SIEMENS

SINUMERIK

SINUMERIK MC
MCU commissioning: NC, PLC, drive

Commissioning Manual

Introduction 1

Fundamental safety instructions 2

Overview 3

Requirements for commissioning 4

Licensing 5

PLC commissioning 6

Commissioning NC-controlled drives 7

NC commissioning 8

Creating and importing archives using SINUMERIK ONE Commissioning 9

Installation / upgrading 10

Installing and setting up PCU-Basesoftware /IPC 11

HT 2 and HT 10 handheld terminals 12

Appendix A

Valid for:
SINUMERIK MC
CNC software V1.24
SIMATIC STEP 7 Professional V19
SINUMERIK STEP 7 Toolbox V19 SP1
SINAMICS drives S120/S210

07/2024
A5E47437618B AJ

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ **DANGER**
indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ **WARNING**
indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ **CAUTION**
indicates that minor personal injury can result if proper precautions are not taken.

NOTICE
indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ **WARNING**
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens Aktiengesellschaft. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E47437618B AJ
Ⓟ 07/2024 Subject to change

Copyright © Siemens 2019 - 2024.
All rights reserved

Table of contents

1 Introduction 9

1.1 About SINUMERIK 9

1.2 About this documentation 10

1.3 Documentation on the internet 11
1.3.1 MC documentation overview 11
1.3.2 Documentation overview SINUMERIK operator components 11

1.4 Feedback on the technical documentation 13

1.5 mySupport documentation 14

1.6 Service and Support 15

1.7 Using OpenSSL 17

1.8 General Data Protection Regulation 18

2 Fundamental safety instructions 21

2.1 General safety instructions 21

2.2 Equipment damage due to electric fields or electrostatic discharge 25

2.3 Warranty and liability for application examples 26

2.4 Cybersecurity information 27

2.5 Residual risks of power drive systems 28

3 Overview 31

3.1 Overview of information relevant to commissioning for SINUMERIK MC 31

3.2 Configuration SINUMERIK MCU 1720 33

3.3 Procedure for the initial commissioning 34

4 Requirements for commissioning 37

4.1 General prerequisites 37

4.2 Software and hardware preconditions 38

4.3 Position of the interfaces 39

4.4 Power-On and boot-up 41
4.4.1 Resetting the NC and PLC 41
4.4.2 Resetting the NC and PLC separately 43
4.4.3 Boot completed 44

4.5 Check the NC and IPC connection of the MCU and configure 45

4.6 Installing SINUMERIK ONE Commissioning or Operate /PCU Modular 47
4.6.1 Installing SINUMERIK ONE Commissioning 47
4.6.2 Operating software SINUMERIK Operate /PCU Modular 48
4.6.2.1 Installing SINUMERIK Operate /PCU Modular 48

4.6.2.2 Setting up SINUMERIK Operate for autologon mode ... 50
4.6.2.3 Switching to the Service Desktop during autostart / autologon operation ... 51
4.6.2.4 Modifying the user account for autologon mode. ... 52
4.6.2.5 Configuring the SINUMERIK Operate display size ... 53
4.6.3 Configuring the PG/PC interface ... 53
4.6.4 Starting and setting up SINUMERIK ONE Commissioning or Operate /PCU Modular ... 55
4.7 Access levels ... 57
4.8 Read-out the MCU serial number for the TIA Portal configuration ... 62
5 Licensing ... 63
5.1 SINUMERIK License Key ... 63
5.2 Web License Manager ... 65
5.3 License database ... 66
5.4 How to perform the assignment ... 67
5.5 Important licensing terms ... 68
6 PLC commissioning ... 71
6.1 PLC commissioning: Overview ... 71
6.2 Starting the TIA Portal ... 72
6.3 Configuring the PLC ... 73
6.3.1 Create a project ... 73
6.3.2 Inserting an MCU ... 73
6.3.3 Configuring the PC system ... 75
6.3.4 Configuring PROFINET for SINUMERIK MCU ... 76
6.3.5 Configuring PROFINET on the PC system ... 77
6.3.6 Compile hardware configuration ... 77
6.3.7 Establish the communication connection ... 78
6.3.8 Load hardware configuration into the PLC ... 80
6.3.9 Loading the WinCC runtime project into the PC system ... 83
6.4 Creating a PLC program ... 86
6.4.1 Overview of the PLC program ... 86
6.4.2 Execution structure PLC program ... 86
6.4.3 Relevant organization blocks ... 89
6.4.4 Inserting program code for calling the basic program ... 90
6.4.5 Inserting the basic PLC program into the project ... 92
6.4.5.1 Opening the PLC basic program system library ... 92
6.4.5.2 Inserting PLC data types ... 93
6.4.5.3 Inserting PLC basic program blocks ... 95
6.4.5.4 Edit blocks ... 97
6.4.5.5 Blocks with user-specific adaptations ... 97
6.4.5.6 Retentivity behavior of the PLC basic program ... 97
6.4.5.7 Programming examples (SCL) ... 98
6.4.6 Handling of blocks and libraries ... 103
6.4.6.1 Use and handling of groups ... 103
6.4.6.2 Copying blocks into a project ... 104
6.4.6.3 Conflicts when copying blocks ... 107
6.4.6.4 Block address range for PLC user program ... 108
6.4.7 NCK hardware interrupts ... 110

