PRODUCT ADVISORY NOTE

Guidelines to Prevent Unauthorized Modifications of Firmware and Configuration ABB Digital Substation Products

Executive summary

This document provides guidelines with the aim to prevent unauthorized modifications to firmware and configuration files in ABB Relion protection relays and digital substation automation products. Protection relays are critical components in electrical power systems, ensuring the safe and reliable operation by monitoring and controlling electrical circuits. Unauthorized alterations to their firmware and configuration can lead to severe operational disruptions and safety hazards.

To mitigate these risks, the guidelines cover best practices, security measures, and procedural controls designed to safeguard these devices against unauthorized access and tampering. Key recommendations include implementing system hardening, strong authentication mechanisms, maintaining firmware integrity through implementing defense-in-depth security techniques, regularly auditing, and monitoring system activity, and establishing robust access control policies.

By adhering to these guidelines, asset owners can enhance the security and resilience of their protection relays and digital substation automation products, so they function correctly and continue to protect critical infrastructure from electrical faults and other anomalies.

Disclaimer

This advisory note provides important actions that the asset owners are strongly encouraged to implement for addressing specific cyber security weaknesses. However, while these actions are critical to enhancing the system security, they are not exhaustive and do not guarantee protection against all possible threats.

Cyber security is a continually evolving field, and comprehensive protection requires ongoing vigilance and multiple layers of defense. We recommend to regularly update systems, follow best practices, and stay informed about new security developments. It is the sole responsibility of the asset owner to provide and continuously ensure a secure connection between the product and the asset owner's network or any other network. The asset owner should establish and maintain any appropriate measures (including but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of anti-virus programs, etc.) to protect the product, the network, its system, and the interface against any kinds of security breach, unauthorized access, interference, intrusion, leakage and/or theft of data or information.

ABB and its affiliates are not liable for damage and/or losses related to such security breaches, unauthorized access, interference, intrusion, leakage, and/or theft of data or information.

1. Products concerned

Product	Description	Firmware version
Relion Protection Relays (refer to section 10, *List of applicable products*)	ABB Relion protection relays and merging units	All versions
REF542plus	Feeder terminal	All versions
SUE 3000	Bay protection and control terminal	All versions
SSC600	Centralized protection	All versions
RIO600	Remote I/O	All versions
COM600	Substation management unit	All versions
SPA ZC-400	Ethernet adapter	All versions
AR_600, REC/RER601/603, ARM600	Arctic Wireless Communication Solution	All versions

2. Effective date

October 21st, 2024

3. Reference documents

3.1. ABB documents

Doc ID	Title
1MRS758337	611 series Cyber Security Deployment Guideline
1MRS758280	615 series Cyber Security Deployment Guideline
2NGA000818	REX610 Cyber Security Deployment Guideline
2NGA001861	REX615 Cyber Security Deployment Guideline
1MRS759122	REX640 Cyber Security Deployment Guideline
1MRS757488	Remote I/O RIO600 Installation and Commissioning Manual
1MRS758410	Substation Merging Unit SMU615 Cyber Security Deployment Guideline
1MRS759013	SSC600 Cyber Security Deployment Guideline

Doc ID	Title
1MRS758294	620 series Cyber Security Deployment Guideline
1MRS756801	630 series Commissioning Manual
1MRS758440	PCM600 Cyber Security Deployment Guideline
1MRS758267	COM600 series 5.1 Cyber Security Deployment Guideline
1MRS758860	Arctic Cyber Security Deployment Guideline

3.2. Related CVE document

CVE-2024-8036 ABB Relion 611, 615, 620, 630 series, REX610, REX640, SMU615, SSC600, Arctic solution, COM600, SPA ZC-400, SUE3000: Guidelines to Prevent Unauthorized Modifications of Firmware and Configuration.

4. Introduction

Protecting Operational Technology (OT) assets, especially those involved in the production, transmission, and distribution of electricity, has become increasingly critical due to recent geopolitical developments. Emerging cyber security threats, such as state-sponsored actors, OT-aware malware toolkits, active ransomware groups, continuously discovered vulnerabilities, and the malicious use of Artificial Intelligence, underscore the importance of this subject.

ABB recognizes cyber security as a fundamental requirement and is dedicated to offering customers products, systems, and services that robustly address these concerns. Beyond new development it is equally important to safeguard existing installations from evolving threats.

4.1. Securing the OT Environment

As embedded systems continue to permeate various sectors, from consumer electronics to critical infrastructure such as power generation, transmission, and distribution systems, ensuring the security of firmware and configuration updates is becoming increasingly important. Firmware, serving as the foundational software governing hardware devices, holds privileged access to system resources, making it an attractive target for malicious actors.

Additionally, firmware updates through unencrypted communication channels can compromise the integrity and confidentiality of data of embedded devices. This paper dives into the opportunities to strengthen the firmware and configuration update security inherent in ABB digital substation products, assesses their potential impacts, and outlines effective cyber security strategies to mitigate these risks.

Widely acknowledged cyber security standards and publications, such as IEC 62443, NIST SP 800-82, and the BDEW white paper, provide valuable guidance on securing the OT environment. Below are ABB's recommendations for essential actions, summarized for convenience. This list is not exhaustive; for comprehensive information, refer to the respective standards and publications.

5. Description

In the last decades, the segregation of the substation network was considered as a suitable defense method against cyber-attacks. Nowadays, there is a paradigm shift towards a zero-trust mindset, with an expectation of the attacker's presence in the substation. Therefore, enhancing the protection of the substation network is essential to effectively mitigate cyber risks.

