

RELION® PROTECTION AND CONTROL

# REX640

## Declaration of Security Conformance



# Table of Contents

<b>1</b>	<b>About this manual .....</b>	<b>4</b>
1.1	Read it first!.....	4
1.2	Document information .....	4
1.3	Safety Information.....	4
<b>2</b>	<b>Abbreviations.....</b>	<b>6</b>
2.1	Abbreviations.....	6
<b>3</b>	<b>Applicable standards .....</b>	<b>8</b>
<b>4</b>	<b>BDEW Whitepaper Security requirements – Conformance statement.....</b>	<b>36</b>
4.1	General Requirements.....	36
4.1.1	Secure System Architecture .....	36
4.1.2	Patching and Patch Management.....	37
4.1.3	Provision of Security Patches for all System Components	38
4.1.4	Support for Deployed System Components.....	38
4.1.5	Encryption of Sensitive Data.....	39
4.1.6	Cryptographic Mechanisms .....	39
4.1.7	Secure Standard Configuration.....	39
4.1.8	Integrity Testing.....	40
4.1.9	Use of Cloud Services .....	40
4.1.10	Documentation Requirements .....	41
4.2	Project Management .....	42
4.2.1	Security and Acceptance Testing.....	42
4.2.2	Secure Data Storage and Transmission .....	42
4.2.3	Delivery of Project-Specific Modifications .....	43
4.3	Base system .....	44
4.3.1	System Hardening.....	44
4.3.2	Malware Protection.....	44
4.3.3	Autonomous User Authentication .....	45
4.3.4	Virtualization Technologies.....	45
4.4	Network and Communications .....	47
4.4.1	Used Protocols and Technologies .....	47
4.4.2	Secure Network Structure .....	48
4.4.3	Documentation of Network Structure and Configuration.	49
4.4.4	Secure Remote Access .....	49
4.4.5	Wireless Technologies.....	50
4.5	Application .....	51
4.5.1	Role Concepts .....	51

4.5.2	User Authentication and Login.....	51
4.5.3	Authorization of Actions at the User and System Levels ...	53
4.5.4	Web Applications and Web Services.....	53
4.5.5	Integrity Testing.....	54
4.5.6	Logging and monitoring controls.....	54
4.6	Development.....	56
4.6.1	Secure Development Standards, Quality Management and Approval Processes.....	56
4.6.2	Secure Development and Testing Systems, Integrity Testing.....	58
4.7	Maintenance.....	59
4.7.1	Maintenance Process Requirements .....	59
4.7.2	Secure Update Processes .....	59
4.7.3	Configuration and Change Management, Rollback.....	60
4.7.4	Handling of Vulnerabilities .....	60
4.8	Data Back-Up and Emergency Planning .....	61
4.8.1	Back-up: Concept, Method, Documentation, Testing.....	61
4.8.2	Emergency Concept and Recovery Plans.....	61

# 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 Cyber Security 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
B	25 Feb 2025	REX640 Product version 2.0, Software version 6.1, PCL6

### 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	<p>REX640 records events locally and has the capability to transmit audit logs to a centralized log server or SIEM via the syslog messages.</p> <p>The Logs are stored with event name, time stamp, username and event ID.</p> <p>The logs are immutable and cannot be modified or edited, ensuring that they are accessible only to authorized users for viewing.</p>

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	Yes	Yes	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.

CR 3.1 RE (1)	Communication authentication	Not Applicable for SL1	Yes	Yes	Yes	<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 verify the digital signature of the firmware file and allow 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 Countermeasures:</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.

## 4 BDEW Whitepaper Security requirements – Conformance statement

### 4.1 General Requirements

#### 4.1.1 Secure System Architecture

**ISO/IEC 27002:2013 / 27019:2017: 9.4.1, 13.1.3, 14.2.5, 14.2.7, 17.2.1**

Individual components and the entire system shall be designed and developed to support secure operations. Secure system design principles include:

**Security by design:** The entire system and its individual components are designed on the basis of and with a focus on security. Deliberate attacks and unauthorized actions are explicitly taken into account while any repercussions arising from a security event are minimized by the system's inherent design.

According to the ABB Minimum Cyber security policy, ABB is following a secure development process. All Products are designed and tested with security considerations. The REX640 Protection relay is designed with a strong emphasis on security, fully aligning with the IEC 62443-4-1 standard. Security considerations are integrated into every stage of our development lifecycle, ensuring that our products are resilient against potential attacks and unauthorized actions.

**Minimal need-to-know principle:** Each component and each user is only assigned the rights they need to execute a desired action. Applications and network services, for example, are not run under administrator privileges, but only with the bare minimum of required system access rights.

REX640 supports an access control mechanism based on Role-Based Access Control (RBAC). RBAC is a security model that restricts system access to authorized users by assigning specific roles with limited privilege. In REX640, Operators are granted access only to the essential functions required for monitoring and operating the relay, such as viewing real-time data and operating circuit breakers. Operators do not have access to configuration settings or security features.

**Defense-in-depth principle:** Security risks are not tackled via single protection measures, but limited through the implementation of staggered, multi-level and complementary security measures.

