

RELION® PROTECTION AND CONTROL

# REX640

## Declaration of Security Conformance



# Table of Contents

<b>Table of Contents</b> .....	<b>1</b>
<b>1 About this manual</b> .....	<b>3</b>
1.1 Read it first! .....	3
1.2 Document information .....	3
1.3 Safety Information .....	3
<b>2 Abbreviations</b> .....	<b>5</b>
2.1 Abbreviations .....	5
<b>3 Applicable standards</b> .....	<b>7</b>

# 1 About this manual

## 1.1 Read it first!

Before attempting any operation with IED from REX640, read carefully the REX640 user documentation, especially the REX640 cybersecurity deployment guideline.

This document is addressed to anyone who needs to interact with REX640 and its IEC 62443 4-2 features in more detail.

## 1.2 Document information

### Revision History

Revision	Date	Note/Version Information
A	13 Oct 2025	REX640 Product version: 2.0

### Applicability

This manual is applicable to all REX640 Protection and Control IED versions mentioned in document Revision History above or newer versions if document update is not required.

## 1.3 Safety Information

There are safety warnings and notes in the following text. They are in a different format to distinguish them from normal text.

### Safety warning

The safety warnings should always be observed. Non-observance can result in death, personal injury or substantial damages to property. Guarantee claims might not be accepted when safety warnings are not respected. They look like below:



**Do not make any changes to the REX640 configuration unless you are familiar with the REX640 and its configuration tool. This might result in dis-operation and loss of warranty.**

**Note**

A note contains additional information worth noting in the specific context, and looks like below:



The selection of this control mode requires caution because operations are allowed both from the HMI and remotely.

## 2 Abbreviations

### 2.1 Abbreviations

<b>DHE</b>	Diffie–Hellman Ephemeral (a key exchange method that provides perfect forward secrecy using temporary keys)
<b>DNP3</b>	Distributed Network Protocol version 3 (used in SCADA systems for communication between devices)
<b>ECDHE</b>	Elliptic Curve Diffie–Hellman Ephemeral (a key exchange protocol using elliptic curve cryptography for perfect forward secrecy)
<b>FTP</b>	File Transfer Protocol
<b>FTPS</b>	File Transfer Protocol Secure
<b>GOOSE</b>	Generic Object-Oriented Substation Event
<b>GPS</b>	Global Positioning System
<b>HMI</b>	Human Machine Interface
<b>HSR</b>	High-availability Seamless Redundancy
<b>IEC 104</b>	IEC 60870-5-104 (protocol for telecontrol in electrical engineering and automation)
<b>IEC 61850</b>	International Electrotechnical Commission standard 61850 (for communication networks and systems in substations)
<b>IED</b>	Intelligent Electronic Device
<b>JTAG</b>	Joint Test Action Group (standard for testing and debugging integrated circuits)
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>MMS</b>	Manufacturing Message Specification
<b>Modbus</b>	A communication protocol for industrial automation systems
<b>PRP</b>	Parallel Redundancy Protocol
<b>PTP</b>	Precision Time Protocol
<b>RSA</b>	Rivest–Shamir–Adleman (a public-key cryptosystem used for secure data transmission)

<b>SCADA</b>	Supervision, Control and Data Acquisition
<b>SIEM</b>	Security Information and Event Management
<b>SMV</b>	Sampled Measured Values
<b>SNTP</b>	Simple Network Time Protocol

### 3 Applicable standards

Cyber security issues have been the subject of standardization initiatives by ISA, IEEE, or IEC for some time and ABB plays an active role in all these organizations, helping to define and implement cyber security standards for power and industrial control systems.

Some of the cyber security standards which are most important for substation automation are still under active development such as IEC 62351 and IEC 62443 (former ISA S99). ABB is participating in development by delegating subject matter experts to the committee working on the respective standard. Since these standards are still under development ABB strongly recommends using existing common security measures and best practices as available on the market, for example, VPN for secure Ethernet Communication.

An overview of applicable security standards and their status is shown in Table 1.

**Table 1. Overview of cyber security standards**

Standard	Description	Status
NERC CIP v5	NERC CIP cyber security regulation for North American power utilities	Released, ongoing
IEC 62351	Data and communications security	Released
IEC 62443-4-2	The standard IEC 62443-4-2 Security is for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components.	Released
IEEE 1686	IEEE standard for substation intelligent electronic devices (IEDs) cyber security capabilities	Released

ABB has identified cyber security as a key requirement and has developed many product features to support international cyber security standards and publications such as NERC-CIP, IEEE1686, as well as local activities like the German BDEW white paper.

This chapter contains a compliance statement of the REX640 2.0 series security functionality against the standard IEC 62443-4-2 Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components.

640 series devices are considered as embedded devices, so "Embedded device requirements" have been selected.