The firmware of the modern protection relays and centralized protection devices is equipped with support for digital signatures (refer to section 10, *List of applicable products*), which serve as a critical security feature to ensure the authenticity and integrity of the firmware. Digital signatures are cryptographic tools that validate that the firmware has not been altered or tampered with and that it originates from a trusted source.

5.1. Digital Signature Overview

Signing the firmware ensures its authenticity and integrity, verifying that it comes from a trusted source and has not been tampered with. It provides security by preventing unauthorized modifications, reducing the risk of malware or other malicious code being introduced.

5.1.1. Digital Signature Creation

When the firmware is developed and finalized, it is digitally signed using a private key held by ABB. This process generates a unique digital signature for the firmware file, provided that the device supports digital signatures. It is important to note that older versions of the Relion protection relays (refer to section 10, *List of applicable products*) do not support digital signatures. Therefore, this chapter applies only to protection relays with digital signature support.

5.1.2. Digital Signature Verification

The corresponding public key is used to verify the digital signature. If the firmware has been modified in any way, the verification process will fail, indicating potential tampering or corruption.

5.2. Verification Process in PCM600

5.2.1. Signature Verification

The PCM600, protection and control IED manager tool, used for configuring the Relion protection relays can verify the digital signatures. PCM600 checks the firmware against its digital signature to ensure it has not been altered and is from a legitimate source. Enabling this verification process is strongly recommended. It is done in the configuration settings of the PCM600 (In PCM600, click *Tools* → *Options* → *Security Settings* → *General tab* → *Security Level* and select "*High*"). The security level should only be set to a lower level in the case of updating legacy devices with non-signed firmware.

5.3. Verification Process in devices

5.3.1. Signature Verification

SSC600 and REX615 devices possess the capability to verify digital signatures embedded within firmware files, thereby ensuring the integrity of the firmware. Other products, using

digitally signed firmware, are relying on the signature verification performed with the PCM600 tool. Refer to the table in section 10, *List of applicable products*.

If digital signatures are not supported, the integrity and authenticity of the firmware cannot be verified. In this case, other layers of defense that are introduced in this document are crucial for securing the firmware updates.

6. Preventive measures for unauthorized modifications of firmware and configuration

6.1. Overview

To protect the substation from security risks, ABB strongly advises asset owners adhering to the outlined preventive measures for safeguarding firmware and configuration integrity. These measures strengthen security, mitigate risks, and ensure compliance with standards. By maintaining firmware integrity, data reliability is preserved, and tampering is prevented.

6.2. Access control

Administrator password and other privileged users' passwords pose a significant vulnerability in OT environments if not adequately managed. Default or weak privileged users' passwords can provide unauthorized access to critical systems, potentially leading to system compromise and operational disruption. Here are usual challenges associated with passwords and mitigation strategies to address them.

6.2.1. Default user credentials

When logging in with web-based human-machine interface (WHMI) or with PCM600, it is important to change the default credentials since they are often well-known and easily accessible, making them a prime target for attackers. Manufacturers do commonly use default passwords for ease of initial setup, but neglect to change those during commissioning pose a significant security risk to the respective OT environment.

6.2.2. Password re-use

While password re-use would increase usability, it is strongly recommended to refrain from doing this. Trying exposed passwords in other system components is a well-known attack method. Define unique passwords per protection relay and especially avoid using privileged passwords (e.g., administrator and engineer users' passwords) in other purpose for which they are intended to. For example, do not re-use administrator or engineer users' passwords as Manufacturing Message Specification (MMS) service's password.

6.2.3. Password complexity

It is recommended to avoid short or otherwise weak (e.g., common, or easily guessable) passwords. Further, it is advised to add special characters to the passwords for increased complexity. Please refer to the Cyber Security Deployment Guideline document or user manual of the product for details on password complexity.

6.2.4. Role-based access control and least privilege principle

We encourage to define access policies based on the least privilege principle, so that each user has only the necessary permissions for their roles. Further, it is advised to periodically

assess user privileges, especially during role changes. Where supported, use individual user credentials to ensure accountability and non-repudiation.

6.3. Network security

The following sections describe methods how to improve network security. Some of the suggested network security controls are made by using external devices, such as network switches, firewalls, or Supervisory Control and Data Acquisition (SCADA) server configuration.

6.3.1. Restricting PCM600 engineering and configuration access to the front port

The relay front port is designated solely for engineering and configuration purposes and can only be used for point-to-point configuration access with PCM600 or WHMI. To minimize the security risk, we advise using the front port for engineering and configuration access and not connecting the front port to any Ethernet network.

All physical ports dedicated to station bus communication can be enabled or disabled in the relay configuration. Unused physical ports to be closed. Refer to the user documentation of the product for more information.

Port ID	Type	Default state	Description
X1...X3	RJ-45 or fiber optic	Open	Ethernet station bus
X5	RS-485	Closed	Serial station bus
X6	RS-232/RS-485	Closed	Serial station bus
X9	ST serial	Closed	Serial station bus
X12	ST serial	Closed	Serial station bus
X16	Fiber-optic Ethernet	Open	Line Differential
Front port	RJ-45	Open	LHMI service access

Table-1 Example of physical ports on relay's communication card

6.3.2. IP protocol suite-based protocols and ports used

Internet Protocol (IP) suite's port security depends on specific installation, requirements, and existing infrastructure. The required external network equipment can be separate devices or devices that combine firewall, router, and secure VPN functionality. When the network is divided into security zones, it is done with substation devices having firewall functionality or with dedicated firewall products.