6.4.7.1 General information on hardware interrupt OBs ... 110
6.4.7.2 Transfer and acknowledgment time of NCK signals ... 111
6.4.7.3 Identification of an NCK event in the PLC program ... 112
6.4.7.4 Defining NCK hardware interrupt event ... 112
6.4.7.5 Use of the associated system constant ... 114
6.4.7.6 Assigning hardware interrupt OB during runtime ... 115
6.4.8 Loading the PLC program to the PLC ... 116

6.5 First commissioning of the PLC completed ... 118

7 Commissioning NC-controlled drives ... 119

7.1 Drive systems for SINUMERIK MC ... 119

7.2 Commissioning drives with "Startdrive" ... 120
7.2.1 Overview ... 120
7.2.2 Reading out the device configuration from the drive ... 120
7.2.3 Inserting the drive offline ... 126
7.2.4 Networking the drive with the control system ... 130
7.2.5 Preparing communication via PROFINET IO ... 131
7.2.5.1 Configure sync domains and send clock ... 131
7.2.5.2 Configuring topology and ports ... 133
7.2.5.3 Set up the sync master and sync slave. ... 135
7.2.5.4 Configure isochronous IO device ... 137
7.2.6 Configuring telegrams ... 139
7.2.6.1 Overview of telegram configuration ... 139
7.2.6.2 Displaying telegram configuration ... 140
7.2.6.3 Settings for SINAMICS S120 ... 141
7.2.6.4 Settings for SINAMICS S210 ... 142
7.2.6.5 Parameterizing sending (actual value/safety actual value) ... 142
7.2.6.6 Parameterizing receiving (setpoint/safety setpoint) ... 144
7.2.6.7 Structure of the telegrams, control and status words ... 145
7.2.6.8 Editing telegrams ... 146

7.3 Commissioning drives via device master files ... 148
7.3.1 Overview ... 148
7.3.2 Inserting and networking a SINAMICS drive ... 148
7.3.3 Configuring network settings for the drive ... 150
7.3.4 Configuring telegrams for communication ... 152
7.3.5 Completing the configuration ... 155

7.4 Assigning the basic parameters in SINUMERIK ONE Commissioning ... 160
7.4.1 Overview of NC and drive communication ... 160
7.4.2 Assignment of the machine data ... 160

8 NC commissioning ... 163

8.1 Machine and setting data ... 163

8.2 Procedure when commissioning the NC ... 165

8.3 Configuring machine axes ... 167
8.3.1 Axis assignment ... 167
8.3.2 Axis names ... 170
8.3.3 Drive assignment ... 171

8.4 Configuring drive units with SINUMERIK ONE Commissioning ... 173

8.5 Configuring the measuring probe ... 175
8.5.1 Measuring probe general ... 175
8.5.2 Distributed measuring probe with S210 ... 175
8.5.3 Central measuring probe with S120 ... 177

9 Creating and importing archives using SINUMERIK ONE Commissioning ... 179

9.1 Overview for archiving and data backup ... 179
9.2 Importing the archive into the SINUMERIK MC ... 183
9.3 Creating a DSF archive on SINUMERIK MC ... 185
9.4 Creating a user-specific DSF archive on SINUMERIK MC ... 188