Following requirement selections from the standard are not considered:

- Host device requirements
- Network device requirements
- Software Application Requirements

**Table 2. Annex 1- IEC 62443 4-2 Security Conformance Declaration**

ID	Requirement	SL1	SL2	SL3	SL4	Implemented in-REX640
CR 1.1	Human user identification and authentication	Yes	Yes	Yes	Yes	<p>REX640 supports identification and authentication using usernames and passwords for both local and centralized account management.</p> <p>It implements role-based access control as defined by IEC 62351-8, ensuring that user access is restricted based on their specific roles and responsibilities</p> <p>To access the Engineering tool (PCM600), WebHMI, or the Local HMI, the user's name, password, and relevant role must be provided.</p>
CR 1.1 RE (1)	Unique identification and authentication	Not Applicable for SL1	Yes	Yes	Yes	<p>REX640 supports unique identification and authentication, ensuring that each user is individually identified, and their identity is verified before accessing the system through centralized or local account management.</p> <p>REX640 can accommodate up to 50 user accounts, with 20 distinct roles, and each role can be assigned up to 10 permissions.</p>
CR 1.1 RE (2)	Multifactor authentication for all interfaces	Not Applicable for SL1	Not Applicable for SL2	No	No	<p>Multifactor authentication can be achieved in central account management, where AD server is configured to handle authentication.</p>

CR 1.2	Software process and device identification and authentication	Not Applicable for SL1	Yes	Yes	Yes	<p>REX640 supports X.509 certificates in the following scenarios for enhanced security:</p> <p><b>Server Authentication for Web HMI:</b> X.509 certificates are used to authenticate the Web HMI server, ensuring that the connection between the user's browser and the Web HMI interface is secure and trusted.</p> <p><b>PC-Based Engineering with PCM600:</b> Certificate based authentication is utilized between the PC (running PCM600) and REX640, providing a secure method for verifying the identity of the device during engineering operations.</p> <p><b>Note:</b> Modbus, SNTP, GOOSE, Sample measured value protocols do not support identification and authentication. Hence, the system-level countermeasures are required to protect these non-secured protocols.</p>
--------	---	------------------------	-----	-----	-----	--

ID	Requirement	SL1	SL2	SL3	SL4	Implemented in-REX640
CR 1.2 RE (1)	Unique identification and authentication	Not Applicable for SL1	Yes	Yes	Yes	<p>REX640 authenticates users through centralized account management using unique usernames and passwords. For device authentication and identification, it utilizes unique certificates, ensuring secure and reliable access control.</p> <p><b>Note:</b> Identification and authentication not supported: Modbus, SNTP, PTP, GOOSE, SMV. Hence, the system-level countermeasures are required to protect these non-secured protocols.</p>
CR 1.3	Account management	Yes	Yes	Yes	Yes	<p>In REX640, both local and central account management involves creating, maintaining, and controlling user accounts within the system. This includes processes such as user creation, password management, assigning roles and permissions based on the user's responsibilities (Ex: engineer, operator, and administrator), and deactivating or deleting accounts when they are no longer needed. These features ensure that only authorized users have access to the relay, with permissions tailored to their specific roles.</p>
CR 1.4	Identifier management	Yes	Yes	Yes	Yes	<p>In REX640, both Local and central identifier management refers to the process of managing unique identifiers assigned to users within the system. This includes assigning usernames or user IDs during account creation, ensuring that each identifier is unique and correctly linked to the appropriate user.</p>

CR 1.5	Authenticator management	Yes	Yes	Yes	Yes	<p>Default usernames and passwords are provided in the documentation. Users must change these default credentials on the relay, as the relay does not automatically enforce a change.</p> <p>Periodic updates to usernames and passwords can be managed through centralized account management. Passwords are not stored in plain text but are hashed using a secure algorithm.</p> <p>When credentials are transferred to Active Directory via LDAP, the information is encrypted and not visible to users.</p>
CR 1.5 RE (1)	Hardware security for authenticators	Not Applicable for SL1	Not Applicable for SL2	No	No	This requirement is not Implemented

ID	Requirement	SL1	SL2	SL3	SL4	Implemented in-REX640
CR 1.6	Wireless access management	Not Applicable	Not Applicable	Not Applicable	Not Applicable	This requirement is not applicable for the Protection relay
NDR 1.6	Wireless access management	Not Applicable	Not Applicable	Not Applicable	Not Applicable	This requirement is not applicable for the Protection relay
NDR 1.6 RE (1)	Unique identification and authentication	Not Applicable	Not Applicable	Not Applicable	Not Applicable	This requirement is not applicable for the Protection relay
CR 1.7	Strength of password-based authentication	Yes	Yes	Yes	Yes	REX640 supports passwords with a maximum length of 20 characters and a minimum length of 6 characters. To strengthen security, REX640 allows passwords to include a combination of numbers, letters, and special characters. Password policies can be configured directly on the protection relay if local account management is used and furthermore, the passwords undergo hashing, making them non-reversible, before being securely stored in a database system for centralized account management, passwords are managed through Active Directory.
CR 1.7 RE (1)	Password generation and lifetime restrictions for human users	Not Applicable	Not Applicable	Yes	Yes	In REX640, password complexity, password expiration policies, prevention of recent password reuse, and account lock-out after a set number of failed login attempts can be configured through centralized account management using Active Directory or other account management software that supports LDAP communication.  These configured rules in centralized account management enforce strong, regularly updated passwords, minimizing unauthorized access and lowering the risk of attackers exploiting weak or outdated passwords.

