Cybersecurity for Industrial Control Systems

Revision 1.05

Rev.	Änderungen	Datum	Name
0.01	initial Version	2023-10-09	F. Gründig
1.0	Formatting, Title Adjustment	2023-10-17	F. Gründig
1.01	Formatting, added JC-420EX, XCOM(S) and JETIP(S)	2025-07-08	T. Föll
1.02	Translated into english	2025-07-09	F. Gründig
1.03	Added chapter 3.2 Ecat, page 7 -> added port 21,52100 and 6000	2025-07-09	T. Föll
1.04	page 7 -> error port 20+21 for FTP corrected, added SNTP	2025-07-09	T. Föll
1.05	Added chapter 6.1 IP Forwarding	2025-11-21	T. Föll

Inhaltsverzeichnis

1 Introduction

This document describes measures and recommendations for improving the cybersecurity of industrial control systems by Bucher Automation AG.
This document applies to the following products:

- JetControl 340
- JetControl 350
- JetControl 365 (MC)
- JetControl 420EXT
- JetControl 440EXT
- JetControl 960EXT / 965EXT
- JetControl 970MC / 975MC

2 References

The following references, in whole or in part, constitute requirements of this document that are essential for its application.
For references to a specific version, only the cited edition applies. For all other references, the latest edition of the referenced document (including any amendments) applies.

Tabelle 2-1 Applicable Documents and Standards

Document	Description	Version
Link zur Betriebsanleitung JC340	Betriebsanleitung JC-340 - Steuerung	1.24.1
Link zur Betriebsanleitung JC350	Betriebsanleitung JC-350 - Steuerung	1.24.1
Link zur Betriebsanleitung JC365 (MC)	Betriebsanleitung JC-365 MC - Steuerung	1.32.1
Link zur Betriebsanleitung JC440 EXT	Betriebsanleitung JC-440 EXT - Steuerung	1.10.1
Link zur Betriebsanleitung JC420 EXT	Betriebsanleitung JC-420 EXT - Steuerung	1.16.1
Link zur Betriebsanleitung JC975 MC	Betriebsanleitung JC-975 MC - Steuerung	1.15.4

3 Terms, Definitions, Symbols, Abbreviations, and Conventions

3.1 Terms and Definitions

3.1.1 Cybersecurity

Context: Organizational Measures

Cybersecurity is the protection of systems, networks and programs from digital attacks. These attacks typically aim to gain access, alter, or destroy confidential information, disrupt business operations, or ransom money.

3.2 Symbols and Abbreviations

Abbreviation	Description
n/a	Not applicable
BA	Bucher Automation AG
NAT	Network Adress Translation
DMZ	Demilitarized Zone
VPN	Virtual Private Network
FTP	File Transfer Protocol
FTPS	FTP via SSL/TLS
SSL	Secure Sockets Layer
TLS	Transport Layer Security
MQTT	Message Queuing Telemetry Transport
UPC UA	Open Plattform Communications Unified Architecture
HTTP	Hypertext Transfer Protocol
SMTP	Simple Mail Transfer Protocol
DNS	Domain Name System
XCOM(S)	BA Communication Protocol between Jetsym and the Control System
JETIP(S)	BA Communication Protocol between Control Systems
Ecat	EtherCAT

4 Organizational Measures

Introduction

Apart from technical cybersecurity measures, there are also numbers of organizational aspects that should be implemented to strengthen security. These include rules for handling passwords and data storage devices, as well as policies regarding system changes and vulnerability management.

Training

Inform and train the employees to raise awareness of potential threats.

Definition of Responsibilities

The lack of responsibilities, tasks, and authorities weakens the security of a system. Define who assumes which role before commissioning.

Least Privilege

It is recommended to grant participants only the rights they need to perform their tasks..

Access Control

Restrict physical access to authorized personnel only. Special attention should be given to control rooms, production cells, control panels, and sensitive equipment.

