Cybersecurity Policy Manual

MU214604 Rev. B

September 29, 2023

www.altus.com.br

According to current legislation in Brazil, the Consumer Defense Code, we are giving the following information to clients who use our products, regarding personal safety and premises.

The industrial automation equipment, manufactured by Altus, is strong and reliable due to the stringent quality control it is subjected to. However, any electronic industrial control equipment (programmable controllers, numerical commands, etc.) can damage machines or processes controlled by them when there are defective components and/or when a programming or installation error occurs. This can even put human lives at risk. The user should consider the possible consequences of the defects and should provide additional external installations for safety reasons. This concern is higher when in initial commissioning and testing.

The equipment manufactured by Altus does not directly expose the environment to hazards, since they do not issue any kind of pollutant during their use. However, concerning the disposal of equipment, it is important to point out that built-in electronics may contain materials which are harmful to nature when improperly discarded. Therefore, it is recommended that whenever discarding this type of product, it should be forwarded to recycling plants, which guarantee proper waste management.

It is essential to read and understand the product documentation, such as manuals and technical characteristics before its installation or use. The examples and figures presented in this document are solely for illustrative purposes. Due to possible upgrades and improvements that the products may present, Altus assumes no responsibility for the use of these examples and figures in real applications. They should only be used to assist user trainings and improve experience with the products and their features.

Altus warrants its equipment as described in General Conditions of Supply, attached to the commercial proposals.

Altus guarantees that their equipment works in accordance with the clear instructions contained in their manuals and/or technical characteristics, not guaranteeing the success of any particular type of application of the equipment.

Altus does not acknowledge any other guarantee, directly or implied, mainly when end customers are dealing with third-party suppliers. The requests for additional information about the supply, equipment features and/or any other Altus services must be made in writing form. Altus is not responsible for supplying information about its equipment without formal request. These products can use EtherCAT® technology (www.ethercat.org).

COPYRIGHTS

OPEN SOURCE SOFTWARE NOTICE

To obtain the source code under GPL, LGPL, MPL and other open source licenses, that is contained in this product, please contact opensource@altus.com.br. In addition to the source code, all referred license terms, warranty disclaimers and copyright notices may be disclosed under request.

Contents

1. Introduction

Cybersecurity plays a crucial role in the industrial automation environment. With the alarming increase in security incidents in factories, plants and other automated applications, effective measures to protect these systems becomes imperative. This document objective is to present and justify the cybersecurity measures implemented in Altus products, notably MasterTool, the development environment for programmable logical controllers (PLCs), and the Nexto, Nexto Xpress and Hadron Xtorm series.

Government institutions such as ICS-Cert and the German Federal Department for Information Security (BSI) have been closely monitoring these increasing incidents. Given this scenario, the development of methodologies to ensure the integrity and protection of systems has become an urgent necessity. A significant milestone in this regard is the international standard guideline IEC 62443, initially published by the Industrial Automation and Control Systems Security Committee (ISA99) of the International Society of Automation (ISA), often referred to as the ISA/IEC 62443 standard.

The scope of cybersecurity measures encompasses the protection of various aspects, including the availability of controller functionalities, application functionality, the confidentiality of source code and the application, the integrity of application functions, of the development system, and of the components employed, as well as the authenticity of the controller and its data.

In this context, this document highlights the cybersecurity strategies adopted by Altus and its products, aiming to safeguard customers and their industrial operations from increasingly sophisticated and persistent threats. The use of the ISA/IEC 62443 standard as a solid reference reflects a commitment to excellence in safeguarding the industrial automation environment against potential cyber risks.

2. Terms and Definitions

2.1. Vulnerabilities

Automation systems might be attacked through different points in its structure:

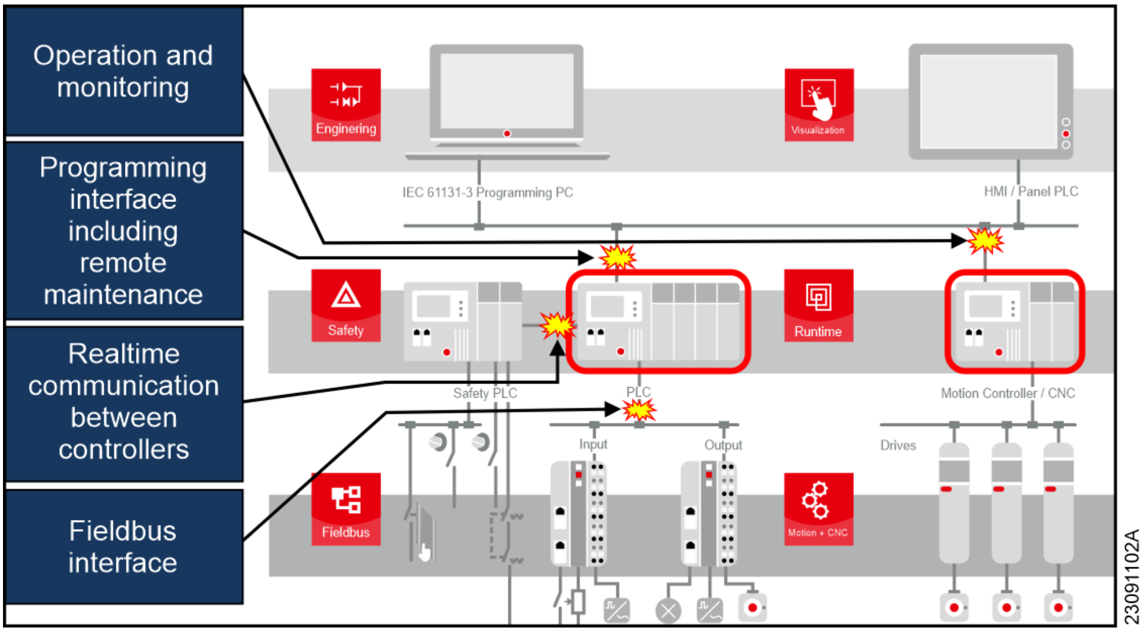

Figure 1: Possible vulnerabilities of a typical automation system.

2.2. Threat

It refers to a set of circumstances and associated sequence of events with the potential to adversely affect operations (including mission, functions, image, or reputation), assets, control systems, or individuals through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. In essence, it is the possibility of malicious or unwanted events occurring that compromise the integrity, confidentiality, or availability of resources and information in an industrial automation environment.

2.3. Protection Levels

To address this comprehensive approach, the ISA/IEC 62443 standard establishes four main levels of protection on an ascending scale, each tailored to address different threats:

- Level 1: Occasional and accidental threats;
  Examples: Hard drive failure, operational errors.
- Level 2: Intentional threats through simple means;
  Example: Successfully guessing a password.
- Level 3: Intentional threats through sophisticated means;
  Example: Utilizing hacking tools.
- Level 4: Intentional threats through sophisticated means and extensive resources.
  Examples: Specialized development, knowledge of the application, or insider corruption.

2.4. Programmable Controller

A computer used in industrial automation systems, which can also be referred to as a PLC (Programmable Logical Controller) or simply a Controller, is a crucial component in these systems. These devices can be targeted in cyberattacks due to their unique characteristics, and they rely on programming designed for specific applications, which can potentially introduce vulnerabilities. The Altus controllers, discussed in this document, belong to the Nexto, Nexto Xpress, or Hadron Xtorm product lines.

2.5. MasterTool

MasterTool IEC XE is a comprehensive tool for programming, debugging, configuring, and simulating user applications. The software is based on the integrated tool concept, providing flexibility and ease of use, allowing users to program in six languages defined by the IEC 61131-3 standard: Structured Text (ST), Sequential Function Chart (SFC), Function Block Diagram (FBD), Ladder Diagram (LD), and Continuous Function Chart (CFC).

2.6. Protected Environment

Every system and piece of equipment needs to be accessed during its installation, operation, and maintenance. However, unrestricted access should be avoided to prevent operational failures and unintentional or intentional damage to the product. To achieve this, the system should be divided into subsystems, with controlled access to each subsystem, ensuring that only authorized individuals can access them, thereby safeguarding the environment.

3. Resposabilities of different security agents in the security of industrial systems

In the configuration of industrial control applications, several active parties and suppliers are involved: software and hardware component providers, system integrators or builders of industrial control applications, and operators. As information technology security is a comprehensive task, all the mentioned parties must make a significant effort to protect the application against attacks.

- Software Provider:
  - Analyze assets and threats;
  - Provide approved security measures;
  - Supply technical documentation;
- Automation Component Provider:
  - Analyze assets and threats;
  - Implement software and hardware security measures;
  - Supply technical documentation;
- System Integrator and Machinery Manufacturer:
  - Analyze assets and threats;
  - Implement software and hardware security measures;
  - Implement system security measures;
  - Implement system security measures;
- Plant Operator/Manager:
  - Analyze assets and threats;
  - Implement software, hardware, and system security measures;
  - Test, audit, and certify the system;
  - Train employees;

4. General Protections for Industrial Automation Systems

First and foremost, all commonly known security measures for computers should be applied in networks with industrial automation equipment, such as:

- Virus protection;
- Strong passwords that are regularly changed;
- Firewall protection;
- Use of VPN tunnels for inter-network connections;
- Caution when dealing with removable storage devices like USB flash drives.

