1.1.4 for REX640 control and protection

Scope

This update release 1.1.4 concerns all REX640 (PCL2) protection relay and LHMI deliveries from the factory manufactured earlier than 30th of May 2022.

To verify whether the update applies to the protection relay and the LHMI version at hand, there are three things to check:

1. Product Connectivity Level shall be two (PCL2). 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 + **PCL2**

2. Relay Firmware version is 1.1, 1.1.1, 1.1.2 or 1.1.3 This can be checked from LHMI or from WHMI

3. LHMI application version is dated **earlier than** 20-05-27-08:27. This can be checked from LHMI only.

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” and the LHMI application version is referred as “HMI version”. The “PCL” part of the composition code is pointed out as well.

ABB Oy
Distribution Solutions
P.O. Box 699
FI-65101 Vaasa
FINLAND

Visiting Address
Strömberg Park,
Muottitie 2 A
FI-65320 Vaasa
FINLAND

Phone: +358 10 2211
Fax: +358 1022 41599
e-mail:
first name.last name
@fi.abb.com

Business identity code:
0763403-0
Domicile: Helsinki
www.abb.fi

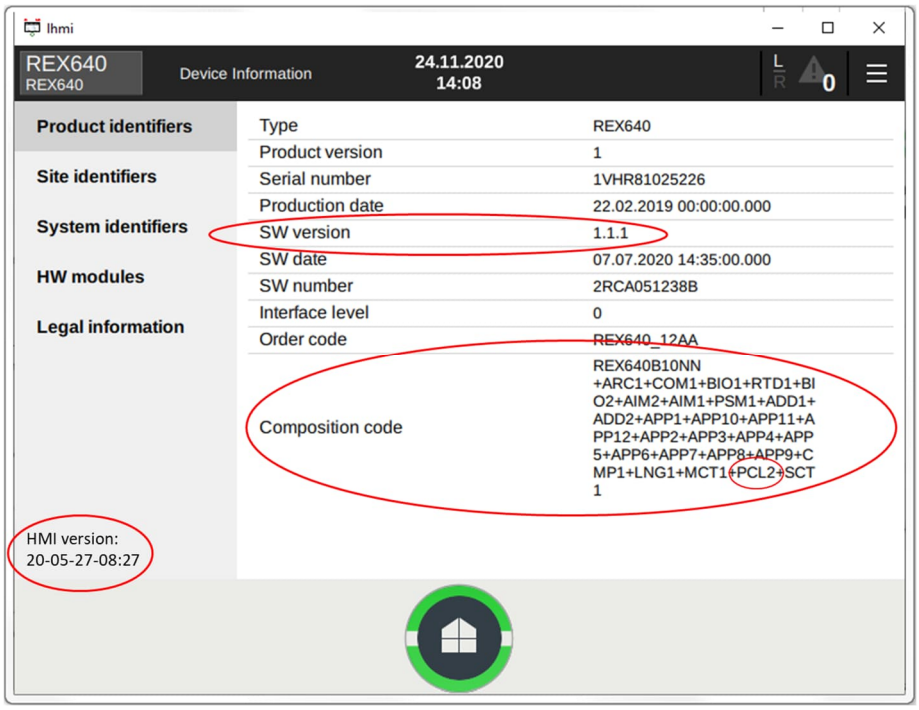

Fig 1. LHMI Device Information page

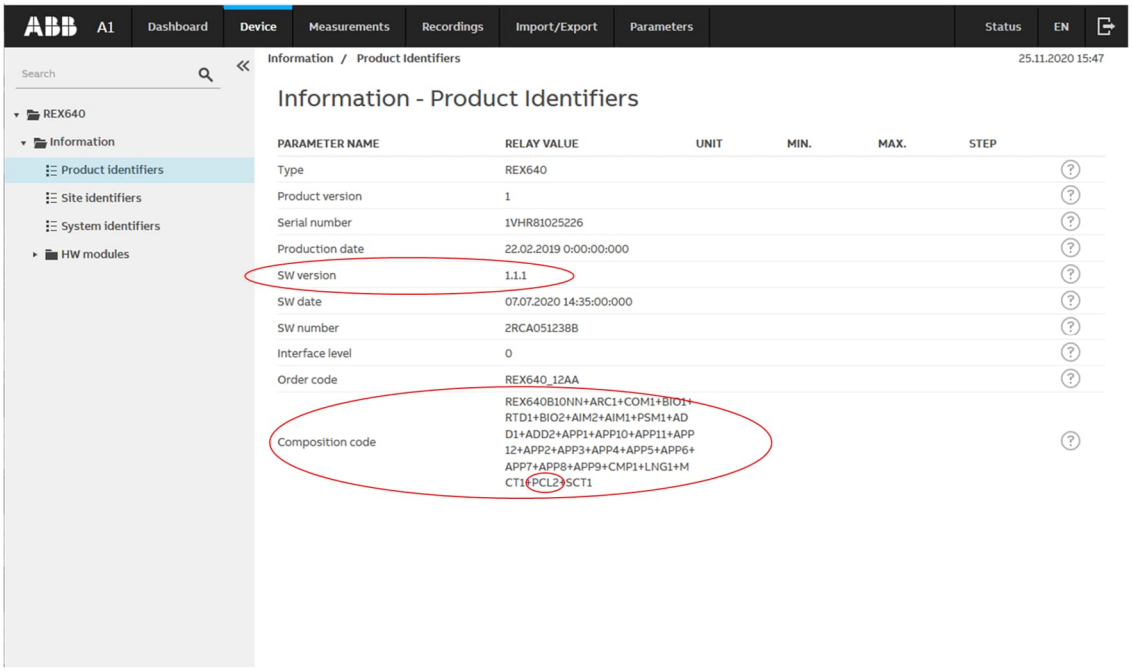

Fig 2. WHMI Product Identifiers page

Implemented usability improvements

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

Firmware update release 1.1.4 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.
  - CVE-2022-1596: Insufficient file access control.