The Defense in Depth Principle is applied in REX640 using a multi-layered security approach. This includes hardening, authentication, authorization, secure communication, audit logs, certificate-based authentication, PCM600

firmware file digital signature verification, backup and recovery, and vulnerability management. Together, these layers work to provide comprehensive protection, ensuring system resilience and security.

**Redundancy principle:** The entire system is designed to ensure that the failure of individual components does not impair security-related functions. The system's design lowers the likelihood and impact of issues caused by unrestricted requests for system resources such as e.g. main memory (RAM) or network bandwidth (so-called resource consumption or DoS attacks).

In REX640, The primary mechanisms used to prevent DoS attacks are the Ethernet Filter and the Rate Limiter which are crucial for ensuring the reliability and availability of the system in a substation network environment.

#### **4.1.2 Patching and Patch Management**

##### **ISO/IEC 27002:2013 / 27019:2017: 12.6.1**

All system components shall be patchable. The supplier shall support a patch management process for both the individual components and the entire system, designed to enable the control and management of security patch testing, installation and documentation.

The operator himself resp. the assigned service provider shall be able to install the security patches and updates. Patch installations resp. uninstalls shall be authorized by the operator and shall not occur automatically.

Any installation resp. uninstall shall be recorded in a transparent and tamper-proof way within the system.

The integrity of security patches and updates shall be verifiable using a cryptographic mechanism.

ABB has a standard patch management process. We confirm that all ABB protection relays are patchable, and a comprehensive patch management process is supported. This process enables controlled and secure management of security patch testing, installation, and documentation. The operator or assigned service provider can install security patches and updates, with proper authorization control. Patch installations and uninstalls will not occur automatically and must be authorized by the operator.

### **4.1.3 Provision of Security Patches for all System Components**

#### **ISO/IEC 27002:2013 / 27019:2017: 12.5.1, 12.6.1**

The supplier shall ensure that security updates are available for all system components throughout the entire contractually stipulated operating timeframe.

The contractor shall obtain, test and – where necessary – forward updates from the respective manufacturers for basic components that were not developed by the contractor himself such as the operating system, libraries or database management systems. All update testing, approval and delivery shall take place within an adequate, contractually stipulated timeframe.

ABB has a well-defined patch management process for security updates of REX640 and PCM600, ensuring minimal effort is required for all protection relays. All patches are thoroughly tested before release, with ABB utilizing a dedicated cyber security testing center to verify vulnerabilities. The process is designed to ensure that security and firmware updates are applied efficiently, minimizing downtime and operational disruption.

### **4.1.4 Support for Deployed System Components**

#### **ISO/IEC 27002:2013 / 27019:2017: 12.6.1, 14.2.7**

The supplier shall ensure that within the planned and contractually stipulated operating timeframe, manufacturer support and security updates are available for system components developed by both the supplier and third-parties (e. g. operating system, database management system etc.). A binding agreement should cover the discontinuation procedure as well as relevant minimum terms like e. g. last customer shipping and end of support.

Security updates are provided in accordance with ABB's life cycle policy for REX640 and PCM600. ABB includes relevant third-party security patches for PCM600 and REX640, subject to availability from the third-party vendors.

#### **4.1.5 Encryption of Sensitive Data**

**ISO/IEC 27002:2013 / 27019:2017: 10.1.1, 12.4.2, 13.1.2, 18.1.3, 18.1.4**

Confidential data shall only be stored resp. transmitted encrypted.

1. Secure communication via FTPS is implemented between REX640 and PCM600, ensuring encrypted data exchange, ensuring data confidentiality.
2. Encrypted communication is used between REX640 and Central Account Management, providing secure and encrypted credential exchanges.
3. Audit logs are read-only and cannot be modified or deleted, ensuring data integrity.
4. Secure IEC 104 and DNP protocols are supported for remote data transmission, ensuring secure communication.
5. Syslog messages are supported for transferring audit logs to a centralized server. The secure Syslog feature will be introduced in REX640 version 2.0 PCL5.

#### **4.1.6 Cryptographic Mechanisms**

**ISO/IEC 27002:2013 / 27019:2017: 10.1.1, 10.1.2, 13.1.4 ENR, 18.1.5**

When selecting cryptographic mechanisms, national legislation shall be taken into account. Only approved mechanisms and minimum key sizes shall be used that are considered secure for the foreseeable future according to state-of-the-art technological knowledge. The supplier shall not use custom cryptographic algorithms.

The standard Public Key Cryptography is supported in both PCM600 and REX640 for secure communication. The protection relay utilizes X.509 certificates along with RSA key pairs, featuring key lengths of either 2048 or 1024 bits. No custom cryptography is used in REX640.

#### **4.1.7 Secure Standard Configuration**

**ISO/IEC 27002:2013 / 27019:2017: 9.4.4, 12.5.1, 14.3.1**

After initial installation, resp. at start-up or restart, the entire system shall be configured for a secure operating state. This defined basic configuration shall be documented. Services and functions as well as data that are only needed for

development or testing shall be removed demonstrably resp. permanently deactivated before delivery resp. before the switch to live operations.

In REX640, by default, only FTP and IEC61850 communications are enabled, facilitating interaction between PCM600 and REX640. All other protocol ports are closed initially. Users can activate required ports through PCM600. This secure default setup minimizes exposure to potential threats by keeping interfaces protected and enabling only the essential services needed for network operation.