The relay may support an option with multiple station communication Ethernet ports. In this case, all ports use the same IP and Media Access Control (MAC) addresses regardless of what redundancy option is activated in the relay configuration. To set up an IP firewall the following example table summarizes the IP-ports used by the device. Only the necessary ports should be opened in the configuration. Ports that are open by default are used for configuring the protection relay.

Port number	Type	Default state	Description
20, 21	TCP	Open	File Transfer protocol (FTP and FTPS)
102	TCP	Open	IEC 61850
80	TCP	Closed	Web Server HTTP
443	TCP	Closed	Web Server HTTPS
123	UDP	Not active	Simple Network Time Protocol
502	TCP	Closed	Modbus TCP
20000	TCP	Closed	DNP TCP
20000	UDP	Closed	DNP UDP

Table-2 Example of IP protocol suite port listing

6.3.3. Secure communication

Secure communication is implemented according to the principles of IEC 62351 for WHMI and file transfer. If the Secure Communication parameter is activated in the relay, protocols require TLS protocol-based encryption method support from the clients. In this case the WHMI must be connected by a Web browser using the Hyper Text Transfer Protocol Secure (HTTPS) protocol. In the case of file transfer, the client must use File Transfer Protocol Secure (FTPS).

In addition to providing safe configuration and firmware transfer, the secure communication also protects against capturing passwords from legitimate users' authentications while logging in to the protection relay. For avoiding already exposed passwords, it is recommended to change the passwords after the secure communication has been taken into use.

Older OT devices may lack secure communication protocols, which means that other defenses must be deployed. Such defenses could include:

- Restricting access to the communication ports with a firewall (80 for HTTP, 20,21 for FTP, 102 for MMS)
- Allowing the traffic only from/to hosts necessary for the task by firewall rules
- Segregating networks into smaller communication zones
- Monitoring the traffic for unexpected activities by using an Intrusion Detection System (IDS)

6.3.3.1. Secure Configuration and WHMI

If supported by the protection relay, verify that the "secure communication" parameter is enabled (default setting). It can be accessed via the following HMI paths:
HMI path *Main menu / Configuration / Communication / Protocols / Network1*
HMI path *Main menu / Configuration / Communication / Protocols / Network2*
HMI path *Main menu / Configuration / Communication / Protocols / HMI Port*

Enabling this configuration parameter enforces the use of secure variants of the communication protocols: HTTPS, used with WHMI and FTPS, used in configuration with ABB PCM600 configuration tool. It is recommended to change passwords when the secure communication is enabled. This will ensure that possibly previously exposed passwords cannot be used.

6.3.3.2. Communication between PCM600 and Protection relay

PCM600 configuration tool communicates with Relion protection relays using different protocols depending on the relay version. Older versions of the protection relays support MMS

and FTP protocols, both of which are unencrypted. Newer versions of the protection relays support both FTP and FTPS, with FTPS providing a secure communication option.

PCM600 tool supports FTPS and can download and upload configuration files in encrypted format to/from the relay. The Secure Communication parameter is enabled by default. It can be accessed via HMI path *Main menu / Configuration / Authorization / Security*. It is recommended to change passwords when the secure communication is enabled. This will ensure that possibly previously exposed passwords cannot be used.

FTPS offers robust security features, including encryption, data integrity, and authentication, making it a preferred choice for secure file transfer operations. By leveraging FTPS, Asset owners can protect sensitive data, and maintain the confidentiality and integrity of their configuration file transfer process.

6.3.3.3. SCADA communication protocols

If supported by the protection relay and respectively by the SCADA system, enabling the secure variants of SCADA communication protocols (i.e., secure IEC 60870-5-104 and secure DNP 3.0) enhances cyber security by creating an end-to-end secured channel for SCADA traffic.

For systems that do not support secure SCADA communication protocols, other defenses should be deployed. Such defenses could include:

- Limiting the attack surface (see section 6.4, *Limiting the attack surface*)
- Restricting access to the communication ports (2404 for IEC 104, 20000 for DNP 3.0) with a firewall
- Allowing the traffic only from necessary hosts' IP addresses and MAC addresses by firewall rules
- Defining the SCADA IP address as allowed client address in protection relays that are supporting it
- Using a VPN tunnel between the area supervisory control network (SCADA) and field network/basic control network (i.e. between protection relays and control room).

6.3.4. Preventive Measures for Unencrypted Protocols

Before delving into the preventive measures for unencrypted communication protocols like MMS and FTP, it is essential to understand the protocols' fundamental nature. MMS (Manufacturing Message Specification) and FTP (File Transfer Protocol) are both communication protocols used for data exchange between PCM600 and Protection relays. Additionally, MMS communication facilitates data exchange between protection relays and SCADA system. Please refer to the details of FTP and MMS.

6.3.5. Understanding MMS and FTP

MMS (Manufacturing Message Specification)
The MMS lacks inherent encryption and robust authentication mechanisms, making it vulnerable to interception and unauthorized access.

FTP (File Transfer Protocol)
FTP transmits data, including user credentials, in plaintext, posing a significant security risk as it can be intercepted and exploited by malicious actors.

FTPS (File Transfer Protocol Secure)

FTPS transmits data in encrypted form, providing a safe channel for sensitive information. Using FTPS instead of FTP, customers can ensure the secure and reliable transfer of sensitive data, protection against unauthorized access, and meet regulatory requirements.