Emergency Practice

To determine whether the policies and technical measures are effective, regular testing should be conducted.

5 Network Protection:

Introduction

The core of the protective measures is network security. The plant network is segmented into zones and conduits, and cross-communication is limited. It can also be helpful to detect anomalies in network traffic and restrict this traffic.

Network Segmentation

In addition to separating the corporate network from the production network, so-called microsegmentation is recommended. This isolates different production systems from each other, thereby preventing global impacts in the event of an attack.

For planning and implementation of segmentation, visibility is required in form of a hardware inventory list, documented vulnerabilities, and a communication matrix.

Network-Firewall

A firewall is a software or hardware device that separates different network zones. A firewall allows or blocks network traffic based on preconfigured policies or rules.

- A firewall is only as good as its rules.
- Use Network Address Translation (NAT) to isolate private network addresses from public addresses.
- Check the traffic for compliance with correct protocol behavior.
- Regularly monitor the firewall for rule updates, reports and metrics, as well as firmware and software patches.

Access Control

Whitelist the required Firewall Ports. The ports needed for the control system are listed in the chapter: "Assigned Ports."

Deep Package Inspection

By inspecting data packets and considering the connection status in transmission decisions, so-called Next Generation Firewalls can block unwanted network traffic.
Virtual patching can mitigate unknown vulnerabilities and prevent their exploitation. Intrusion Prevention systems can stop intrusion attempts by attackers.

DMZ

It is recommended to prevent direct communication between operations and corporate networks. Instead, connect the networks via an additional DMZ (Demilitarized Zone) network.

Remote Access

Remote access to a machine is considered a common entry point for attackers. It is recommended to perform remote maintenance within a secure environment, for instance via “Virtual Private Network” (VPN). The VPN connection should be authenticated and encrypted.

6 Hardening Recommendations:

Introduction

The PLC is a key component. It controls automatic processes, monitors sensors, and drives actuators.
In addition to the automation program, it can also receive, store, process, and transmit critical information.
Therefore, it is important to protect the controller from unauthorized use, manipulation, and malfunction.

Physical Protection

To protect the device from physical tampering, it is recommended to install the PLC in a lockable control cabinet.

Password Change

The controller is delivered with default passwords. It is recommended to change them as follows:

The controller's file system has two predefined users, "**admin**" and "**system**," each with assigned permissions.

These two users cannot be deleted. Password changes are made by modifying the configuration file **/System/users.ini**.

To edit these settings or to create and manage additional users, follow these steps:

Step	Procedure
1	Establish an FTP connection to the device. Log in using **administrator rights**.
2	Open the file /**System/users.ini**
3	Modify the entries (passwords)
4	Save the modified file on the device
5	Restart the device

Configuration of the PLC Firewall

It is possible to configure the local firewall on the control system (host-based). This allows to block unnecessary ports, network connections, or explicitly permit required connections.

Enabling Secure Data Transfer (FTPs)

It is possible to enable the encrypted FTPs protocol.

Use of Encrypted Protocols

For machine-to-machine (M2M) communication, you can use one of the standard protocols: "MQTT", "OPC UA" or "JETIP(S)". These can be encrypted using certificate-based encryption.

Assigned Ports

To configure the firewall (host-based or network firewall), the following port list can be used.

Note: Some ports can be adjusted via controller configuration. Please take this into account when creating the corresponding rules.

This following list presents the required ports in their default configuration. While some services are essential for commissioning, engineering, and remote access of the controller, others only need to be permitted through the host firewall (within the internal network) or the network firewall when traffic crosses network boundaries.