10 Installation / upgrading ... 189

10.1 With the help of an MCU service system ... 189
10.1.1 Introduction, upgrading ... 189
10.1.2 Upgrading the CNC software using VNC Viewer on PC/PG ... 190
10.2 Creating a service system ... 191
10.2.1 This is how you create a service system for the MCU ... 191
10.2.2 This is how you operate the service system ... 192

11 Installing and setting up PCU-Basesoftware /IPC ... 195

11.1 Delivery state ... 195
11.1.1 PCU-Basesoftware /IPC with Microsoft Windows 10 ... 195
11.1.1.1 Overview ... 195
11.1.1.2 Supplied software ... 196
11.1.2 Hardware configuration of the internal MCU-IPC ... 197
11.1.2.1 Network settings ... 197
11.1.2.2 Partitioning of the SSD ... 198
11.1.3 Directory structure and file conventions ... 198
11.2 Commissioning the internal MCU-IPC for the first time ... 200
11.2.1 Overview ... 200
11.2.2 Adapting the installation settings ... 200
11.2.3 Installing PCU-Basesoftware /IPC ... 201
11.3 Configuration of the system ... 203
11.3.1 Overview ... 203
11.3.2 Managing user accounts ... 203
11.3.3 Changing the name of the PC system ... 204
11.3.4 Setting the IP address and domain ... 204
11.3.5 Configuring USB interfaces ... 204
11.3.6 Configuring network access on the USB data storage medium ... 205
11.3.7 Configuring the keyboard layout ... 206
11.3.8 Setting up an external screen ... 206
11.3.9 Setting the screen resolution ... 207
11.3.10 Set the resolution in the tcu.ini ... 207
11.3.11 Setting the color depth in the tcu.ini file ... 209
11.3.12 Configuring the SITOP UPS module for use with the PCU-Basesoftware /IPC ... 210
11.3.12.1 Overview of SITOP UPS ... 210
11.3.12.2 SITOP modules for IPC ... 211
11.3.12.3 Configuring SITOP software for PCU Base ... 211
11.3.12.4 Hardware configuration of the SITOP UPS module ... 217

11.3.13 Configuration of the Service Center ... 219
11.3.13.1 Overview ... 219
11.3.13.2 Configuration of the network adapter ... 220
11.3.13.3 Configuration of the host ... 221
11.3.14 Adapting the firewall settings ... 222
11.3.14.1 Overview ... 222
11.3.14.2 Factory setting of the Microsoft Windows Firewall on the MCU-IPC ... 223
11.3.14.3 General information on the operating principle of the Microsoft Windows Firewall ... 224
11.3.14.4 General information on the settings recommended for Microsoft Windows ... 225
11.3.14.5 Configuration by means of a prompt or script/batch file ... 225
11.3.14.6 Enabling SNMP communication ... 226
11.3.14.7 Activating remote access to the internal PC system ... 228
11.3.14.8 Activation/deactivation of the file and printer release ... 231
11.3.14.9 Activation of the ping execution (ICMP) ... 240
11.3.14.10 Saving and restoring firewall settings ... 242
11.3.15 Using the BitLocker drive encryption ... 246
11.3.15.1 Activating BitLocker setup ... 247
11.3.15.2 Configuring BitLocker via Microsoft Windows ... 249
11.3.15.3 Configuring BitLocker using a script ... 250

11.4 Installing and configuring updates and automation software ... 252
11.4.1 Overview ... 252
11.4.2 Patch management and security updates ... 252
11.4.3 Configuring saving Windows log files ... 253
11.4.4 Configuring a key filter for HMI software ... 253
11.4.5 PCU Installer ... 257
11.4.5.1 Overview ... 257
11.4.5.2 Activating the PCU Installer ... 258
11.4.5.3 Deactivating the PCU Installer ... 259
11.4.5.4 Copying and adapting the configuration file ... 260
11.4.5.5 Reference to the PCUInst.ini configuration file ... 261
11.4.5.6 Installing software with the PCU Installer ... 266
11.4.5.7 Procedure example of an installation with the PCU Installer ... 266
11.4.5.8 Log files (.log) ... 267
11.4.5.9 Program application Configure for CMC ... 268