ID	Requirement	SL1	SL2	SL3	SL4	Implemented in-REX640
CR 1.7 RE (2)	Password lifetime restrictions for all users (human, software process, or device)	Not Applicable for SL1	Not Applicable for SL2	Not Applicable for SL3	No	<p>In REX640, password complexity, password expiration policies, prevention of recent password reuse, and account lock-out after a set number of failed login attempts can be configured through centralized account management using Active Directory</p> <p>REX640 is designed to work with PKI, which includes certificate creation, expiration validation, and certificate revocation management. Additionally, the IED supports updating the necessary lifetime restrictions through manual certificate updates for both devices and software processes.</p>
CR 1.8	Public key infrastructure certificates	Not Applicable for SL1	Yes	Yes	Yes	<p>REX640 supports integration with customer-managed Public Key Infrastructure (PKI) for certificate management. This feature allows users to leverage their existing PKI systems to manage digital certificates, ensuring secure and authenticated communications. By utilizing customer PKI, REX640 can work with certificates issued by the customer's trusted certificate authority, facilitating secure interactions and providing enhanced control over certificate issuance and management.</p>
CR 1.9	Strength of public key-based authentication	Not Applicable for SL1	Yes	Yes	Yes	<p>Implemented according to IEC 62351.</p>
CR 1.9 RE (1)	Hardware security for public key-based authentication	Not Applicable for SL1	Not Applicable for SL2	Yes	Yes	<p>Managed via inbuilt security module known as the Trusted Platform Module (TPM) and internal database.</p>

ID	Requirement	SL1	SL2	SL3	SL4	Implemented in-REX640
CR 1.10	Authenticator feedback	Yes	Yes	Yes	Yes	In REX640, passwords are masked as asterisks (*) to ensure privacy and security when users enter their username and password in the LHMI or WEBHMI. This masking technique prevents unauthorized individuals from viewing the actual password characters during entry or display
CR 1.11	Unsuccessful login attempts	Yes	Yes	Yes	Yes	A user account is locked out for 30 seconds after five unsuccessful login attempts. An Audit trail event is logged to record this information, Maximum number of invalid login attempts and duration for lockout is not configurable
CR 1.12	System use notification	Yes	Yes	Yes	Yes	REX640 displays a system use notification message on the LHMI before authentication when providing local user access. This message can be configured by authorized personnel through PCM600.
NDR 1.13	Access via untrusted networks					Requirement not applicable for the protection relay
NDR 1.13 RE (1)	Explicit access request approval					Requirement not applicable for the protection relay
CR 1.14	Strength of symmetric key-based authentication	Not Applicable	Not Applicable	Not Applicable	Not Applicable	REX640 support asymmetric key based authentication and hence not applicable.
CR 1.14 RE (1)	Hardware security for symmetric key-based authentication	Not Applicable	Not Applicable	Not Applicable	Not Applicable	REX640 support asymmetric key based authentication and hence not applicable.
CR 2.1	Authorization enforcement	Yes	Yes	Yes	Yes	Authorization enforcement is managed through a role-based access control system and centralized account management.

CR 2.1 RE (1)	Authorization enforcement for all users (humans, software processes and devices)	Not Applicable for SL1	Yes	Yes	Yes	Authorization enforcement is implemented for human users and is supported across Web HMI and PCM600. Secure Authentication is supported for IEC104, DNP3 and MMS Protocols. Note: Modbus protocol does not support authentication and Authorization, Hence, system level countermeasure is needed
---------------	--	------------------------	-----	-----	-----	--