To mitigate the inherent security risks associated with MMS and FTP, it is crucial to implement preventive measures.

If FTPS is supported in the protection relay
It is recommended to enable FTPS to ensure secure communication between PCM600 and protection relays. In addition, disable MMS, and FTP on protection relays and PCM600 where possible to prevent their use.

If FTPS is not supported in the protection relay
If secure communication via FTPS is not supported in the protection relay (refer to section 10, *List of applicable products*), it is advisable to implement preventive measures within the substation network. This involves configuring essential security settings on the Ethernet switch and Firewall to enhance protection.

Please refer to section 6.3.3 *Secure communication* for further defenses and to the next chapter for recommendation of access control lists (ACLs) or firewall rules to secure FTP communication through network devices.

6.3.6. Access Control Lists (ACLs):

An access control list (ACL) is a set of rules configured on a network device, such as a router or switch, to control the flow of traffic based on specified criteria. These criteria typically include source and destination IP addresses, ports, and protocols. ACLs can permit or deny traffic based on these criteria, providing a basic level of security by regulating access to network resources.

Identify the source and destination IP addresses or ranges associated with FTP communication, such as PCM600 and the list of installed protection relay IP addresses.
Configure ACL entries to either allow or block FTP traffic according to the identified criteria. Then, apply the ACL to the relevant switch interfaces. However, note that these steps do not include specific details on configuring ACLs in the switch. Please consult your network administrator to undertake the ACL configuration based on the installed network devices.

Firewalls operate at the network boundary and enforce security policies by controlling the flow of traffic between networks. Configure firewall rules to permit or deny FTP traffic based on specified criteria, such as source/destination IP addresses, ports, or protocols. Specify whether to allow or block FTP traffic and apply the rules to the appropriate firewall interfaces or zones.

Logging: Enable logging for denied FTP traffic to monitor and investigate potential security incidents.

By implementing IP-based ACLs or firewall rules to restrict TCP-based FTP traffic, organizations can prevent unauthorized access and protect sensitive data from interception or exploitation. These measures contribute to strengthening network security and mitigating the risks associated with FTP communication.

6.4. Limiting the attack surface

The aim for limiting the attack surface is two-fold. First, it is to reduce the probability for breaking into the system and second, to limit the attacker's lateral movement in the system in case of a successful attack. In OT systems, the attack surface can be reduced e.g., by reducing the number of entry points, applying access controls, filtering/inspecting protocols, minimizing configuration options and hardening system components.

6.4.1. Network isolation and zoning

Dividing an OT network into smaller zones is decreasing the attack surface. If an asset would be compromised, the attacker would have limited possibilities for further lateral movement in a segmented network. Zoning means grouping assets with similar cyber security requirements into the same zone. Zones would be separated by firewalls, limiting the traffic flow (i.e., conduits) between the zones.

The OT system should be isolated by firewall from other systems (e.g., office network and surveillance network) and from the internet.

The firewall configuration should be performed by "whitelisting" principle, i.e., explicitly allowing only the required ports and protocols and categorically blocking any other traffic.

Local switches can limit the traffic by dividing the network into different Virtual Local Area Networks (VLANs) and use Media Access Control (MAC) address filtering. This will further isolate the network and prevent or delay attackers' lateral movement.

It is a good practice to limit the exposure of the PCs (e.g., laptops) running configurator tools. If dedicated PCs are not an option, it is recommended to investigate PCs by running full virus scan with recently updated signature files before introducing the respective PC to the OT environment.

Restricting physical access to the site limits the exposure of the OT network to potential attackers. Physical access controls may include perimeter fencing, locking, electronic surveillance and personnel identification and access control. Refer to section 6.5 *Physical security* for more information.

6.4.2. Configuring devices and updating firmware

When the "Secure communication" is enabled in the devices that are supporting it, the configuration and firmware transfer to the device are secured. Care should be taken to store the configurations as backup files into a secure place, with access to them allowed on role-basis.

With devices that are not supporting secure communication, an additional defense-in-depth method would be to perform the configuration locally, by connecting the PC running the configurator tool directly to the configured device (e.g., to the front port of a protection relay). This method secures the transferred configuration from man-in-the-middle attack and protects user credentials.

While it is good practice to use the latest firmware versions in the OT devices, there may be situations where it is not possible (e.g., because of uptime requirements). Such a risk should be assessed by e.g., examining the firmware release notes. In this case, based on the assessed risk level, other mitigations and defense mechanisms described in this document can be considered.

We strongly recommend protecting PCs running configurator tools with anti-malware suites with recent updates of signature files. The latest versions of PCM600 configurator tool, connection packages and hotfixes are recommended. Any data, such as device configurations and firmware update files transferred to the OT environment should be virus scanned prior to transferring.

6.4.3. Remote connections

Remote connections are an attack vector to OT systems as the traffic is typically routed through the internet. Consider using a well-known Virtual Private Network (VPN) solution, which is frequently patched. It is not recommended to have direct remote connection to IED from untrusted network. The remote connections should terminate to OT Demilitarized Zone (OT DMZ), which would be segregated from other networks by firewalls.

6.5. Physical security

Ensuring the physical security of protection relays in control rooms is crucial for safeguarding the integrity and reliability of electrical power systems. Any unauthorized access or physical tampering can lead to operational disruptions and safety hazards. Here are recommended physical protection measures for protection relays in electrical substations.

