Harmony HMI/iPC

Cybersecurity Guide

EIO0000004948.01
01/2024

www.se.com

Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this document are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owner.

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof.

Table of Contents

Safety Information

Important Information

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result** in minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

Please Note

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

About the Book

Document Scope

The Cybersecurity Guide defines the elements that help you configure a system that is less susceptible to cyber attacks.

NOTE: The term security is used throughout this document in reference to cybersecurity topics.

Validity Note

This documentation is valid for Harmony Human Machine Interface (HMI) and industrial PC (iPC) products.

The characteristics of the products described in this document are intended to match the characteristics that are available on www.se.com. As part of our corporate strategy for constant improvement, we may revise the content over time to enhance clarity and accuracy. If you see a difference between the characteristics in this document and the characteristics on www.se.com, consider www.se.com to contain the latest information.

Registered Trademarks

Microsoft® and Windows® are registered trademarks of Microsoft Corporation in the United States and/or other countries.

Product names used in this manual may be the registered trademarks owned by the respective proprietors.

Related Documents

You can download the technical publications and other technical information from the Schneider Electric download center (www.se.com/ww/en/download).

Information on Non-Inclusive or Insensitive Terminology

As a responsible, inclusive company, Schneider Electric is constantly updating its communications and products that contain non-inclusive or insensitive terminology. However, despite these efforts, our content may still contain terms that are deemed inappropriate by some customers.

Introduction

Cybersecurity is intended to help protect your communication network and all equipment connected to it from attacks, that could disrupt operations (availability), modify information (integrity), or give away confidential information (confidentiality). The objective of cybersecurity is to provide increased levels of protection for information and physical assets from theft, corruption, misuse, or accidents while maintaining access for their intended users. There are many aspects to cybersecurity including designing secure systems, restricting access using physical and digital methods, identifying users, as well as implementing security procedures and best practice policies.

This section provides information on how and help to secure your system from a malicious cyber-attack.

For essential cybersecurity best practices, refer to Schneider Electric's Recommended Cybersecurity Best Practices.
https://www.se.com/en/download/document/7EN52-0390/

⚠WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Change default passwords at first use to help prevent unauthorized access to device settings, controls and information.
- Disable unused ports/services and default accounts, where possible, to minimize pathways for malicious attacks.
- Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).
- Apply the latest updates and hotfixes to your Operating System and software.
- Use cybersecurity best practices (for example: least privilege, separation of duties) to help prevent unauthorized exposure, loss, modification of data and logs, interruption of services, or unintended operation.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Product Defense-in-depth

Secure Development Lifecycle

Schneider Electric uses a Secure Development Lifecycle (SDL) process, a key product development-based framework that helps ensure products follow secure design processes across all lifecycle stages. The Schneider Electric SDL process complies with IEC 62443-4.1.

Security Features Provided

For the cybersecurity features provided by the Schneider Electric product, refer to the user guide. The features provide security capabilities which contribute towards protecting the product from potential security threats.

Defense-in-depth Measures Expected in User Environment

Defense-in-depth Approach

Schneider Electric recommends a defense-in-depth approach to cybersecurity for its customers. Defense-in-depth is a hybrid, multi-layered security strategy that provides holistic security throughout an industrial enterprise. The following are recommendations for a defense-in-depth approach to cybersecurity.

Cybersecurity Policy

Formulating a security plan, policies and procedures that cover risk assessment, risk mitigation and methods to recover from disaster. Developing an available and up-to-date guidance on governing the use of information and technology assets in your company.

Network Separation

Separating the industrial automation and control system from other networks by creating Demilitarized Zones (DMZ) to protect the industrial system from enterprise network requests and messages.

Perimeter Security

Using firewalls, authentication, authorizations, VPN (IPsec) and antivirus software to prevent unauthorized access. Installed devices, and devices that are not in service, are to be in an access-controlled or monitored location.

Network Segmentation

Containment of a potential security breach to the only affected segment by using switches and VLANs to divide the network into sub-networks and by restricting traffic between segments. This helps contain malware impact to one network segment; thus limiting damage to the entire network.

Device Hardening

Password management, user profile definition and deactivation of unused services to strengthen security on devices. Controls against malware - detection, prevention and recovery controls to help protect against malware are implemented and combined with appropriate user awareness.