#### **4.1.8 Integrity Testing**

##### **ISO/IEC 27002:2013 / 27019:2017: 12.5.1, 14.2.1, 14.2.4**

It shall be possible to check system files, applications, configuration files and application parameters for integrity, for example through cryptographic checksums.

REX640 firmware file is digitally signed, and digital signatures can be verified using PCM600. Additionally, PCM600 includes a plausibility check feature to validate the configured applications. The PCM600 and REX640 support authentication and Authorization to prevent unauthorized access of configuration files and applications.

#### **4.1.9 Use of Cloud Services**

##### **ISO/IEC 27002:2013 / 27019:2017: 15.1.1, 15.1.2, 15.2.1**

Where cloud services are used, the following requirements apply:

- a) Agreements shall be made with the cloud service provider about security-related processes for cloud infrastructure operations.
- b) Functions for the control of Critical Infrastructures, where manipulations could threaten the energy supply, shall not be realized in external cloud services.
- c) Downtime of a cloud service resp. access to this service shall not lead to significant restrictions of the system's defined basic function. Cloud service disruptions or outages shall also be considered in the emergency concept and restoration plans (see 4.8.2).

Cloud services are not used in REX640 and PCM600. Hence it is not applicable.

#### **4.1.10 Documentation Requirements**

##### **ISO/IEC 27002:2013 / 27019:2017: 7.2.2, 12.1.1, 14.1.1, 14.2.7**

At the latest, the client shall receive project-specific documentation at the system's handover.

For individual components and entire systems, the documentation shall cover a description of all security-related system settings and parameters as well as their standard values. Furthermore, the documentation shall list and briefly describe security-specific implementation details (like the employed cryptographic mechanisms).

The documentation shall also comprise additional information on the entire system's system architecture.

This includes the system's basic and fundamental structure as well as interactions between all involved components. In particular, this part of the documentation shall highlight security-related or sensitive system components as well as their mutual dependencies and interactions.

The REX640 Cyber Security Deployment Guideline offers in-depth information on all security-related settings, hardening procedures, secure communication protocols, certificate management, secure engineering configurations, and encryption mechanisms, along with their standard values. Additionally, the documentation provides a thorough overview of all cyber security features.

## 4.2 Project Management

### **ISO/IEC 27002:2013 / 27019:2017: 6.1.1, 6.1.5, 15.1.2**

The supplier shall define a contact who is responsible for IT security during the tender process and the system development phase as well as throughout the planned operations and maintenance timeframe.

This is a system level requirement and it is applicable for the system Integrator.

### **4.2.1 Security and Acceptance Testing**

#### **ISO/IEC 27002:2013 / 27019:2017: 14.2.7, 14.2.8, 14.2.9, 15.2.1**

Prior to delivery, the entire system's components and key functions shall be subjected to security and stress testing by the contractor – in a representative configuration and by an organizational unit independent of the development team. The actual procedure shall be discussed and agreed in coordination with the client. The results of these tests as well as the associated documentation (software versions, test configuration etc.) shall be made available to the client.

In addition, the client shall have the right to undertake these tests himself or to have them carried out by an external service provider. The type and scope of the acceptance tests shall be defined by the client.

For these tests, the client resp. the assigned service provider shall be given system access with a maximum of technologically possible access rights.

From the product/Component perspective, REX640 undergoes testing by ABB's Device Security Assurance Center to assess its robustness and identify vulnerabilities. Any vulnerabilities discovered during testing will be addressed and retested before the product is released to customers. This requirement applies to both PCM600 and all protection relays offered by ABB.

### **4.2.2 Secure Data Storage and Transmission**

#### **ISO/IEC 27002:2013 / 27019:2017: 6.2.1, 8.3.3, 10.1.1, 13.2.2, 13.2.3, 13.2.4, 14.3.1**

Confidential client data that is required or processed during the development and maintenance process shall be encrypted during transmission via insecure

connections. When saved on mobile storage media or systems, such data shall only be stored encrypted. The amount and duration of data storage shall be limited to a contractually specified minimum.

By default, only FTP and IEC61850 communications are enabled, facilitating interaction between PCM600 and REX640. All other protocol ports are closed initially. Users can activate additional ports through PCM600. This secure default setup minimizes exposure to potential threats by keeping interfaces protected and enabling only the essential services needed for network operation.

The REX640 2.0 PCL5 will include a secure boot feature with a crypto chip (TPM), enhancing the integrity of the boot process, ensuring secure firmware loading, and protecting private keys.

Passwords stored in PCM600 and REX640 are hashed.

### **4.2.3 Delivery of Project-Specific Modifications**

#### **ISO/IEC 27002:2013 / 27019:2017: 14.2.7**

For custom projects and project- resp. client-specific expansions, adjustments and engineering services, all project-specific parameterizations, changes and adaptations shall be comprehensively documented and supplied to the client in full.

This is a system level requirement and it is applicable for the system Integrator.