Service	Port	Protocol	Internal required	External
Debugger (XCOM)	52000	TCP	Yes	Yes (via remote main-tenance)
Debugger (XCOMS)	52100	TCP	Yes	Yes (via remote main-tenance)
JetIP(S) (PCOM)	50000 - 50002	TCP/IP UDP	Yes	Yes (via remote main-tenance)
Jetsync & Pub/Sub	20662	UDP	Yes	No
FTP(S)	20,21	TCP	No	No
SMTP	25	TCP	No	No
OPC UA	48020	TCP	No	No
Modbus TCP	502	TCP	No	No
HTTP	80	TCP	No	No
MQTT	1883, 8883	TCP	No	No
Telnet	23	TCP	No	No
SNTP	123	UDP	No	No
Websockets	9876 (determined in Regis-ternumber 543040)	TCP	No	No
Ecat RAS (Only needed for Ecat diag-nostic data for Jetsym 6.1 and above)	6000	TCP	Yes	(via remote main-tenance)

6.1 Enable/Disable IP Forwarding

To disable IP forwarding, use the mechanism via register 104521.

Register 104521 -> IP forwarding On = 1 / Off = 2

Default state:
JC-3xx -> not possible.
JC-4xx -> default state after switching on IP forwarding “Off” -> value 2
JC-9xx -> default state after switching on IP forwarding “On” -> value 1

7 Backup & Recovery

Introduction

The backup of a control system is structured in multiple stages, devided into:

- program code
- register data
- Configuration data

To replace a defective control system, all of these information are required. The operating system (OS) is not part of the backup and must be updated separately to the desired version if necessary.

Prerequisites

It is recommended to use the currently deployed version of the **Jetsym** software for creating the backup

Backup of a Jetsym Project

Introduction

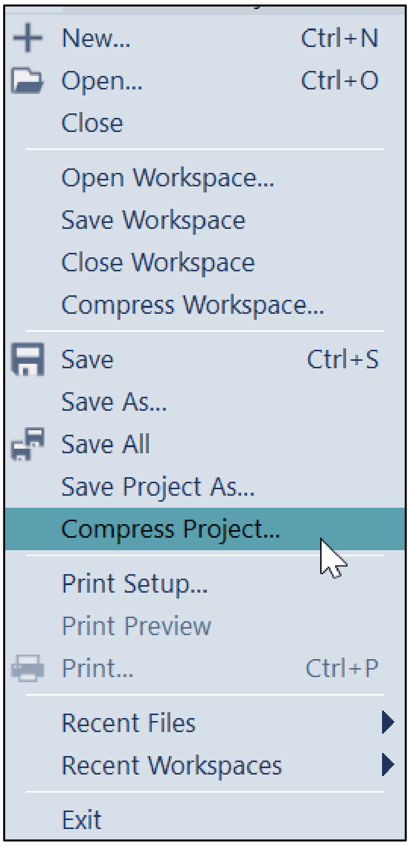
The project configuration, i.e., the control program, hardware tree, as well as any required libraries and saved register data, can be easily exported as a ZIP file.

Prerequisites

The delivery state of the project must be available to Jetsym, and a network connection to the control system must be established.

Compress project

Click on the "**File**" tab and select "**Compress project**," then specify the desired storage location.
Note: The original file paths are used when creating the ZIP archive.



Backup

If necessary, save the created ZIP file to an additional backup medium, such as a USB stick or a network resource.

Backup Register Data

Introduction

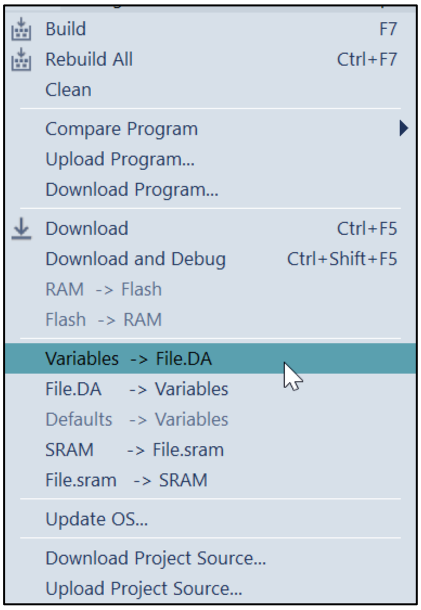
Stored register data, such as recipes, process values, or similar, can be extracted from the control system.