ID	Requirement	SL1	SL2	SL3	SL4	Implemented in-REX640
CR 2.1 RE (2)	Permission mapping to roles	Not Applicable for SL1	Yes	Yes	Yes	Role-based access control is supported in accordance with IEC 62351-8. Users can be assigned specific roles, which can then be mapped to corresponding permissions
CR 2.1 RE (3)	Supervisor override	Not Applicable for SL1	Not Applicable for SL2	No	No	Not supported
CR 2.1 RE (4)	Dual approval	Not Applicable for SL1	Not Applicable for SL2	Not Applicable for SL3	No	Not supported
CR 2.2	Wireless use control	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Wireless communication is not used in REX640, Hence this requirement is not applicable.
CR 2.3	Use control for portable and mobile devices	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Requirement not applicable for the protection relay
SAR 2.4	Mobile code	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Requirement not applicable for the protection relay
SAR 2.4 RE (1)	Mobile code authenticity check	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Requirement not applicable for the protection relay
EDR 2.4 EDR 2.4 RE (1)	Mobile code	Not Applicable	Not Applicable	Not Applicable	Not Applicable	REX640 does not support user executable mobile code, therefore this requirement is not applicable.
HDR 2.4	Mobile code	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Requirement not applicable for the protection relay
HDR 2.4 RE (1)	Mobile code authenticity check	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Requirement not applicable for the protection relay
NDR 2.4	Mobile code	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Requirement not applicable for the protection relay
NDR 2.4 RE (1)	Mobile code authenticity check	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Requirement not applicable for the protection relay

ID	Requirement	SL1	SL2	SL3	SL4	Implemented in-REX640
CR 2.5	Session lock	Yes	Yes	Yes	Yes	After a configurable period of inactivity in LHMI or WebHMI, the user is automatically logged out from both WebHMI, PCM600 and the Local HMI. This means that if there is no activity or interaction from the user for a certain amount of time, REX640 terminates the user's session to ensure security and prevent unauthorized access
CR 2.6	Remote session termination	Not Applicable for SL1	Yes	Yes	Yes	Remote session applicable for WebHMI. After a configurable period of inactivity, the user is automatically logged out from WebHMI, this means that if there is no activity or interaction from the user for a certain amount of time, REX640 terminates the user's session to ensure security and prevent unauthorized access
CR 2.7	Concurrent session control	Not Applicable for SL1	Not Applicable for SL2	Yes	Yes	REX640 supports concurrent session control to ensure secure, efficient, and reliable system performance. It allows for the management and regulation of multiple session attempts by supporting a maximum of 8 communication sessions (client connections) at any given time, regardless of the protocol type. Additionally, only one active PCM600 connection and one active Web HMI session are allowed per relay.
CR 2.8	Auditable events	Yes	Yes	Yes	Yes	REX640 records events locally and has the capability to transmit audit logs to a centralized log server or SIEM via the syslog messages.  The Logs are stored with event name, time stamp, username and event ID.  The logs are immutable and cannot be modified or edited, ensuring that they are accessible only to authorized users for viewing.

ID	Requirement	SL1	SL2	SL3	SL4	Implemented in-REX640
CR 2.9	Audit storage capacity	Yes	Yes	Yes	Yes	The protection relay stores up to 2,048 audit trail events in non-volatile memory. Additionally, it retains 1,024 process events in a non-volatile event list. A FIFO buffer is used for the audit trail, where old events are overwritten by new ones when the buffer becomes full
CR 2.9 RE (1)	Warn when audit record storage capacity threshold reached	Not Applicable for SL1	Not Applicable for SL2	No	No	<b>REX640</b> supports a circular buffer for audit events, automatically deleting older events when the storage limit is reached to make room for new ones. Additionally, it can transfer audit events to an external server in syslog format. As a result, explicit management of audit warnings is not required, ensuring that the relay complies with the relevant requirements.
CR 2.10	Response to audit processing failures	Not Applicable for SL1	Not Applicable for SL2	Yes	Yes	<b>REX640 Relay</b> not only stores audit events locally but also supports streaming to back up data to a syslog server. Additionally, it utilizes cyclic storage to avoid capacity overload by automatically replacing older events with newer events when the storage capacity is reached. This ensures that storage remains within manageable limits. With these features, the <b>REX640 Relay</b> enables efficient audit log management and maintains stability while preventing disruptions from storage limitations or overload.
CR 2.11	Timestamps	Yes	Yes	Yes	Yes	The <b>REX640 relay</b> generates audit events with time stamps, which are recorded in UTC by default. Optionally, the local time zone and Day light saving can be configured within the IED. Timestamps are available for local security log and central activity logging syslog events.
CR 2.11 RE (1)	Time synchronization	Not Applicable for SL1	Yes	Yes	Yes	SNTP and PTP are supported, and the system can connect to a GPS clock for precise time synchronization.