Additionally, it is mandatory to have well-defined user and permission management for access to controllers and their interconnected networks.

4.1. Use in protected Environment

Locating the controller in a protected environment is absolutely necessary to prevent accidental or intentional access to the controller or its application, which is crucial for the operation of the machinery or installation.

This protected environment can be, for example, within:

- Locked electrical control cabinets with no external communication access;
- An intranet network with well-defined user rights and no external access;
- A network with internet access only through a well-configured firewall via a VPN tunnel.

Clearly, the level of protection decreases as you move down this list.

To establish such a protected environment, several rules must be followed:

- Keep the trusted network as small as possible and independent of other networks;
- Safeguard cross-communication between controllers and communication between controllers and field devices using standard communication protocols (fieldbus systems) through appropriate measures;
- Isolate and strictly separate these networks from common access;
- Use fieldbus systems exclusively in protected environments, as they lack additional security measures like encryption. Open physical or data access to fieldbus systems and their components poses a significant security risk.

4.2. Security-aware Users

Security-aware users play a crucial role in cybersecurity as most reported security incidents occur unintentionally due to handling errors or device misuse. Therefore, both machine and facility manufacturers and operators need to be aware of potential threats and the necessary infrastructure measures to prevent them. To achieve this goal, it is advisable for users to participate in specialized training provided by security experts, whether within the company or by external professionals. These training sessions are designed to empower users to adopt proper security practices and understand how to apply the appropriate protective measures in the development and operation of industrial controllers.

5. Security Measures Available in MasterTool

This chapter provides information on the cybersecurity features within the MasterTool program, emphasizing their significance, and how to locate them in the product manuals. Below the subchapter titles, the relevant component requirement (RC) from the IEC 62443-4-2:2019-02 standard to which each feature corresponds is specified.

5.1. Administrator user on project levels

CR 1.1 of norm IEC 62443-4-2

MasterTool offers the capability of read/write protection for individual objects within the project with user administration. This protection can be defined for menu commands as well as for specific object types (e.g., task creation, POUs, methods, GVLs, etc.) or existing objects in the project (such as project settings or POUs or specific tasks).

Through user administration, it's possible to limit the range of functionalities in a more granular way, allowing tailored access rights to specific security needs, thereby safeguarding the confidentiality of intellectual property as well as the integrity of the application code.

The step-by-step instructions for using these MasterTool functions can be found in the "User and Access Rights Management" chapter of the MasterTool Manual.

5.2. Runtime System Access with Permissions Management/Authentications

CR 1.4 of norm IEC 62443-4-2

There are different phases in an industrial application, from the initial development of the source code to its commissioning, production with the machine or plant, and maintenance. These phases are typically operated by different technicians with appropriate levels of qualification.

Considering these qualification levels and the threats of potential misuse beyond the assigned task or competence, it makes sense to restrict usage to certain user groups.

MasterTool supports authentication and permissions management for an individual user or a group of administrators. Depending on the security policy of the runtime system, user management may or may not be enabled by default. If not, all users are members of the administrator group and have unlimited rights on the controller until user management is activated. When using it, it's necessary for the first activation to occur during the initial login, specifying an administrator user.

Once at least one new user is added, all users must authenticate with their usernames and passwords for each online connection to the controller. Passwords are transmitted encrypted (by default, using asymmetric encryption) and stored encoded as cryptographic hashes in the runtime system.

This measure reduces the threat of accidental or intentional access to the running controller, which could impact the availability or integrity of the compiled application executed on the controller.

Secure login on the programmable controller provides a way to protect the user's application from any unauthorized access. By enabling this feature, the Nexto Series PLC will request a user password before executing any commands between MasterTool IEC XE and the PLC, such as stopping and programming the application or forcing outputs on a module.

Step-by-step instructions for using these MasterTool functions can be found in the "User and Access Rights Management" chapter of the MasterTool Manual.

5.3. Configuring Symbols Set via User Management

CR 2.1 of norm IEC 62443-4-2

Within SymbolConfiguration, subsets of all defined symbols (symbolSets) can be created. With user management enabled, these symbol sets can be assigned to dedicated users for visibility and determination of read/write access rights, thereby safeguarding the confidentiality of data exchanged with connected clients.

Step-by-step instructions for using these functions in MasterTool can be found in the "User and Access Rights Management" chapter of the MasterTool Manual.