Prerequisites

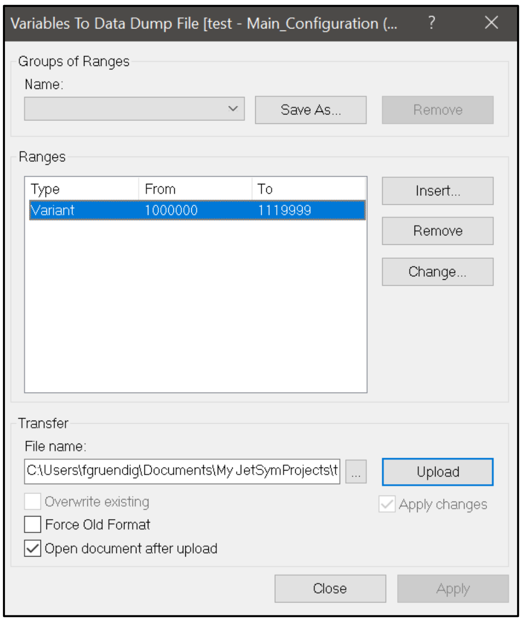
The control system must be connected, and the corresponding project must be open in Jetsym.

Load Register Data

To load the register data, click on the "**Build**" tab and select "**Variables → File.DA**".



In the following window, you can select the register ranges and the backup path. By Clicking “**Upload**” an “STXDA” file will be generated.



Backup

If necessary, save the created **STXDA** file to an additional backup medium, such as a USB drive or a network resource.

Backup of the System Configuration

Introduction	The control system itself contains configuration data such as the IP address, subnet, and similar information.
Prerequisites	To back up configuration files from the control system, the FTP protocol is used. An FTP client, such as Total Commander, is required to establish the connection.
FTP-Connection	Use the FTP tool of your choice to connect to the control system as the user: **"System"**.
Copy System-Data	Copy the following files from the **/System** directory to a backup directory of your choice: • „config.ini“ • „eds.ini“ • Licence file „Serial.lic“ All other folders and files in the **/System** directory are not relevant for backup and restore purposes.
Additional Folders	Back Up additional Folders: • /App (compiled programs) • /Motion (Axis configuration, Motion-Data) • /SysConfig (Connected peripherals)

PLC Replacement

Introduction	In the event of a control system replacement due to a defect, the following information remains stored on the backplane module. In this case, the configuration files do not need to be reloaded onto the new control system.. • IP-Adress • Subnet Mask • Gateway • DNS-Server • PLC Name • File name for the AutoCopy function • IP-Ports for Debug-Server and IP-Server
Change of PLC type	Any controller type within the JetControl 400 family can be replaced with another type from the same controller family.

Restore

Introduction Restoring the functionality of a control system is a multi-step process.

Prerequisites For the restore process, it is recommended to use a ZIP program, an FTP client, and the current version of the Jetsym software.
Additionally, the following files are required: the saved STX backup file (.STXDA), the saved configuration files (.ini), and the Jetsym project as a ZIP file.

Configuration Restore Establish an FTP connection to the control system using the user: **"System"**.
Then, copy the saved configuration files to the control system.
After the transfer is complete, restart the control system to activate the configuration.

Project Restore The Jetsym project package can be restored by extracting the saved ZIP file to your local hard drive.
Extract the file into an empty folder on your hard drive.

The project can then be opened using Jetsym and loaded onto the connected control system.

Register Data Restore The register values can be transferred to the control system using Jetsym via the "**Build**" tab and the entry "**File.DA** → **Variables**".
In the dialog, select the backup file and click "**Open.**"“.

Disposal

Introduction A control system may contain confidential information. This data should be deleted before decommissioning the device.

Data Deletion & Factory Reset In the Jetsym project, under **System Commands**, you will find two buttons for resetting the system to factory settings:

- Reset remanent parameters
- Format Flash disk