11.5 Backing up and restoring data ... 270
11.5.1 Overview ... 270
11.5.2 Starting the Service Center ... 270
11.5.3 Functions of the Service Center ... 271
11.5.4 Network settings in the Service Center ... 272
11.5.5 Create a disk image of the SSD ... 275
11.5.6 Restore a disk image of the SSD ... 278
11.5.7 Create a disk image of a partition ... 280
11.5.8 Restore a disk image of a partition ... 283
11.5.9 Network settings in the Service Center ... 285
11.5.10 Decrypting BitLocker-protected partitions ... 287
11.5.11 Starting the Paragon Hard Disk Manager directly ... 288
11.5.12 Creating an emergency boot system USB flash drive ... 289
11.5.13 Operating a service PC/PC in the network ... 291
11.5.13.1 Overview ... 291
11.5.13.2 Connection options in the system network ... 291
11.5.13.3 Configuring routing in the network ... 293

11.5.13.4 Configure the network settings of the PG/PC 294
11.5.13.5 Release directory of the PC/PC in the network 297
11.5.13.6 Creating a shortcut to the network drive 300
11.5.14 Starting up the replacement SSD 301

11.6 Remote access for diagnostics 302
11.6.1 Overview 302
11.6.2 Searching for devices in the system network 302
11.6.3 Display of accessible nodes in SINUMERIK ONE Commissioning 302
11.6.4 Remotely accessing the MCU for operation and maintenance 303
11.6.5 Setting up and using SSH 304
11.6.6 Encryption via SSH protocol 305

12 HT 2 and HT 10 handheld terminals 307

12.1 Handheld terminals overview 307

12.2 Connecting handheld terminals to the MCU 310

12.3 Setting up the PLC configuration for the HT function 311

A Appendix 315

A.1 Script example for BitLocker activation 315

A.2 Abbreviations 317

A.3 Information about third-party software used 319

Index 321

Introduction

1

1.1 About SINUMERIK

From simple, standardized CNC machines to premium modular machine designs – the SINUMERIK CNCs offer the right solution for all machine concepts. Whether for individual parts or mass production, simple or complex workpieces – SINUMERIK is the highly dynamic automation solution, integrated for all areas of production. From prototype construction and tool design to mold making, all the way to large-scale series production.

Visit our website for more information SINUMERIK (https://www.siemens.com/sinumerik).

1.2 About this documentation

Target group

This document is intended for commissioning personnel.

The plant or system is installed, connected, and ready to start. For the following steps, e.g. configuring the individual components, the Commissioning Manual contains all the necessary information or at least references.

Standard scope

This documentation only describes the functionality of the standard version. This may differ from the scope of the functionality of the system that is actually supplied. Please refer to the ordering documentation only for the functionality of the supplied drive system.

It may be possible to execute other functions in the system which are not described in this documentation. This does not, however, represent an obligation to supply such functions with a new control or when servicing.

For reasons of clarity, this documentation cannot include all of the detailed information on all product types. Further, this documentation cannot take into consideration every conceivable type of installation, operation and service/maintenance.

The machine manufacturer must document any additions or modifications they make to the product themselves.

Websites of third-party companies

This document may contain hyperlinks to third-party websites. Siemens is not responsible for and shall not be liable for these websites and their content. Siemens has no control over the information which appears on these websites and is not responsible for the content and information provided there. The user bears the risk for their use.

1.3 Documentation on the internet

1.3.1 MC documentation overview

Comprehensive documentation about the functions provided in SINUMERIK MC Version 1.12 and higher is provided in the SINUMERIK MC documentation overview (https://support.industry.siemens.com/cs/ww/en/view/109771043).



You can display documents or download them in PDF and HTML5 format.

The documentation is divided into the following categories:

- User: Operating
- User: Programming
- Manufacturer/Service: Commissioning
- Manufacturer/Service: Functions
- Manufacturer/Service: Hardware
- Manufacturer/Service: Safety Integrated
- Information and training

1.3.2 Documentation overview SINUMERIK operator components

Comprehensive documentation about the SINUMERIK operator components is provided in the Documentation overview SINUMERIK operator components (https://support.industry.siemens.com/cs/document/109783841/technische-dokumentation-zu-sinumerik-bedienkomponenten?dti=0&lc=en-WW).

You can display documents or download them in PDF and HTML5 format.

The documentation is divided into the following categories:

- Operator Panels
- Machine control panels
- Machine Pushbutton Panel
- Handheld Unit/Mini handheld devices
- Further operator components

An overview of the most important documents, entries and links to SINUMERIK is provided at SINUMERIK Overview - Topic Page (https://support.industry.siemens.com/cs/document/109766201/sinumerik-an-overview-of-the-most-important-documents-and-links?dti=0&lc=en-WW).