5.4. User Management of the Integrated Visualization

CR 2.1 of norm IEC 62443-4-2

The integrated visualization of MasterTool allows for direct operation of the controller and the application. It is strongly recommended to separate operation into different sections or screens according to their level of functional and security influence. MasterTool provides the capability to protect individual visualization elements as well as entire visualization screens in the project through a special user visualization management.

This user management allows for limiting the scope of functionality for specific operators. Critical safety operation modes, such as exporting production data, the plant startup and shutdown process, and access to dedicated service functions, can be restricted to operators with explicitly assigned permissions, ensuring the confidentiality of intellectual property as well as the availability and reliability of the machine or plant process.

For detailed instructions on using these functions in MasterTool, please refer to the “User and Access Rights Management” chapter in the MasterTool Manual.

5.5. Encryption of the Communication with WebVisu

CR 3.1 of norm IEC 62443-4-2

To prevent the interception of communication between the controller and the web browser on the computer, you can use an encrypted HTTPS connection. This can be configured with a self-signed certificate or with one generated by a Certificate Authority (CA). In the Device Security Settings screen, the use of HTTPS can be configured as mandatory or allowed in addition to HTTP connections.

5.6. Secure OPC UA Server

CR 3.1 of norm IEC 62443-4-2

OPC UA is an industrial communication protocol for interoperability developed by the OPC Foundation. MasterTool is equipped with an OPC UA server functionality to provide access to the controller and its application. Several security measures are provided, including an OPC UA server operating with encrypted communication based on X.509 certificates and acting with access to a specific user-defined set of symbols, ensuring greater confidentiality for the data exchanged with connected clients.

5.6.1. OPC UA Server: Users management available

CR 2.1 of norm IEC 62443-4-2

With an activated user management for OPC UA, the establishment of a session is restricted to specific users. This measure reduces the threat of accidental or intentional access to the MasterTool’s OPC UA server.

5.6.2. OPC UA Server: Support of X.509 based communication

CR 3.1 of norm IEC 62443-4-2

One of the features of the OPC UA Server is to operate with encrypted communication based on X.509 certificates. Different security profiles are defined by the OPC Foundation.

Depending on the profile, this protects the integrity (for signed profiles only) or the integrity and confidentiality (for signed and encrypted profiles) of the data exchanged with connected clients.

This measure safeguards the confidentiality of the data exchanged with connected clients.

5.7. Signing of compiled IEC libraries

CR 4.1 of norm IEC 62443-4-2

An IEC library can be signed with an X.509 certificate if it is saved as a compiled library. While compiled libraries ensure the protection of the source code, the signature allows for verification of its authenticity.

The status of library signatures can be observed through icons in the “Library Manager” or through the details in the “Add Library” menu.

5.8. Encryption of the source code of the application

CR 4.1 of norm IEC 62443-4-2

The application source code contains detailed information about the system in question and, therefore, the intellectual property of its manufacturer. Thus, protecting the application source code is a priority in the presence of confidential information.

MasterTool allows for project-wide encryption using passwords or physical security keys like USB Dongles. As described in IEC 62443-4-2 under “Component Requirement 4.3”, password encryption is based on the AES (Advanced Encryption Standard) methods, while solutions based on security keys are provided by the company WIBU Systems. Using passwords has the advantage of not requiring additional hardware, but using security keys provides a much higher level of protection since a password can be hacked or leaked.

Multiple different keys can also be linked to a project simultaneously, limiting access to the source code based on the number of keys and minimizing the risk of losing access to the code if a key is destroyed or lost. For this purpose, it is recommended to associate more keys than what would be strictly necessary.

The source code can also be protected using X.509 certificates. In this scenario, the source code will be symmetrically encrypted (AES algorithm). The symmetric key will then be asymmetrically encrypted (RSA algorithm) using the public key of each user who shares the source code. Optionally, the source code can also be digitally signed using the private key associated with the current user’s X.509 certificate. The signature will be saved alongside the source code in a file with the “.p7s” extension, following the PKCS #7 format for digital signatures.

If encryption is not possible, it is established that the project file is saved in a proprietary format, and its integrity is verified each time the project is loaded, thus protecting the confidentiality of intellectual property.

6. Security Measures Available in Altus PLCs

Altus PLCs are equipped with various security features to prevent vulnerabilities during their operation. Some measures are present in only certain controller models, so always check on the specific documentation of the product for the desired security features. Below the subchapter titles, the component requirement (CR) or Network Device Requirement (NDR) of the IEC 62443-4-2:2019-02 standard to which it pertains is provided.