6.5.1. Controlled Entry

Implement access control mechanisms, such as keycard systems, biometric scanners, or PIN (Personal Identification Number) codes, to restrict entry to control rooms.

6.5.2. Authorization Levels

Establish various levels of access authorization to ensure only qualified personnel have access to critical equipment.

6.5.3. Secure Enclosures

If allowed by safety protocols, house protection relays in locked cabinets or enclosures, providing an additional layer of security.

6.5.4. Alarm Systems

Install alarm systems that trigger alerts in the event of unauthorized entry or tampering.

6.5.5. Logging Mechanisms

Implement access logging mechanisms to record entry and exit of personnel in the substation or control room.

6.5.6. Regular Audits

Conduct regular audits of access logs to identify and investigate any unusual or unauthorized access attempts.

6.5.7. Personnel Training

Train staff on security protocols and the importance of physical security measures.
Ensure personnel are familiar with emergency procedures and response plans in case of a security incident.

6.5.8. Importance of Physical Security

By implementing these physical security measures, organizations can significantly reduce the risk of unauthorized access and tampering with protection relays. This ensures the reliability and safety of the electrical power system.

6.6. Patch Management

We advise to regularly update PCM600 software and if possible, also relay firmware to the latest versions, ensuring that security patches and enhancements are applied. Supporting systems, such as PCs used for configuration should also be regularly updated. Asset lists can be used to assist the patch management process.

6.7. System hardening

It is important to utilize the defense-in-depth concept when designing automation system security. It is not recommended to connect any device directly to the Internet without adequate additional security components. The different layers and interfaces in the system should use security controls. Robust security means, besides product features, enabling and using the available features and enforcing their use by company policies. Adequate training is also needed for the personnel accessing and using the system.

It is recommended that the following general hardening guidelines are considered when planning system protection.

- Recognizing and familiarizing all parts of the system and the system's communication links and removing all unnecessary communication links in the system
- Rating the security level of remaining connections and improving with applicable methods
- Hardening the system by removing or deactivating all unused processes, communication ports and services
- Checking that the entire system has backups available from all applicable parts
- Collecting and storing backups of the system components and keeping those up to date
- Removing all unnecessary user accounts
- Defining password policies
- Changing default passwords and using strong passwords
- Checking that the link from substation to upper-level system uses strong encryption and authentication
- Segregating public network (untrusted) from automation networks (trusted)
- Segmenting traffic and networks
- Using firewalls and demilitarized zones
- Assessing the system periodically
- Using malware protection in workstations and keeping those up to date

7. Restoring the functionality

In case of suspected cyber-attack, inspect the suspected devices for abnormal functionality, inspect their log files and inspect the network devices' (such as routers and firewalls) log files as well. Additionally, consider using network monitoring tools to analyze traffic patterns. Look for anomalies such as unexpected connections, unusually high data transfer rates, or communication with abnormal IP addresses. It is worth considering hiring an external consultant for leading the investigation.

If there is an indication that a product's configuration is compromised, the fast and efficient recovery is relying on up-to-date configuration backups. The product is first restored into factory settings and then previously backed-up configuration is uploaded into the device.

7.1. Procedures for restoring factory settings

The procedures for restoring the factory default settings are differing based on the product. Generally, the instructions are described in the Operation Manual, User Manual or Installation and Configuration Manual. See the following link for user documentation in ABB library (*Category / ABB Products / Medium Voltage Products and Systems*): https://library.abb.com/

If not being able to find necessary information or having problems in restoring factory settings, please contact ABB Technical Support. The following page lists ABB contact centers globally: https://new.abb.com/contact-centers

8. Summary

As the threat landscape continues to evolve, securing OT environments in the energy sector becomes increasingly critical. This white paper has outlined best practices and recommendations for enhancing cyber security measures.

By adopting these practices, asset owners can significantly reduce the risk of cyber threats, ensuring the integrity, availability, and confidentiality of their critical infrastructure. Proactive measures such as secure communication, stringent authentication policies, network isolation, firmware security are essential components of a robust cyber security strategy.

By prioritizing these actions, asset owners can protect their assets, safeguard operational continuity, and contribute to the overall security of the energy sector.

9. Summary of Preventive measures

The following checklist of preventive measures summarizes the suggested controls and explains the defense in depth mechanism, example control and type of threat that can be mitigated. ABB recommends implementing the controls as mentioned in the table below.

SL.NO	Defense in depth mechanism	Subject	Example Control	Threat addressed
1.	Account management controls	Default user credentials	• Change the default credentials into non-defaults	Enlarged attack surfaces, unauthorized access to the system
2.	Account management controls	Password reuse	• Do not re-use passwords within the system ○ E.g., Do not configure Administrator or Engineer user password as the MMS service password	Enlarged attack surfaces, unauthorized access to the system
3.	Account management controls	Administrator password	• Use Administrator or another privileged user's password only when required by the task	Enlarged attack surfaces, unauthorized access to the system