  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 IEC 60870-5-104 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.

- Improved robustness on functionality when disconnecting IEC 60870-5-104 communication.

- 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 regardless of previous state.

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

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

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.

- 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.

Supervision

- Improving supervision and handling of PKI certificate renewal.

- User Account Management (UAM) enhancements.
  - Updates to default user Roles and rights.
  Note: Activating updated default role changes requires relay factory restore or restoring the user accounts from PCM600 after update, and then custom roles and rights can be written again (Customer configuration) to relay.
  - 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.

Firmware update release 1.1.3 for relay

HMI

- LHMI performance improvement.
  Earlier LHMI might have acted slow under some heavy configurations.

Supervision

- Fixing performance issue leading to reccurring IRF116 at certain HSR and PRP network systems.
  At some HSR and PRP network systems it has been possible to experience recurring IRF116 (WD2) COM card error leading to relay self-recovery reboot.
  (Impacted FW 1.0.5 & 1.0.6.)

Communication

- Improved SFP module handling and reporting.
  (SFP Module related to Line Differential and Line Distance applications.)

- Improving secure communication stability at IEC104 and DNP3 (TLS or Application authentication enabled). Earlier there had been marginal change for Watchdog error WD10 self recovery restart at some network systems where secure communication in use at IEC104 or DNP3 protocols.

Firmware update release 1.1.2 for relay

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.

- Enhancing relay restart process from Supply voltage breaks.
  In case of Supply voltage break, on rare occasions, relay was restarting to fault (EEPROM error on slot A2) and indicating "Card error, slot A2" at Event list.

HMI

- Improvements in WebHMI to better support Google Chrome 83 & 84 new security features. previously issues was seen at least with relay settings import and login.

- Improving WebHMI access via X0/HMI port after cable disconnection.

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.

Engineering

- Improving Special Character < > & handling at User Defined Names (UDN) and alarm texts. Which earlier may have caused relay program error and preventing successful relay restart.

Firmware update release 1.1.1 for relay and LHMI application version dated 20-05-27-08:27

Supervision

- Enhancing PKI certificate handling performance and stability. Previously may have sometimes lead to memory handling issue causing watchdog reset.

- Improving security event reporting. Implementing security events both to Event Viewer Tool (EVT) and syslog when PKI certificate created or renewed.

HMI

- Enhancing LocalHMI “testing and commissioning / Secondary injection Monitoring” page function “ON/OFF” restoration while switching from Test mode to Normal mode. When returning to normal mode operation without turning temporarily deactivated function(s) back to “ON” under test mode, some function(s) have remained “OFF” instead restoring automatically its original “ON”-state.

- GOOSE and SMV Sending pages on LocalHMI might have been showing incorrect receiver names when Flexible Product Naming (FPN) used.

- Removing unnecessary repetitive “Viewed Security Event logs Succesfully” Syslog messages seen at Report Summary page when using WebHMI.

- LocalHMI update process improvements. LHMI Software update, including Modification Sales update, may have sometimes failed by timeout.

Time Synchronization

- Improving SNTP Time synchronization server switch from primary to secondary server.

- GNRLLTMS ALARM signal was not activated simultaneously with WARNING signal in case primary SNTP server lost and secondary server was disabled.

Tools for updating the REX640 (PCL2) relay

Tools needed to update to SW version 1.1.4:

- PCM600 2.10 (Hotfix 20201215) or later
- REX640 Connectivity package 1.2.1 or later
- Relay Update file version 1.1.4 (REX640_ALL_Config_640_Version_1.1.4_2RCA051238E.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 (PCL2) relays and LHMI product deliveries manufactured later than 30th of May 2022, include the stated relay firmware update 1.1.4 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 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
DT	Definite Time
EEPROM	Electrically erasable programmable read-only memory
EVT	Event Viewer Tool
FPN	Flexible Product Naming
FUT	Firmware Update Tool
FW	Firmware
GNSS	Global navigation satellite systems
GOOSE	Generic Object-Oriented Substation Event
GPS	Global Positioning System
HMI	Human-machine interface
HW	Hardware
IDMT	Inverse definite minimum time
IEC104	IEC 60870-5-104 communication protocol
IEEE 1588	Standard for a Precision Clock Synchronization Protocol for networked measurement and control systems
IP	Internet Protocol
IRF	1. Internal fault 2. Internal relay fault"
LHMI	Local human-machine interface
MMS	Manufacturing message specification
PCL	Product Connectivity Level
PCM600	Protection and Control IED Manager – Software
PKI	Public Key Infrastructure
PTP	Precision Time Protocol
SCADA	Supervision, control and data acquisition
SFP	Small Form-factor Pluggable - transceiver
SMV	Sampled measured values
SNTP	Simple Network Time Protocol
SW	Software
TCP/IP	Transmission Control Protocol / Internet Protocol
UAM	User Account Management
UDN	User Defined Names
WHMI	Web human-machine interface