## 4.3 Base system

### 4.3.1 System Hardening

#### **ISO/IEC 27002:2013 / 27019:2017: 9.4.4, 12.6.2, 13.1.2, 14.2.4, 14.2.10 ENR**

All components of the base system shall be permanently hardened according to recognized best practice guidelines and the latest service packs and security patches shall be installed. Unnecessary users, default users, software, network protocols and services shall be uninstalled or – where an uninstall isn't possible – permanently deactivated and protected from accidental reactivation. The entire system's secure basic configuration shall be reviewed and documented.

Hardening details can be found in the PCM600 and REX640 Cyber Security Deployment Guidelines. Security patches for these products are released on time as needed.

### 4.3.2 Malware Protection

#### **ISO/IEC 27002:2013 / 27019:2017: 12.2.1**

All networked systems shall be equipped with malware protection at the appropriate location. Alternatively to malware protection provided on all system components, the supplier can submit a comprehensive malware protection concept that provides equal protection.

Where the use of a pattern-based solution is intended, these pattern files shall be updateable in a timely and automated manner. Such updates shall not take place via direct connection to update servers on external networks like the internet. For terminal systems, the time of updates needs to be configurable.

PCM600 verifies the signature of the firmware before downloading it to the controller and already it is supported.

Role-based access control allows only authorized persons to load the firmware and configuration files to REX640.

Additionally, the Secure boot features will be implemented in the **REX640 2.0 PCL5**, This feature provides enhanced malware protection -The secure boot feature will authenticate all software executables including boot binary, control firmware, and relevant hardware logic. The Relay runs executables produced and signed by ABB. A secured boot is accomplished by using the hardware root of a trusted boot mechanism. An access control procedure is applied to software production that involves signing operations. The access is

limited to relevant personnel only. The software that is modified or downloaded maliciously does not run during the startup.

The PCM600 computers are protected by Anti-virus installations.

### **4.3.3 Autonomous User Authentication**

#### **ISO/IEC 27002:2013 / 27019:2017: 9.2.1, 9.2.2, 9.4.2**

Data required for user identification and authentication shall not be obtained exclusively from outside the process network.

Authorized users can configure both local and centralized account management settings in the IED to control and limit user authentication, The users accounts roles and permissions are controlled by role based access control.

### **4.3.4 Virtualization Technologies**

#### **ISO/IEC 27002:2013 / 27019:2017: 12.1.3, 12.3.1, 12.6.1, 13.1.3, 17.2.1**

The following requirements govern the use of virtualization technologies:

- a) Virtualized components assigned to different security or trust zones (e.g. internal components and DMZ components) shall not be operated on the same virtualization servers. It shall not be possible to bypass the network segmentation of segregated security zones via virtualization servers.
- b) Networks used for management and administration services as well as data storage of the virtualization infrastructure shall be segregated from other networks by firewalls with only the minimum of required network services enabled in a restrictive manner. Access to the management and administration services and the above-mentioned networks shall be restricted to administrators only.
- c) The virtualization layer, the management and administration interfaces as well as the associated infrastructure shall be configured, secured and hardened identically and according to manufacturer recommendations. They shall also be included in the patch management and backup concept.
- d) The virtualization servers shall have sufficient resources for operating all of the virtualized components they are running. This is especially important for high-load operating situations.

- e) Any outage of virtualization servers or of other components of the virtualization infrastructure shall have no negative impact on the defined availability requirements. Disruptions and outages of the virtualization environment shall also be covered and considered in the emergency concept and restoration plans (see 4.8.2).

REX640 Protection relay does not support Virtualization technology.

PCM600 can be installed in a Virtual machine VMware

**Note.** ABB SSC600, the centralized protection and control supports Virtualization technology.

It is the responsibility of the asset owner or system integrator to manage virtual technologies and servers according to the project's requirements.

## 4.4 Network and Communications

### 4.4.1 Used Protocols and Technologies

**ISO/IEC 27002:2013 / 27019:2017: 9.4.1, 9.4.2, 10.1.1, 10.1.2, 12.9.1 ENR, 13.1.1, 13.1.2, 13.1.3, 13.1.4 ENR**

- a) In general, only secure communication standards and protocols that include integrity protection, authentication and, if applicable, encryption shall be used if and where the technology allows. This is a non-negotiable requirement for any protocols used for remote administration and parameterization and shall also be taken into account where non-standard resp. proprietary protocols are used.
- b) It shall be possible to integrate the entire system and any associated network components into the overall company's network concept. Central administration for relevant network configuration parameters like IP addresses shall be possible. For administration and monitoring secure protocols that ensure integrity protection, authentication and encryption shall be used. Network components shall be hardened, unnecessary services and protocols deactivated and management interfaces protected via ACLs.
- c) Network components provided by the supplier shall be capable of integrating into a central inventory and patch management.
- d) Where the technology allows it, WAN connections shall use the IP protocol and unencrypted application protocols shall be secured by encryption on the lower network layers (e. g. via TLS encryption or encrypted VPN technology).
- e) Where network infrastructure components are shared (e. g. by the use of VLAN or MPLS technologies), the network with the highest protection requirement level shall indicate the respective hardware and parameterization requirements. The shared use of network components shall only be shared in case of different protection requirements when this shared use can in no way decrease the protection level or availability.

Secure communication is supported for REX640 IEC104 and DNP3 protocol according to IEC 62351-3 and 5 for SCADA communication.