CR 2.11 RE (2)	Protection of time source integrity	Not Applicable for SL1	Not Applicable for SL2	Not Applicable for SL3	No	Not supported, it is recommended to configure firewall rules to protect the clock synchronization messages.
----------------	-------------------------------------	------------------------	------------------------	------------------------	----	---

ID	Requirement	SL1	SL2	SL3	SL4	Implemented in-REX640
CR 2.12	Non-repudiation	Yes	Yes	Yes	Yes	All user actions are logged in the audit trail, provided that role-based access control is properly configured in the IED using either local account management or centralized account management, The Audit trail logs the username and roles, Date, and time of the user action. It ensures non-repudiation.
CR 2.12 RE (1)	Non-repudiation for all users	Not Applicable for SL1	Not Applicable for SL2	Not Applicable for SL3	No	Non-repudiation can only be achieved by users accessing the IED through PCM600 or Web HMI or Local HMI. Non-repudiation through communication protocols such as IEC104, DNP3, or IEC61850 are not implemented
EDR 2.13	Use of physical diagnostic and test interfaces	Not Applicable for SL1	Yes	Yes	Yes	The physical factory diagnostic and test interfaces are protected and not accessible during rest and transit.
EDR 2.13 RE (1)	Active monitoring	Not Applicable for SL1	Yes	Yes	Yes	JTAG interface is disabled in the factory and user cannot access the interface.
HDR 2.13	Use of physical diagnostic and test interfaces	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Requirement not applicable for the protection relay
HDR 2.13 RE (1)	Active monitoring	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Requirement not applicable for the protection relay
NDR 2.13	Use of physical diagnostic and test interfaces	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Requirement not applicable for the protection relay
NDR 2.13 RE (1)	Active monitoring	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Requirement not applicable for the protection relay
CR 3.1	Communication integrity	Yes	Yes	Yes	Yes	TLS 1.2 or 1.3 is utilized for secure PCM600 engineering configuration through FTPS, and secure HTTPS for WebHMI access, Secure IEC 61850 MMS, Secure IEC104 and Secure DNP3 supported.

<p>CR 3.1 RE (1)</p>	<p>Communication authentication</p>	<p>Not Applicable for SL1</p>	<p>Yes</p>	<p>Yes</p>	<p>Yes</p>	<p>TLS 1.2 or 1.3 based Certificate exchange method is used to authenticate device communication with PCM600, as well as to authenticate communication between Relay, SCADA and WebHMI.</p> <p><b>Note:</b> Communication authentication not supported: Modbus, SNTP, PTP, GOOSE, SMV. Hence, the system-level countermeasures are required to protect these non-secured protocols.</p>
----------------------	-------------------------------------	-------------------------------	------------	------------	------------	---

ID	Requirement	SL1	SL2	SL3	SL4	Implemented in-REX640
SAR 3.2	Protection from malicious code	Yes	Yes	Yes	Yes	PCM600 files and connectivity packages are digitally signed
EDR 3.2	Protection from malicious code	Yes	Yes	Yes	Yes	The firmware file is digitally signed and validated by REX640 through secure boot mechanism to ensure the firmware integrity and authenticity.
HDR 3.2	Protection from malicious code	N/A	N/A	N/A	N/A	Requirement not applicable for the protection relay
HDR 3.2 RE (1)	Report version of code protection	N/A	N/A	N/A	N/A	Requirement not applicable for the protection relay
NDR 3.2	Protection from malicious code	N/A	N/A	N/A	N/A	Requirement not applicable for the protection relay
CR 3.3	Security functionality verification	Yes	Yes	Yes	Yes	Guidance for verifying security functionality is provided in the REX640 Cyber Security Deployment Guideline. Instructions for triggering security events are included.
CR 3.3 RE (1)	Security functionality verification during normal operation	Not Applicable for SL1	Not Applicable for SL2	Not Applicable for SL3	No	You can verify access control, authorization, centralized account management, audit access, and secure communication during relay operation. However, we do not recommend online verification of the Ethernet filter and rate limiter functionality.
CR 3.4	Software and information integrity	Yes	Yes	Yes	Yes	The firmware file is digitally signed and validated by PCM600 before being downloaded to REX640.
CR 3.4 RE (1)	Authenticity of software and information	Not Applicable for SL1	Yes	Yes	Yes	The REX640 Secure boot with integrity and authenticity checks guarantees the integrity of the firmware. Importing a configuration includes integrity and authenticity checks
CR 3.4 RE (2)	Automated notification of integrity violations	Not Applicable for SL1	Not Applicable for SL1	No	No	
CR 3.5	Input validation	Yes	Yes	Yes	Yes	REX640 validates the syntax, content, and length of input data before allowing it to be processed by the control and protection application.