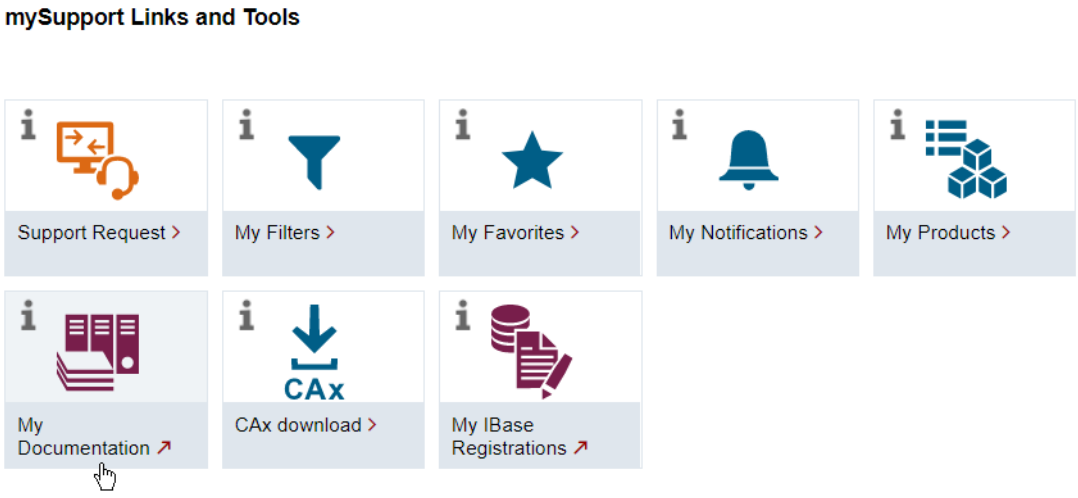
1.4 Feedback on the technical documentation

If you have any questions, suggestions, or corrections regarding the technical documentation published in the Siemens Industry Online Support, use the "Provide feedback" link which appears at the end of the entry.

1.5 mySupport documentation

With the "mySupport documentation" web-based system you can compile your own individual documentation based on Siemens content, and adapt it for your own machine documentation.

To start the application, click on the "My Documentation" tile on the "mySupport links and tools" (https://support.industry.siemens.com/cs/ww/en/my) portal page:



The configured manual can be exported in RTF, PDF or XML format.

Note

Siemens content that supports the mySupport documentation application can be identified by the presence of the "Configure" link.

1.6 Service and Support

Product support

You can find more information about products on the internet:

Product support (https://support.industry.siemens.com/cs/ww/en/)

The following is provided at this address:

- Up-to-date product information (product announcements)
- FAQs (frequently asked questions)
- Manuals
- Downloads
- Newsletters with the latest information about your products
- Global forum for information and best practice sharing between users and specialists
- Local contact persons via our Contacts at Siemens database (→ "Contact")
- Information about field services, repairs, spare parts, and much more (→ "Field Service")

Technical support

Country-specific telephone numbers for technical support are provided on the internet at address (https://support.industry.siemens.com/cs/ww/en/sc/4868) in the "Contact" area.

If you have any technical questions, please use the online form in the "Support Request" area.

Training

You can find information on SITRAIN at the following address (https://www.siemens.com/sitrain).
SITRAIN offers training courses for automation and drives products, systems and solutions from Siemens.

Siemens support on the go



With the award-winning "Industry Online Support" app, you can access more than 300,000 documents for Siemens Industry products – any time and from anywhere. The app can support you in areas including:

- Resolving problems when implementing a project
- Troubleshooting when faults develop
- Expanding a system or planning a new system

Furthermore, you have access to the Technical Forum and other articles from our experts:

- FAQs
- Application examples
- Manuals
- Certificates
- Product announcements and much more

The "Industry Online Support" app is available for Apple iOS and Android.

1.7 Using OpenSSL

This product can contain the following software:

- Software developed by the OpenSSL project for use in the OpenSSL toolkit
- Cryptographic software created by Eric Young.
- Software developed by Eric Young

You can find more information on the internet:

- OpenSSL (https://www.openssl.org)
- Cryptsoft (https://www.cryptsoft.com)

1.8 General Data Protection Regulation

Overview

Siemens observes standard data protection principles, in particular the data minimization rules (privacy by design).