4.	Account management controls	Password complexity	• Use complex passwords with special characters • Avoid common or easily guessable passwords	Enlarged attack surfaces, unauthorized access to the system
5.	Account management controls	Role-based access control and least privilege principle	• When supported by the device, define access policies based on the least privilege principle, ensuring each user has only the necessary permissions for their roles	Enlarged attack surfaces, unauthorized access to the system
6.	Account management controls	Local HMI password	• Enable the local HMI password, if supported by the device and if allowed by safety practices	Enlarged attack surfaces, unauthorized access to the system
7.	Network controls	Secure communication	• Enable "Secure Communication" parameter, if supported by the device o It can be accessed via following HMI paths: HMI path *Main menu/Configuration/Communication/Protocols/Network1* HMI path *Main menu/Configuration/Communication/Protocols/Network2* HMI path *Main menu/Configuration/Communication/Protocols/HMI Port*	Eavesdropping or tampering of data in transit
8.	Network controls	Secure communication	For relays that do not support "Secure Communication", consider the following controls: • Restrict access to the communication ports (80/HTTP, 20,21/FTP, 102/MMS) with a firewall • Allow the traffic by firewall rules only from/to hosts necessary for the task • Segregate networks into smaller communication zones • Monitor the traffic for unexpected activities by using an Intrusion Detection System (IDS) • If possible, connect the engineering PC directly to the relay when updating the configuration or firmware	Eavesdropping or tampering of data in transit
9.	Network controls	Secure communication	• Verify that PCM600 is using secure communication (HMI path *Main menu/Configuration/Authorization/Security*)	Eavesdropping or tampering of data in transit
10.	Network controls	Secure SCADA	If secure protocol variants are supported by the protection relay and SCADA system:	Eavesdropping or tampering of

		communication	• Enable secure variants of IEC 60870-5-104 or DNP 3.0	data in transit
11.	Network controls	Secure SCADA communication	If secure SCADA communication protocols are not supported, consider the following controls: • Limit the attack surface (see section 6.4 *Limiting the attack surface*) • Restrict access to the communication ports (2404/IEC 104, 20000/DNP 3.0, 502/Modbus) with a firewall • Allow the traffic only from necessary hosts' IP addresses and MAC (Medium Access Control) addresses by firewall/switch rules • Define the SCADA IP address as allowed client address in relays that are supporting it • Use a VPN tunnel between the area supervisory control network (SCADA) and field network/basic control network (protection relays and centralized protection)	Eavesdropping or tampering of data in transit
12.	Network controls	Isolation	• Close unused physical ports in the relay • Open only the necessary IP protocol suite's ports in the relay's configuration • If possible, restrict configuration and engineering to front port only	Enlarged attack surfaces, unauthorized access to the system
13.	Network controls	Isolation	• Isolate the OT system by firewall from other systems (e.g., office network and surveillance network) and from the internet ○ It is not recommended to connect any device directly to the Internet without adequate additional security components • Limit the station traffic by dividing the network into different VLANs • Use Access Control Lists in switches for limiting the traffic (by source/destination IP addresses and port numbers) • Use MAC address filtering • If possible, use dedicated site PCs for upgrading and engineering purposes	Enlarged attack surfaces, unauthorized access to the system
14.	Network controls	Zoning	• Divide an OT network into smaller zones with a firewall restricting traffic between the zones • Perform firewall configuration by "white-listing" principle, i.e., explicitly allowing only the required ports and protocols and blocking any other traffic • Use OT DMZ for terminating any connections from outside the OT network	Enlarged attack surfaces, unauthorized access to the system
15.	Hardware and software controls	Hardening	• Recognize and familiarize all parts of the system and the system's communication links • Remove all unnecessary communication links in the system	Enlarged attack surfaces, unauthorized access to the system

			• Rate the security level of remaining connections and improve them with applicable methods • Remove or deactivate all unused processes, communication ports and services • Remove all unnecessary user accounts • Define password policies • Check that the link from substation to upper-level system uses strong encryption and authentication	
16.	Hardware and software controls	Anti-malware	• Verify that anti-malware solution is installed to all PCs and updated frequently • Investigate PCs by running full virus scan with recently updated signature files before introducing the PC to the OT environment • Run virus scan to all data, such as device configurations and firmware update files, transferred to the OT environment	Enlarged attack surfaces, unauthorized access to the system
17.	Hardware and software controls	Updates and upgrades	We advise to regularly update PCM600 software, connection packages, hotfixes, and relay firmware to the latest versions, ensuring that security patches and enhancements are applied. • While it is good practice to use the latest firmware versions in the OT devices, there may be situations where it is not possible (e.g., because of uptime requirements) • Such a risk should be assessed by e.g., examining the firmware release notes. In this case, based on the assessed risk level, consider other mitigations and defense mechanisms and controls described in this document • If supported by the product, the firmware can be upgraded to a newer version, introducing new cyber security features • Consider upgrading old devices to new ones, having improved cyber security features • With signed firmware upgrade, verify that the PCM600 is checking the digital signature by clicking *Tools* / *Options* / *Security Settings* / *General tab* / *Security Level* and selecting "*High*" o The security level should only be set to a lower level in case of updating legacy devices with non-signed firmware • Supporting systems, such as PCs used for configuration should also be regularly updated	Enlarged attack surfaces, unauthorized access to the system