Secure FTPS communication is supported between REX640 and PCM600 through TLS 1.3

Secure HTTPS communication is supported between REX640 and WEB HMI through TLS 1.3

Communication between IED and centralized account management -Active Directory) is Encrypted and the credential transfer from IED to Centralized account management is kept confidential

Syslog protocols are supported, Secure syslog protocol support based on TLS 1.2 will be supported in REX640 2.0 PCL5

Secure MMS communication will be supported in REX640 2.0 PCL5.

SNMP V3 support will be available in REX640 2.0 PCL6.

#### **4.4.2 Secure Network Structure**

**ISO/IEC 27002:2013 / 27019:2017: 9.4.1, 12.9.1 ENR, 13.1.1,13.1.2, 13.1.3, 13.1.4 ENR, 13.1.5 ENR**

- a) Vertical network segmentation: Where applicable and technologically feasible, the system's underlying network structure shall be divided into zones with different functions and protection requirements.
- b) Where the technology allows it, these network zones shall be separated by firewalls, filtering routers or gateways. Communications with other networks shall only occur via the communication protocols approved by the client and in compliance with the applicable security guidelines.
- c) Horizontal network segmentation: Where applicable and technically feasible, the system's underlying network structure shall also be subdivided horizontally, into independent zones (e. g. according to sites) that are also separated by firewalls, filtering routers or gateways.

This is a system level requirement and it is applicable for the system Integrator.

#### **REX640 VLAN**

VLANs provide logical network segmentation, preventing direct access between segments. Using VLANs to implement zones ensures that protection relays in different security zones can only communicate with authorized devices through a firewall. VLAN functionality will be supported in REX640 2.0 PCL6 and can be configured via PCM600.

### **4.4.3 Documentation of Network Structure and Configuration**

#### **ISO/IEC 27002:2013 / 27019:2017: 8.1.1**

The following shall be documented: network design and configuration; all physical, virtual and logical network connections and the employed protocols, IP addresses and ports; and any network perimeters that are part of the system or interact with it. Any changes, e. g. via updates, shall be included in the documentation as part of the overall change management. This documentation shall also cover information on normal and maximum expected data transmission rates, to allow for limiting data transmission rates on the network components to prioritize traffic and prevent DoS issues, where necessary.

REX640 Cyber Security Deployment Guideline has all the information about the description of all security-related system settings and parameters as well as their standard values. Furthermore, the documentation briefly describes security-specific implementations.

REX640 relay supports Ethernet filtering to limit communication traffic and supports a rate limiter functionality to protect against DoS attacks. Detailed usage and configuration of the traffic filter and rate limiter are provided in the REX640 Cyber Security Deployment Guideline.

### **4.4.4 Secure Remote Access**

#### **ISO/IEC 27002:2013 / 27019:2017: 9.1.2, 9.4.1, 9.4.2**

- a) It shall be possible to administrate, maintain and configure all components via an out-of-band network, e. g. via local access, a serial port, a network or direct control of the input devices (KVM).
- b) Any remote access shall take place via centrally administrated access servers that are under control of the system operator. These access servers shall be operated within a DMZ and ensure isolation of the process network. Here, two factor authentication is mandatory.
- c) Strictly no direct dial in access to terminal devices.
- d) Any remote access shall be logged centrally; recurring failed attempts shall be reported.
- e) All remote access options shall be documented.

This is a system level requirement and it is applicable for the system Integrator

REX640 supports Centralized account management through LDAP and centralized audit log transfer through syslog. All the user actions, Process events and security related events are logged in REX640.

#### **4.4.5 Wireless Technologies**

##### **ISO/IEC 27002:2013 / 27019:2017: 10.1.1, 13.1.1, 13.1.2, 13.1.3**

Short-range wireless technologies (e. g. Wi-Fi, Bluetooth, ZigBee, RFID etc.) shall only be used after assessment of the related risks, under consideration of the following minimum-security measures and after consultation with and approval by the client:

- Wireless transmission technology shall to be secured with state of- the-art measures.
- Wi-Fi technology shall only be operated in dedicated network segments that are separated by firewalls and application proxies.
- Wi-Fi networks shall be configured in a way that ensures that existing Wi-Fi networks are not affected, disrupted or impaired.

Wireless communication is not supported by REX640 and therefore is not applicable.

## 4.5 Application

### 4.5.1 Role Concepts

#### ISO/IEC 27002:2013 / 27019:2017: 6.1.2, 9.2.1, 9.2.3, 9.2.6, 9.4.1

The entire system shall support granular access control to data and resources. To this end, it shall support user concept that covers at least the following user roles:

- Administrator: user who installs, maintains and manages the system. Among others, this gives the administrator the right to change security and system configurations.
- User: User who operates the system according to the intended usage scenario, including the right to change operationally relevant settings.
- Read-only user: User permitted to access the system status and pre-defined operating data without the right to make any changes.

The standard access rights shall reflect a secure system configuration. Only the administrator role shall be able to read and change security related system settings and configuration values. Regular system use shall only require user or read-only user rights. It shall be possible to deactivate user accounts individually without having to remove them from the system.

REX640 support role-based access control according to the IEC62351-8. It supports 8 roles and the detailed information is available in the Cyber Security Deployment Guideline.