ID	Requirement	SL1	SL2	SL3	SL4	Implemented in-REX640
CR 3.6	Deterministic output	Yes	Yes	Yes	Yes	When the device encounters an error during normal operation, all outputs are automatically reset to a predefined default state. This state is set by the REX640 and cannot be modified by the user
CR 3.7	Error handling	Yes	Yes	Yes	Yes	Only necessary error messages are provided without revealing any additional information which is potentially harmful
CR 3.8	Session integrity	Not Applicable for SL1	Yes	Yes	Yes	When a user logs out or remains inactive for a specific duration without any operations all active sessions will be automatically terminated. Only Limited sessions are permitted. This is applicable for REX640 WebHMI, LHMI and PCM600.
CR 3.9	Protection of audit information	Not Applicable for SL1	Yes	Yes	Yes	The REX640 supports audit logs that are read-only, and they can be accessed only by security administrators, ensuring they cannot be modified or deleted. Additionally, these logs can be securely transmitted to a central server using syslog protocols.
CR 3.9 RE (1)	Audit records on write-once media	Not Applicable for SL1	Not Applicable for SL2	Not Applicable for SL3	No	REX640 supports syslog-based audit log transfer for centralized log management. It is the customer's responsibility to store these logs on write-once media, ensuring tamper-proof storage. The solution provides flexibility for customers to select their preferred write-once media devices. This approach ensures secure and compliant log storage for long-term integrity.
EDR 3.10	Support for updates	Yes	Yes	Yes	Yes	The protection relay is equipped with an update mechanism that supports both secure firmware upgrades and downgrades with proper access control. This allows for seamless updates, keeping the devices current with the latest features, improvements, and security patches.

EDR 3.10 RE (1)	Update authenticity and integrity	Not Applicable for SL1	Yes	Yes	Yes	The PCM600 and REX640 verifies the digital signature of the firmware file and allows the firmware download if the signature is valid.
HDR 3.10	Support for updates					Requirement not applicable for the protection relay
HDR 3.10 RE (1)	Update authenticity and integrity					Requirement not applicable for the protection relay
NDR 3.10	Support for updates					Requirement not applicable for the protection relay
NDR 3.10 RE (1)	Update authenticity and integrity					Requirement not applicable for the protection relay

ID	Requirement	SL1	SL2	SL3	SL4	Implemented in-REX640
EDR 3.11	Physical tamper resistance and detection	Not Applicable for SL1	Yes	No	No	<p>Changes to HW configuration are logged, JTAG port is disabled in factory for making tampering more difficult.</p> <p><b>Physical Compensating Countermeasure:</b></p> <ul style="list-style-type: none"> <li>• Implement strong access control for the protection relay control room, restricting key access to authorized personnel only.</li> <li>• Ensure the control panel is securely locked to prevent unauthorized tampering.</li> <li>• Deploy 24/7 surveillance cameras and motion/intrusion detection alarms to monitor and protect the area housing the relay.</li> </ul>
EDR 3.11 RE (1)	Notification of a tampering attempt	Not Applicable for SL1	Not Applicable for SL2	No	No	
HDR 3.11	Physical tamper resistance and detection	N/A	N/A	N/A	N/A	Requirement not applicable for the protection relay
HDR 3.11 RE (1)	Notification of a tampering attempt	N/A	N/A	N/A	N/A	Requirement not applicable for the protection relay
NDR 3.11	Physical tamper resistance and detection	N/A	N/A	N/A	N/A	Requirement not applicable for the protection relay
NDR 3.11 RE (1)	Notification of a tampering attempt	N/A	N/A	N/A	N/A	Requirement not applicable for the protection relay
NDR 3.10 RE (1)	Update authenticity and integrity	N/A	N/A	N/A	N/A	Requirement not applicable for the protection relay

ID	Requirement	SL1	SL2	SL3	SL4	Implemented in-REX640
EDR 3.12	Provisioning product supplier roots of trust	Not Applicable for SL1	Yes	Yes	Yes	REX640 relay uses a Supplier Root of Trust to ensure secure identity provisioning during manufacturing. Each device is assigned a unique IDEVID with a cryptographic X.509 certificate, signed by the manufacturer's PKI. This certificate verifies the authenticity of the relay, and the private key is securely stored to prevent tampering. Upon deployment, the relay's identity is validated, ensuring trusted communication, and protecting against unauthorized access. This process guarantees that REX640 remains secure from the moment it leaves the factory during manufacturing
HDR 3.12	Provisioning product supplier roots of trust					Requirement not applicable for the protection relay
NDR 3.12	Provisioning product supplier roots of trust					Requirement not applicable for the protection relay
EDR 3.13	Provisioning asset owner roots of trust	Not Applicable for SL1	Yes	Yes	Yes	REX640 supports Provisioning Asset Owner Roots of Trust using Public Key Infrastructure (PKI) or Asset owners can generate and load their own certificates into REX640. This ensures secure provisioning of cryptographic credentials like keys and X.509 certificates, enabling robust root of trust for secure communication and authentication,
HDR 3.13	Provisioning asset owner roots of trust					Requirement not applicable for the protection relay
NDR 3.13	Provisioning asset owner roots of trust					Requirement not applicable for the protection relay