18.	Hardware and software controls	Remote connections	Remote connections are an attack vector to the OT system as the traffic is typically routed through the internet. • Use a well-known Virtual Private Network (VPN) solution, which is frequently patched • It is not recommended to have direct remote connection to IED from untrusted network • The remote connections should terminate to OT Demilitarized Zone (OT DMZ), which would be segregated from other networks by firewalls	Enlarged attack surfaces, unauthorized access to the system
19.	Physical controls	Physical access	Restrict physical access to the sites. It limits the exposure of the OT network to potential attackers. Physical controls may include: • Perimeter fencing • Locking, personnel identification, and access control (use keycard systems, biometric scanners, or PIN (Personal Identification Number) codes, to restrict entry) • Implementing access logging mechanisms to record entry and exit of personnel and auditing logs frequently • Establishing various levels of access authorization • Using electronic surveillance ○ Install alarm systems that trigger alerts in case of unauthorized entry or tampering • If allowed by safety protocols, housing protection relays in locked cabinets or enclosures • Training of staff on security protocols and the importance of physical security measures • Creating emergency procedures and response plans in case of a security incident	Enlarged attack surfaces, unauthorized access to the system
20.	Policies and procedures	Secure use	• Follow cyber security best practices for installation, operation, and decommissioning described in the Cyber Security Deployment Guideline or user manual of the product	Enlarged attack surfaces, unauthorized access to the system
21.	Policies and procedures	Periodical reviews	• Assess the whole system's cyber security posture periodically • Review the role-based access controls periodically	Enlarged attack surfaces, unauthorized access to the system
22.	Policies and procedures	Vulnerabilities	• Follow vulnerabilities in ABB products. See ABB cyber security alerts and notifications page: **https://global.abb/group/en/technology/cyber-security/alerts-and-notifications** • Report vulnerabilities to ABB: **cybersecurity@ch.abb.com**	Unnoticed vulnerabilities in systems and products

23.	Policies and procedures	Backup and restore	• Introduce a backup Policy, which will ensure periodical backups and backup revision numbering • Check that the entire system has backups available from all applicable parts • Create regular backup from the protection relay and Create Project backup using PCM600 • Store the backups in a safe place, restricted by role-based access control mechanisms • Ensure the security of the configuration PCs that may have local copies of configurations	Unauthorized tampering of configuration files and databases, denial of service

Table-3 Summary of preventive measures

10. List of applicable products

The preventive measures apply to the products mentioned in the following sections.

10.1. Relays and digital substation automation products

Product	Versions	Supports secure communication	Checks FW signature
RE_611 IEC	1.0	No	No
RE_611 IEC	2.0	Yes	No
REX610	1.0, 1.1, 1.2	Yes	No
REF615 IEC	1.0, 1.1	No	No
REF615 ANSI	1.0, 1.1	No	No
REF615R ANSI	4.0, 4.0 FP1	No	No
RED615 IEC	1.1	No	No
615 series IEC	2.0, 3.0, 4.0, 4.0 FP1	No	No
615 series IEC	5.0, 5.0 FP1	Yes	No
615 series CN	2.0, 3.0, 3.1, 4.0 FP1	No	No
615 series CN	5.0 FP1	Yes	No
615 series ANSI	2.0, 4.0, 4.0 FP1, 4.0 FP2	No	No
615 series ANSI	5.0 FP1	Yes	No
RER615	1.0, 1.1	No	No

Product	Versions	Supports secure communication	Checks FW signature
RER615	2.0	Yes	No
REC615	1.0, 1.1	No	No
REC615	2.0	Yes	No
SMU615	1.0	Yes	No
RBX615	1.0, 2.0	No	No
REX615	PCL1	Yes	Yes
RER620 ANSI	1.0, 1.1, 1.2, 1.3	No	No
620 series ANSI	2.0, 2.0 FP1	No	No
620 series IEC/CN	2.0	No	No
620 series IEC/CN	2.0 FP1	Yes	No
RE_630	1.0, 1.1, 1.2, 1.3	No	No
REX640	PCL1, PCL2, PCL3, PCL4	Yes	No
SSC600	1.0, 1.0 FP1, 1.0 FP2, 1.0 FP3, 1.0 FP4	Yes	Yes
RIO600	1.0, 1.1, 1.2, 1.5, 1.6, 1.7, 1.8	No	No
COM600	3.3, 3.4, 3.5, 4.0, 4.1, 5.0, 5.1	No	No
COM600F ANSI	4.1, 5.0	No	No
SPA ZC-400	All	No	No
SPA ZC-402	All	No	No
REF542plus	R1.0, R1.1, R2.0, R2.5, R2.5 ATEX, R2.5 SP3, R2.6, R3.0, R3.0 SP1, R3.0 SP3	No	No
SUE 3000	2.6 V4F07x, 3.0FP1 V4F11x, V4D02x, V4E0xx	No	No