6.1. Cryptography in OPC UA Communication

CR 3.1 of norm IEC 62443-4-2

If desired, the user can configure encryption for OPC UA communication using the Basic256 SHA256 profile to establish a secure connection.

To configure encryption on an OPC UA server, you should create a certificate for it. The step-by-step instructions can be found in the “Configuration” chapter, in the section titled “Protocol Configuration - OPC UA Server” in the Nexto Series CPU User Manual.

6.2. Firewall

NDR 5.2 of norm IEC 62443-4-2

The Firewall was developed to enhance the device’s security during its use. The main function of the Firewall is to filter incoming and outgoing data packets. The implemented filter uses information from each data packet to determine whether that packet is allowed or not. The main parameters used for this determination include input/output interfaces, port, transport layer protocol, and source and destination addresses.

Step-by-step instructions for using this function can be found in the “Configuration” chapter, in the section titled “Firewall” in the Nexto Series or Nexto Xpress CPU User Manual.

6.3. VPN

NDR 5.3 of norm IEC 62443-4-2

VPN (Virtual Private Network) is used for browsing on unsecured networks, transmitting important data, or simply accessing the internet with a high level of privacy. The VPN’s virtual network can be thought of as a tunnel through which information travels securely, protected by certificates and security keys. OpenVPN is an open-source service, meaning it is free to use and distribute, with its source code open for modifications if needed. The primary goal of a VPN is to establish secure communication over an unsecured network. To achieve this, data is encrypted based on certificates and keys generated using TLS, Transport Layer Security, a protocol that provides 256-bit encryption, one of the most secure methods.

Step-by-step instructions for using this function can be found in the “Configuration” chapter, in the section titled “OpenVPN” in the Nexto Series or Nexto Xpress CPU User Manual. In the same document’s appendix, you can find a section on “TLS Certificate and Key Management”, which covers certificate generation and security.

6.4. Protection Against Flood-type Attacks

CR 7.1 of norm IEC 62443-4-2

The NX5000 (Ethernet) module is equipped with protection against flood-type attacks. This essential security feature is designed to detect and effectively mitigate flood attacks, in which a large amount of data is sent simultaneously to overload the system and cause unavailability or service disruption.

6.5. Potential Sources of Risks

Connecting the device to the internet without proper Firewall and VPN configuration poses significant risks. The USB Host port present in the controllers of some series allows you to expand the controller’s capabilities using various types of USB dongles, including SIM chip modems and WiFi adapters. For devices in bridge mode or routers with enabled external access (port forwarding), once connected to the internet, anyone who knows the modem’s IP address can remotely access the controller. Therefore, for security reasons, it is extremely important and recommended to configure User Rights on the controller to restrict online operations of MasterTool IEC XE with login and password. Through the management Web page, you can even stop the controller, which is a risk not only to cybersecurity but also to the physical safety of employees and assets.

6.6. TCP/UDP Reserved Ports

The following TCP/UDP ports of both local and remote Ethernet interfaces are typically used by CPU services (subject to availability as per the PLC manual) and are therefore reserved and should not be used by the user.

Service	TCP	UDP
System Web Page	80	-
SNTP	-	123
SNMP	-	161
MODBUS TCP	502*	-
MasterTool MT8500	1217*	1740:1743
SQL Server	1433	-
MQTT	1883* / 8883*	-
EtherNet/IP	44818	2222
IEC 60870-5-104	2404*	-
OPC UA	4840	-
WEBVISU	8080	-
CODESYS ARTI	11740	-
PROFINET	-	34964

Table 1: Reserved TCP/UDP ports

* Default port, but user changeable.

7. Conclusion

Security in control systems is of utmost importance in an increasingly interconnected and digitized industrial automation landscape. Security incidents have been on the rise, demanding that integrators and users remain vigilant and proactive in observing and mitigating these risks.

While it's true that cybersecurity can never be guaranteed at 100%, it's essential to understand that the adoption of security measures and proper precautions can significantly elevate the level of protection for a specific application. Awareness of potential threats and the implementation of preventive measures can create a strong barrier against potential hazards.

Therefore, collaboration among suppliers, integrators, operators, and users is crucial in fostering a robust and effective security culture. By investing in training and education, as well as adopting appropriate security technologies, it's possible to mitigate significant risks and ensure the resilience of control systems in industrial environments.

In this ever-evolving environment, it's crucial to recognize that security is a continuous effort. We must stay attuned to the latest trends and developments in cybersecurity, regularly updating and enhancing our security practices and protocols. This way, we can tackle security challenges in an increasingly digital world, safeguarding our operations and ensuring a safer and more reliable industrial automation environment.