ID	Requirement	SL1	SL2	SL3	SL4	Implemented in-REX640
EDR 3.14	Integrity of the boot process	Yes	Yes	Yes	Yes	REX640 supports Secure Boot,. Secure Boot ensures that the device boots only with trusted and authenticated software by verifying the digital signature of each software component during the boot process. It relies on a hardware-based root of trust to build a chain of trust, halting the boot or initiating recovery if any component fails verification. This mechanism protects against tampering and unauthorized software execution.
EDR 3.14 RE (1)	Authenticity of the boot process	Not Applicable for SL1	Yes	Yes	Yes	REX640 ensures the authenticity of the boot process through Secure Boot mechanisms. This process guarantees that only trusted and verified software is executed during boot.
HDR 3.14	Integrity of the boot process	N/A	N/A	N/A	N/A	Requirement not applicable for the protection relay
HDR 3.14 RE (1)	Authenticity of the boot process	N/A	N/A	N/A	N/A	Requirement not applicable for the protection relay
NDR 3.14	Integrity of the boot process	N/A	N/A	N/A	N/A	Requirement not applicable for the protection relay
NDR 3.14 RE (1)	Authenticity of the boot process	N/A	N/A	N/A	N/A	Requirement not applicable for the protection relay

ID	Requirement	SL1	SL2	SL3	SL4	Implemented in-REX640
CR 4.1	Information confidentiality	Yes	Yes	Yes	Yes	<p>REX640 supports TLS 1.2 or TLS 1.3 with RSA/DHE/ECDHE encryption to protect information during transit. For data at rest, the protection relay and PCM600 implement robust access control measures, password hashing, key encryption to ensure security. The secure communication mechanisms supported are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Engineering tool PCM600 to REX640:</b> Secure communication is achieved using FTPS (File Transfer Protocol Secure).</li> <li>• <b>SCADA to REX640:</b> Supports secure protocols such as Secure IEC104, Secure DNP, and Secure MMS for communication.</li> <li>• <b>CAM Server (Centralized Account Management) to REX640:</b> Utilizes LDAP Secure for secure account management.</li> </ul> <p><b>Central Audit Logging:</b> Communication between the Syslog server and REX640 is secured using Secure Syslog with TLS 1.2 or 1.3</p> <p><b>Note:</b> Modbus, SNTP, GOOSE, Sample measured value protocols do not support encryption. Hence, the system-level countermeasures are required to protect these non-secured protocols.</p>
CR 4.2	Information persistence	Not Applicable for SL1	Yes	Yes	Yes	<p>The REX640 Protection relay supports a device decommissioning feature that allows for the complete removal of all information, including device data, logs, and configuration data. When a device is decommissioned, all its associated data and logs are securely erased, ensuring that no sensitive information remains on the device.</p>

CR 4.2 RE (1)	Erase of shared memory resources	Not Applicable for SL1	Not Applicable for SL2	No	No	Not implemented
CR 4.2 RE (2)	Erase verification	Not Applicable for SL1	Not Applicable for SL2	No	No	Not implemented

ID	Requirement	SL1	SL2	SL3	SL4	Implemented in-REX640
CR 4.3	Use of cryptography	Yes	Yes	Yes	Yes	The REX640 Protection Relay complies with RSA/DHE/EC-DHE standards for implementing cryptographic algorithms. It utilizes an X.509 certificate and an RSA key pair with a key length of either 1024, 2048, 3072 and 4096 bits. The RSA key embedded in the certificate facilitates secure communication.
CR 5.1	Network segmentation	Yes	Yes	Yes	Yes	Network segmentation is supported by REX640 through the configuration of the necessary Ethernet ports and relevant network settings. VLAN is supported for GOOSE and Sampled values for separating the critical messages from other ethernet traffic.
NDR 5.2	Zone boundary protection	N/A	N/A	N/A	N/A	Requirement not applicable for the protection relay
NDR 5.2 RE (1)	Deny all, permit by exception	N/A	N/A	N/A	N/A	Requirement not applicable for the protection relay
NDR 5.2 RE (2)	Island mode	N/A	N/A	N/A	N/A	Requirement not applicable for the protection relay
NDR 5.2 RE (3)	Fail close	N/A	N/A	N/A	N/A	Requirement not applicable for the protection relay
NDR 5.3	General purpose, person-to-person communication restrictions	N/A	N/A	N/A	N/A	Requirement not applicable for the protection relay
CR 6.1	Audit log accessibility	Yes	Yes	Yes	Yes	In REX640, authorized users have read-only access to audit logs, which can be viewed through LHMI, PCM600 and WebHMI. These logs capture all security-related and process-related events, and the audit files cannot be edited or modified. Audit logs can be transferred to central server through syslog protocol
CR 6.1 RE (1)	Programmatic access to audit logs	Not Applicable for SL1	Not Applicable for SL2	Yes	Yes	The SIEM server can access the REX640 audit logs using the Syslog protocol
CR 6.2	Continuous monitoring	Not	Yes	Yes	Yes	The REX640 audit logs can be transferred to the SIEM via the