Table-4 List of applicable products

10.2. Arctic Wireless Product Family

Product	Versions	Secure Configuration (HTTPS, SSH)	Uses encrypted firmware	Checks FW signature
ARG600				
ARG600A1220NA	3.0.1…3.4.13	Yes	Yes	No
ARG600A1230NA	3.0.1…3.4.13	Yes	Yes	No
ARG600A1240NA	3.0.1…3.4.13	Yes	Yes	No
ARG600A1260NA	3.0.1…3.4.13	Yes	Yes	No
ARG600A2622NA	2.0.10…3.4.13	Yes	Yes	No
ARG600A2625NA	2.0.10…3.4.13	Yes	Yes	No
ARP600				
ARP600A2200NA	3.0.1…3.4.13	Yes	Yes	No
ARP600A2220NA	3.0.1…3.4.13	Yes	Yes	No
ARP600A2250NA	3.0.1…3.4.13	Yes	Yes	No
ARP600A2260NA	3.0.1…3.4.13	Yes	Yes	No
ARP600A2651NA	2.0.10…3.4.13	Yes	Yes	No
ARP600A2560NA	2.0.10…3.4.13	Yes	Yes	No
ARR600				
ARR600A3201NA	3.0.1…3.4.13	Yes	Yes	No
ARR600A3202NA	3.0.1…3.4.13	Yes	Yes	No
ARR600A3221NA	3.0.1…3.4.13	Yes	Yes	No
ARR600A3222NA	3.0.1…3.4.13	Yes	Yes	No
ARR600A3251NA	3.0.1…3.4.13	Yes	Yes	No
ARR600A3252NA	3.0.1…3.4.13	Yes	Yes	No
ARR600A3261NA	3.0.1…3.4.13	Yes	Yes	No
ARR600A3262NA	3.0.1…3.4.13	Yes		
ARC600				
ARC600A2325NA	3.0.1…3.4.13	Yes	Yes	No
ARC600A2323NA	3.0.1…3.4.13	Yes	Yes	No
ARC600A2324NA	3.0.1…3.4.13	Yes	Yes	No
ARM600				
ARM600A2500NA	4.1.2…5.0.3	Yes	No	No
ARM600B2500NA	4.1.2…5.0.3	Yes	No	No
ARM600C2500NA	4.1.2…5.0.3	Yes	No	No
ARM600A2505NA	4.1.2…5.0.3	Yes	No	No
ARM600B2505NA	4.1.2…5.0.3	Yes	No	No

Product	Versions	Secure Configuration (HTTPS, SSH)	Uses encrypted firmware	Checks FW signature
ARM600C2505NA	4.1.2…5.0.3	Yes	No	No
ARM600SW				
ARM600SW1A1	5.0.1…5.0.3	Yes	No	No
ARM600SW2A3	5.0.1…5.0.3	Yes	No	No
ARM600SW3A3	5.0.1…5.0.3	Yes	No	No
REC601/603				
REC601	1.1	No	No	No
REC601	1.2	No	No	No
REC603	1.1	No	No	No
REC603	1.2	No	No	No

Table-5 List of applicable wireless products

11. Glossary

Access control Protection of system resources against unauthorized access

ACL Access Control List

Authenticate Verify the identity of a user, user device or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an information system, or to establish the validity of a transmission

Authentication A security measure designed to establish the validity of a transmission, message, or originator or a means of verifying an individual's authorization to receive specific categories of information

Authorization Right or permission that is granted to a system entity to access a system resource

Compromise Unauthorized disclosure, modification, substitution, or use of information

Conduits Conduits group the elements that allow communication between two zones

Confidentiality Assurance that information is not disclosed to unauthorized individuals, processes, or devices

DMZ Demilitarized zone is a dedicated network, which is used as an additional layer of security between company's other networks and untrusted networks, such as the internet. It is separated from internal and external networks by firewalls.

DNP A distributed network protocol originally developed by Westronic. The DNP3 Users Group has ownership of the protocol and assumes responsibility for its evolution

Ethernet	A standard for connecting a family of frame-based computer networking technologies into a LAN
Firewall	A network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules
FTP	File transfer protocol
FTPS	Secure file transfer protocol is a network protocol that provides file access, file transfer, and file management over any reliable data stream
Hardening	The process of securing a system by reducing its surface of vulnerability
HMI	Human–machine interface
HTTP	Hypertext transfer protocol is an application protocol for distributed, collaborative, hypermedia information systems
HTTPS	Also called HTTP over TLS, HTTP over SSL, and HTTP Secure, is a protocol for secure communication over a computer network that is widely used on the internet
IDS	Intrusion detection system
IEC 61850	International standard for substation communication and modeling
IEC 61850-8-1	A communication protocol based on the IEC 61850 standard series
IEC 61850-9-2	A communication protocol based on the IEC 61850 standard series
IEC 61850-9-2	Lite Edition of IEC 61850-9-2 offering process bus interface
IEC104	IEC 60870-5-104 Network access for IEC 60870-5-101
IED	Intelligent electronic devices
Integrity	Quality of a system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data
IP	Internet Protocol
LHMI	Local human-machine interface
LAN	Local area network
MAC	Media access control
MMS	Manufacturing message specification
Modbus	Modbus is a client/server data communication protocol.
OT	Operational technology
PCM600	PCM600 Protection and control IED manager
RIO600	Remote I/O unit
SCADA	Supervisory control and data acquisition
SSH	Secure shell is a cryptographic (encrypted) network protocol to allow remote login and other network services to operate securely over an unencrypted network

TCP	Transmission control protocol
TCP/IP	Transmission control protocol/Internet protocol
TLS	Transport Layer Security and its predecessor SSL are cryptographic protocols designed to provide communications security over a computer network (privacy and data integrity between two communicating computer applications)
UDP	User datagram protocol used for message broadcast or multicast
VLAN	Virtual local area network. Any broadcast domain that is partitioned and isolated in a computer network at the data link layer
VPN	Virtual Private Network
WHMI	The Integrated web-based human-machine interface in the protection relay and other embedded devices
Zone	A zone is defined as a grouping of logical or physical assets that share common security requirements based on factors such as criticality and consequence

12. Revision history

Rev. Ind.	Rev. date	Page / Chapter	Department	Change description
A	2024-10-21	all	ELDS	Initial version

ABB Distribution Solutions
Digital Substation Products
P.O. Box 699
FI-65101 VAASA, Finland
Phone +358 10 22 11

www.abb.com/mediumvoltage
www.abb.com/relion
www.abb.com/substationautomation
www.abb.com/mediumvoltage

Trademarks

Document ID: 2NGA002288

Revision: A Public

Security level: Public

Status: Approved