It is possible to define the custom roles according to the user need.

### 4.5.2 User Authentication and Login

#### ISO/IEC 27002:2013 / 27019:2017: 9.3.1, 9.4.2, 9.2.1, 9.2.2, 9.4.3, 12.4.1

The application shall use personal users to identify and authenticate each individual user; group accounts require special permission by the client and shall only be used in narrowly defined exceptional cases.

- a) Without successful user authentication, the system shall only allow a range of narrowly defined actions.

REX640 supports role-based access control (RBAC), where users are assigned specific roles, each mapped to permissions that reflect the nature of their duties. Users are allowed to access the IED only after

successful authentication. User accounts can be configured directly within REX640 or managed centrally in the active directory through LDAP

- b) The system shall support a state-of-the-art password policy.

**Local Account management:** The user must enter the user name and password through the login banner, REX640 verifies the user name and password and allows the users to access REX640, The password policies can be configured through PCM600

**Central Account Management:** The user must enter their username and password via the login banner. REX640 transmits these credentials in an encrypted format to the central server (Active Directory) using LDAP communication. The Active Directory verifies the credentials, and upon successful verification, it creates a session for the user based on their assigned role. Detailed role and permission details are available in the REX640 Cyber Security Deployment Guideline. The secure LDAPS (LDAPS uses SSL/TLS to encrypt the LDAP traffic) and RADIUS (Remote Authentication Dial in user service) Authentication protocol will be implemented in REX640 PCL6 for enhancing the support for centralized account management.

- c) Where technologically possible, strong two factor authentication shall be employed, e. g. via tokens or smart cards.

The two-factor authentication is not implemented in REX640, as it is intended to be installed and operated within the substation facility. For the EON customer requirement, the authentication system server must support two-factor authentication, and the REX640 relay needs to allow sufficient time for the two factor authentication process to complete.

- d) Data required for user identification and authentication shall not be obtained exclusively from outside the process network (see also 4.3.3).

REX640 local account management is supported and also it supports freely configurable AD server addresses which means the AD server can be installed inside process network.

It is a customer's responsibility to install and maintain the account management server within the process network.

- e) Any successful or failed login attempts shall be centrally logged. It shall also be possible to centrally alarm in case of unsuccessful login attempts.

REX640 allows a maximum of 5 failed login attempts; after this, the IED locks the user account until the timeout period expires. All failed and successful login attempts are recorded in the audit log and can be transmitted to the central server via the syslog protocol.

### **4.5.3 Authorization of Actions at the User and System Levels**

#### **ISO/IEC 27002:2013 / 27019:2017: 9.4.1, of.4.4**

Certain security-related or safety-critical actions shall require prior authorization of the requesting user resp. the requesting system component.

Such actions might also include a read-out of process data points or configuration parameters.

The role-based access control in accordance with IEC 62351-8 configured in the protection relay ensures that only authorized personnel can perform specific operations. User credentials are validated either by REX640 or AD servers, depending on whether local or centralized account management is used.

### **4.5.4 Web Applications and Web Services**

#### **ISO/IEC 27002:2013 / 27019:2017: 14.2.5**

For web applications, web interfaces and web services, the recommendations of the OWASP TOP 10 and OWASP Application Security Verification Standard projects as well as the BSI Guideline on the Development of Secure Web Applications shall be applied.

Any deviations from these guidelines require justification and prior approval by the client.

OWASP TOP 10 vulnerabilities are tested by ABB Device Security Assurance Test Center (DSAC) and any gaps identified will be fixed before the product release.

REX640 supports a Web HMI interface where only authorized users can log in by providing a valid username and password configured either in REX640 or through a centralized Active Directory. Users are permitted to perform actions limited by their assigned roles. Session management is integrated into the

Web HMI, automatically locking out users after a configured period of inactivity.

#### 4.5.5 Integrity Testing

##### ISO/IEC 27002:2013 / 27019:2017: 14.2.5

The integrity of data processed as part of security-related activities shall be verified prior to processing (e. g. checked for plausibility, correct syntax and value range).

**Electrical Parameters:** PCM600 verifies that parameters fall within specified minimum and maximum ranges and their corresponding engineering units. If values are outside these ranges, an error message is displayed, and the PCM600 prevents the user from storing incorrect parameter ranges

Only validated parameters are transferred from PCM600 to REX640.

**Password storage:** The REX640 passwords are stored in a hashed format. This adds a layer of security, as the actual password is not stored.

#### 4.5.6 Logging and monitoring controls

##### ISO/IEC 27002:2013 / 27019:2017: 12.4.1, 12.4.2, 12.4.3, 12.4.4, 18.1.3

- a) The entire system shall have a uniform system time as well as an option for synchronizing this system time with an external secure time source.

REX640 uses both SNTP and PTP as time synchronization protocols. It is possible to configure external SNTP masters in the IED to receive time from an external source i.e. GPS.

- b) The system shall log user actions as well as security-related actions, events and errors in a format that is suitable for later and central processing. For a configurable minimum time period, these logs shall record date and time, the users and systems involved as well as the actual event and result.