		Applicable for SL1				Syslog (Secure) protocol, enabling continuous monitoring for anomaly detection. It includes security events and process events.
--	--	--------------------	--	--	--	---

ID	Requirement	SL1	SL2	SL3	SL4	Implemented in-REX640
CR 7.1	Denial of service protection	Yes	Yes	Yes	Yes	The DOS attacks are mitigated using an Ethernet rate limiter. This technique controls the amount of traffic sent or received by REX640. To monitor the DoS events, a dedicated function block (GSAL) can be configured within the REX640 Protection relay.
CR 7.1 RE(1)	Manage communication load from component	Not Applicable for SL1	Yes	Yes	Yes	An Ethernet filter is a mechanism in REX640 used to selectively permit or block network traffic based on protocol type. It can be configured for each physical port to control the flow of GOOSE and Sampled Measured Value (SMV) traffic, preventing unnecessary data from reaching unwanted ports.
CR 7.2	Resource management	Yes	Yes	Yes	Yes	<p><b>CPU Management:</b> The rate limiter in REX640 controls CPU usage, preventing overload from any single application.</p> <p><b>Memory Management:</b> Memory allocation is optimized to avoid crashes and ensure efficient resource use.</p> <p><b>Network Bandwidth Management:</b> REX640 prioritizes critical communications, such as GOOSE and SMV, over other protocols. Additionally, The Ethernet Filter in REX640 helps block unwanted network traffic, reducing unnecessary strain on bandwidth.</p> <p><b>Storage Management:</b> Log sizes are controlled, and a circular buffer is used to prevent buffer overflow by overwriting older events with new ones when the buffer is full.</p>

ID	Requirement	SL1	SL2	SL3	SL4	Implemented in-REX640
CR 7.3	Control system backup	Yes	Yes	Yes	Yes	Backups in PCM600 and REX640 includes the entire project configuration, individual protection relay offline configurations, and online configuration files captured from the relay during operation. This comprehensive approach ensures a complete record of the system's state for effective recovery. Additionally, REX640 supports periodic backups and allows you to schedule backup frequencies in PCM600. This ensures automatic saving of the latest configuration changes in the relay.
CR 7.3 RE (1)	Backup integrity verification	Not Applicable for SL1	Yes	Yes	Yes	In PCM600 and REX640, backup files are digitally signed and hashed to ensure data integrity and authenticity. Any modification to a backup file will be detected and the user will be notified.
CR 7.4	Control system recovery and reconstitution	Yes	Yes	Yes	Yes	In the event of failure, the REX640 protection relay can be returned to a secure operational state through a two-step recovery process: <ol style="list-style-type: none"> <li>1. <b>Factory Restore:</b> This step resets all settings and configurations to their secure default values, eliminating any potentially compromised data.</li> <li>2. <b>Backup Restore:</b> The latest secure backup is then loaded from PCM600, reinstating the previous settings and configurations.</li> </ol>
CR 7.5	Emergency power	Not Applicable for SL1	Not Applicable for SL2	Not Applicable for SL3	Not Applicable for SL4	REX640 supports both AC and DC power inputs, allowing for the connection of a UPS or battery power to ensure an uninterrupted power supply to the relay.

CR 7.6	Network and security configuration settings	Yes	Yes	Yes	Yes	REX640 user guides offer step-by-step instructions for configuring network and security settings and are easily accessible through PCM600. Comprehensive cyber security procedures are outlined in the cyber security deployment guidelines of REX640 and PCM600.
CR 7.6 RE (1)	Machine-readable reporting of current security settings	Not Applicable for SL1	Not Applicable for SL2	Yes	Yes	It is possible to export the required security settings from PCM600

ID	Requirement	SL1	SL2	SL3	SL4	Implemented in-REX640
CR 7.6 RE (1)	Machine-readable reporting of current security settings	Not Applicable for SL1	Not Applicable for SL2	Yes	Yes	It is possible to export the required security settings from PCM600
CR 7.7	Least functionality	Yes	Yes	Yes	Yes	REX640 provides the ability to disable unnecessary functions, ports, protocols, and services. Only mandatory services for PCM600 (FTPS) and HMI (HTTPS) are enabled by default. Both physical ports and communication protocol logical ports can be deactivated and read/write access for each protocol can be configured to prevent unauthorized write operations. Detailed information on these configurations is available in the REX640 Cyber security Deployment Guidelines.
CR 7.8	Control system component inventory	Not Applicable for SL1	Yes	Yes	Yes	The Protection relay serial number, Technical Key, firmware version, Connectivity package type can be obtained from PCM600 and HMI. The same inventory information can be accessible through IEC 61850 MMS communication.

—  
**ABB Oy**  
**Distribution Solutions**  
P.O. Box 699  
65101 Vaasa, Finland

[abb.com/mediumvoltage](http://abb.com/mediumvoltage)