Security Practices for Removable Devices

When using removable devices such as external hard drives or USB drives, refer to the following recommended actions to protect against unauthorized access and unintended disclosure of data.

- Scan any devices used to exchange data before using them in any node connected to the network.
- Encrypt your files.
- Use password protection.
- Do not store sensitive data in removable media, or if you need to store sensitive data in removable media, manage it properly in a secure location.
- Disable unused ports or limit available devices.

Monitoring and Update

Surveillance of operator activity and network communications. Regular updates of software and firmware.

Secure Deployment

Network

Improve security of networked devices by using multiple layers of cyber defense (such as firewalls, network segmentation, and network intrusion detection and protection). Disable unused ports/services and default accounts to help minimize pathways for malicious attackers.

To reduce the security risks associated with networks, follow these guidelines:

- Use firewalls and other security devices or settings to limit access to the host network, based on your security risk assessment.
- When using a firewall:
  Restrict communication to the expected ports, as per your network configuration. Only open those ports that are necessary for network communication.
- When using network switches:
  Close or disable unused network ports to prevent unauthorized connection of network nodes or other devices.

Patching

Be sure that all Windows updates and hotfixes, especially Windows security updates are regularly applied on the operating system.

Allowlisting

Zero-day cybersecurity attacks take place before a software vendor is aware of a cybersecurity exploit. Meaning that neither software, nor anti-virus programs have been created or updated to protect against the zero-day threat or attack.

Application allowlisting is recommended to protect against zero-day attacks. This specifies an index of approved software applications and processes that are permitted to be present and active on the operating system.

Secure Account Management

User Access

Cybersecurity policies that govern user accounts and access, such as least privilege and separation of duties, vary from site to site. Work with the facility IT System Administrator to ensure that user access adheres to the site-specific cybersecurity policies.

Account Management

Windows-based products require the sign-in password to be set in order to reduce the risks of unauthorized access, intrusion and infection of malicious software.

NOTE: In order to build and operate a secure system, we strongly recommend that you use a different authority account in each phase as follows.

Phase	Account type (authority)
System development	Administrator
Operation	Standard user
Maintenance	Administrator

Secure Maintenance

Software Update

Maintain up-to-date version of any software related to the product, such as security updates, drivers, utilities, configuration tools.

For the latest version of the software we provide, refer to the following URL.
www.se.com/ww/en/download

Network Monitoring

When using a firewall:

- Periodically monitor the firewall to ensure the configuration has not been changed, and that the firewall status does not indicate communication has occurred on unexpected ports.
- Only open those ports that are necessary for network communication.

When using network switches:

- Periodically monitor the switch to ensure the configuration has not been changed, and that the switch status does not indicate communication has occurred on unexpected ports.

Monitoring Operating System

Install operating system patches and anti-virus software updates on the product, as they are released.

Periodically monitor the Windows accounts available on the product to ensure that only the necessary personnel can log on to the product, with the appropriate level of access. Remove inactive or unnecessary user accounts.

Review the Windows System Events Log to monitor logon and logoff activity, and to detect attempted unauthorized activity.

Periodically review user accounts and their roles and privileges to ensure compliance with your organization's policy.

Maintaining Current Backups

The most effective way to recover from a malware attack, unauthorized access or unintended data exposure is backing up your systems and data regularly and store it in a secure, separate, non-shared location.

Back up all critical resources off the network and keep a copy in a secure, tamperproof, or offline environment.

Secure Decommissioning

Before decommissioning the product, review the following recommended actions to decommission it in a protected environment:

- Ensure all important data from the product is saved before performing a reset.
- Document disposal actions according to your company's policies and standards to keep a record of activities.
- Wipe the device before decommissioning it to help prevent potential disclosure of data.
- Follow decommission and sanitization tasks as described by your organization or contact your network administrator.

Secure Disposal

Follow device removal tasks described by your organization or contact your network administrator to determine a responsible method of disposal.

Dispose the device according to the legislation of the country.

Security Notification

Product security notification posted can be viewed via the following URL.
https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp

Vulnerability Reporting

Cybersecurity incidents and potential vulnerabilities can be reported via the following URL.
https://www.se.com/ww/en/work/support/cybersecurity/report-a-vulnerability.jsp

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

As standards, specifications, and design change from time to time, please ask for confirmation of the information given in this publication.

EIO0000004948.01