REX640 includes an audit logging feature as per IEEE 1686 that records process events, user actions, and security-related events in chronological order. Each event is logged with the username, timestamp, event ID, and event description. REX640 stores 2048 audit trail events to the non-volatile audit trail. Additionally, 1024 process events are stored in a non-volatile event list. Both the audit trail and the event list work according to the FIFO principle.

- c) Log files shall be stored centrally at a freely configurable location. A mechanism for the automated transfer of the log file to central components shall be available.

Audit log messages can be transferred to a central server using the Syslog protocol. The automatic transfer of audit logs to the centralized server is supported by configuring the IP address of the central server (AD server) in REX640 through PCM600.

- d) The log file shall be protected from subsequent modification.

The log file is protected and set to read-only mode, preventing any modifications or deletion of events in REX640.

- e) Older entries shall be overwritten on the log file overflow. The system shall send an alert before the log storage runs out of space.

REX640 uses a ring buffer, where older log entries are automatically overwritten by new events when the buffer reaches its capacity. Alerts can be configured on the centralized log server based on the audit logs generated by REX640.

- f) It shall be possible to include security-related log messages in a pre-existing alarm management.

Security-related log messages are stored in REX640 and sent to the centralized audit server. Alarm management for these logs should be handled on the centralized log server.

## 4.6 Development

### 4.6.1 Secure Development Standards, Quality Management and Approval Processes

**ISO/IEC 27002:2013 / 27019:2017: 9.4.5, 14.2.2, 14.2.3, 14.2.4, 14.2.5, 14.2.6, 14.2.7, 14.2.8, 14.2.9, 14.3.1**

- a) The system shall be developed by reliable and professionally trained employees. Where the development or parts thereof are subcontracted to a third party, this requires written permission by the client. The subcontractor shall meet at least the same security requirements as the supplier.

ABB has a dedicated cyber security development team responsible for implementing cyber security for REX640 and PCM600. This team consists of highly trained and experienced professionals, including architects, developers, and testing experts. Both development and testing are conducted in-house at ABB.

- b) The supplier shall develop the system in line with recognized development standards and quality management/assurance processes. As part of the development process, the following security related development steps require special attention:

- Definition of the security requirements
- Threat modelling and risk analysis
- Deduction of requirements for system design and implementation
- Secure programming
- Requirement testing
- Security checks before commissioning

ABB adheres to the IEC 62443-4-1 secure development process, which incorporates secure architecture, secure requirements, secure development practices, security verification, security update management, validation, and security guidelines. ABB has [IEC62443 4-1 certification](#) obtained from Exida.

- c) Testing shall be subject to the dual control principle: Development and testing shall be carried out by different people. Testing plans and procedures as well as expected and actual test results shall to be

documented and comprehensible. It shall be ensured that they can be reviewed by the client as needed.

ABB has a dedicated team for development, product verification testing, and security testing. Test cases, procedures, and results are thoroughly validated and documented. Test specifications are continuously updated to address emerging threats. The ABB Device Security Assurance Center utilizes advanced security tools to conduct vulnerability testing.

- d) The supplier shall have a documented development security process in place that covers physical, organizational and personal security and protects the system's integrity and confidentiality. The effectiveness of the above-stated process may be verified by an external audit.

ABB has implemented a documented development security process, verified and certified by the third-party certification authority Exida. ABB has achieved [IEC 62443-4-1 maturity level 3 certification](#), indicating that security processes are standardized and consistently applied across the organization. This maturity level reflects a well-documented, organization-wide approach to product security, with proactive processes that include continuous monitoring and improvement.

- e) The supplier shall have a programming guideline in place that explicitly covers security-related requirements, e.g. avoiding insecure programming techniques and functions or the verification of input data to avoid buffer overflow errors. Where possible, security-enhancing compiler options and libraries shall be used.

ABB has standard coding guidelines, and it is followed for all the digital substation automation products to ensure the integrity and confidentiality of the products.

- f) The approval of the system resp. of updates/security patches needs to follow a specified and documented approval process.

ABB has guidelines for releasing the new firmware, and security patches for all the digital substation automation products which include PCM600 and REX640.

All Secure Development processes mentioned are supported, Please refer to the [IEC 62443-4-1 secure development process certification](#).

## 4.6.2 Secure Development and Testing Systems, Integrity Testing

### ISO/IEC 27002:2013 / 27019:2017: 9.4.5, 12.1.4, 14.2.7, 14.3.1

- a) Development shall take place on secure systems; the development environment, source code and binary data all shall be protected from external access. All development systems shall be hardened according to recognized state-of-the-art and best practice specifications. Up-to-date malware protection shall be employed on the systems and all the latest security patches shall be installed.

REX640 and PCM600 development is conducted on secure systems where the development environment, source code, and binary data are safeguarded from external access. These systems are hardened according to the latest best practices, with current malware protection and security patches applied.

- b) Development and testing of the system, updates, extensions and security patches shall take place in a testing environment that is separated from the productive system.

REX640 and PCM600 testing environment and Production system are maintained separately.

- c) No source code (except for interpreted scripting languages) shall be stored on productive systems.

REX640 and PCM600 Source codes are stored on a separate system and are not connected to the production environment.

- d) It shall be possible to check the integrity of source code and binary data for unauthorized changes, for example via secure checksums.

Integrity checks for REX640 firmware and PCM600 application coding are integral parts of the development process, protecting against unauthorized modifications.

- e) A version history that tracks any changes to the software shall be kept for all employed software.

The version history of REX640 and PCM600 is maintained, and all the coding changes are performed according to the secure coding standard, The changes are traceable.

## 4.7 Maintenance

### 4.7.1 Maintenance Process Requirements

**ISO/IEC 27002:2013 / 27019:2017: 9.1.2, 9.2.1, 9.2.2, 15.1.1, 15.1.2**

- a) Any remote and on-site access shall only be carried out by a predefined and properly trained group of people and only originating from secured systems. Access systems and IT infrastructures used for remote and on-site access need to be hardened according to recognized state-of-the-art standards and best practice specifications. Up-to-date malware protection shall be employed and all the latest security patches shall be installed.
- b) A pre-defined maintenance process shall be established to ensure that maintenance personnel only receives access to the systems, services and data as well as the respective physical premises that are actually required to carry out the related maintenance activities.
- c) Interactive remote access shall occur via personalized accounts and using two factor authentication. Special user IDs shall be established for automated processes – these shall only be able to execute specific functions and not have interactive access.
- d) Technical measures shall ensure that remote access is only possible if and where the responsible operator has explicitly approved this access. Each remote access session by external service providers shall require individual approval and disconnection. Sessions shall automatically disconnect after a reasonable amount of time. Access systems used for remote access, in particular, shall be logically or physically isolated from other networks during remote access. Here, a physical separation is preferable to logical uncoupling.

This is applicable for system-level requirements and managed by a system Integrator and asset owner.

### 4.7.2 Secure Update Processes

**ISO/IEC 27002:2013 / 27019:2017: 12.5.1, 14.2.2, 14.2.3, 14.2.7, 14.2.9**

The provision and installation of updates, extensions and patches needs to occur according to a defined process and in coordination with the client.

ABB technical support team assists with installing hot fixes and updating the firmware as needed. Additionally, the product release notes will provide detailed instructions for upgrading the firmware and applying hot fixes.

### **4.7.3 Configuration and Change Management, Rollback**

**ISO/IEC 27002:2013 / 27019:2017: 12.1.2, 12.5.1, 12.6.2, 12.9.1 ENR, 14.2.2, 14.2.9**

- a) The system shall be developed and operated with a configuration and change management in place.
- b) The system shall support rollback to a pre-defined number of configuration states.

The configuration and change management processes are supported by a scheduled backup mechanism in PCM600. However, rollback is not automated; users must manually restore configurations from backup files saved at different time points.

### **4.7.4 Handling of Vulnerabilities**

**ISO/IEC 27002:2013 / 27019:2017: 12.6.1, 16.1.2, 16.1.3**

The supplier shall have a documented vulnerability handling process in place. Within this process, all concerned – including external parties – shall be able to report actual or potential vulnerabilities. In addition, the supplier shall stay up-to-date on current security issues that might affect the system or individual components. The vulnerability handling process defines how and in what timeframe a known or reported vulnerability shall be reviewed, classified, remedied and reported to all affected clients, including respective recommended measures. When the supplier finds out about a vulnerability, he shall inform the client in a timely manner and under consideration of the necessary confidentiality restrictions, even when no patch to fix the issue is available yet.

This is supported. ABB has clearly defined vulnerability handling policy and it can be identified from [ABB's approach to software](#).

## **4.8 Data Back-Up and Emergency Planning**

### **4.8.1 Back-up: Concept, Method, Documentation, Testing**

#### **ISO/IEC 27002:2013 / 27019:2017: 12.1.1, 12.3.1**

Documented and tested procedures for data back-up and recovery of the individual components resp. the entire system and the respective configurations shall exist. There shall be the possibility for central back-up of the configuration parameters of distributed components.

After relevant system updates, the documentation and procedures shall be updated and retested accordingly.

The protection relay configuration can be backed up in two ways. An offline backup allows users to back up configurations individually for each relay or entire project configurations, including relay settings, entire project configurations, application configurations, communication files, and hardware configurations.

An online backup of the relay configuration can also be performed using PCM600. Additionally, users can schedule automatic backups by configuring the backup interval.

The Cyber Security Deployment Guidelines outline the backup and restore capabilities for PCM600 and REX640 in detail.

A factory restore can be performed to reset the relay to its initial configuration.

### **4.8.2 Emergency Concept and Recovery Plans**

#### **ISO/IEC 27002:2013 / 27019:2017: 17.1.1, 17.2.1**

The supplier shall provide documented and tested procedures and recovery plans – including expected restoration times – for relevant emergency and crisis scenarios. After relevant system updates, this documentation and these procedures shall be updated and retested as part of the approval process for release changes.

The protection relay configuration can be backed up in two ways. An offline backup allows users to back up configurations individually for each relay or entire project configurations, including relay settings, entire project configurations, application configurations, communication files, and hardware configurations.

An online backup of the relay configuration can also be performed using PCM600. Additionally, users can schedule automatic backups by configuring the backup interval.

The product guides for PCM600 and REX640 detail the backup and restore capabilities.

A factory restore can be performed to reset the relay to its initial configuration.



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

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