For the SINUMERIK Operate, this means:

The product processes/saves the following personal data:

- FullName (optional): Only if user management is activated
- User name + password: Only if user management is activated
- UserID: nur bei aktivierter Benutzerverwaltung
- IP address
- Security events
- Time stamp

It does not involve data from the personal or private sphere.

The above data is required for the user log-in function. The storage of data is appropriate and limited to what is necessary, as it is essential for the identification of the authorized operator. (Mandatory here are: user name + password; the FullName is optional.)

The above-mentioned data cannot be stored anonymously or – with the exception of the user name – pseudonymously, as otherwise the purpose of identifying the operating personnel cannot be achieved.

Our products do not automatically delete the data mentioned above. The data and logs can be deleted manually by authorized personnel.

The above data is secured against loss of integrity and confidentiality by Industry State-of-the-Art Product Security mechanisms.

SINUMERIK ONE Commissioning Tool

If you use SINUMERIK NC in conjunction with a SINAMICS S210 drive, you can commission and parameterize the Safety Integrated Functions integrated in the drive only via the TIA Portal application "Startdrive".

After uploading the configuration from the TIA Portal to the control system, the SINUMERIK ONE Commissioning Tool is mainly used to manually enter the machine data into the control system.

The handling of the SINUMERIK ONE Commissioning Tool has been derived from SINUMERIK Operate.

Rules for SINUMERIK-conformal telegram configuring of SINAMICS drives

To configure the data exchange between a SINUMERIK 828D, SINUMERIK ONE or SINUMERIK MC and SINAMICS S120 drives, the following rules must be observed for the PROFIBUS/PROFINET configuration of the drives:

- For SINAMICS drive devices (CU3xx) on PROFIBUS/PROFINET, the PROFIBUS/PROFINET configuration must be identical to the standard configuration of the telegrams of the drives on the integrated PROFIBUS (SINAMICS Integrated or NX) of a SINUMERIK 828D or SINUMERIK ONE with regard to the telegrams structure.
- The identical structure of the telegrams refers specifically to the sequence of telegrams for a drive (CU3xx). The telegrams must be configured in the following order:
  - Telegrams for SERVO or HLA drive objects
  - Telegram for the Control Unit drive object
  - Telegram for the infeed drive object
- The following rules must be observed for the telegrams of the individual drive objects:
  - The input and output address of a telegram must have the same value.
    Exception: User-specific telegrams that only have input or output values.
  - The input and output data of a telegram are generally transferred via the same slot. If two different slots are used for data exchange (for PROFIBUS or PROFIBUS Integrated), make sure that the input slot is defined first. The output slot must have the following slot number.

Fundamental safety instructions 2

2.1 General safety instructions



⚠ WARNING

Electric shock and danger to life due to other energy sources

Touching live components can result in death or severe injury.

- Only work on electrical devices when you are qualified for this job.
- Always observe the country-specific safety rules.

Generally, the following steps apply when establishing safety:

1. Prepare for disconnection. Notify all those who will be affected by the procedure.
2. Isolate the drive system from the power supply and take measures to prevent it being switched back on again.
3. Wait until the discharge time specified on the warning labels has elapsed.
4. Check that there is no voltage between any of the power connections, and between any of the power connections and the protective conductor connection.
5. Check whether the existing auxiliary supply circuits are de-energized.
6. Ensure that the motors cannot move.
7. Identify all other dangerous energy sources, e.g. compressed air, hydraulic systems, or water. Switch the energy sources to a safe state.
8. Check that the correct drive system is completely locked.

After you have completed the work, restore the operational readiness in the inverse sequence.



⚠ WARNING

Electric shock due to connection to an unsuitable power supply

When equipment is connected to an unsuitable power supply, exposed components may carry a hazardous voltage. Contact with hazardous voltage can result in severe injury or death.

- Only use power supplies that provide SELV (Safety Extra Low Voltage) or PELV- (Protective Extra Low Voltage) output voltages for all connections and terminals of the electronics modules.



⚠ WARNING

Electric shock due to equipment damage

Improper handling may cause damage to equipment. For damaged devices, hazardous voltages can be present at the enclosure or at exposed components; if touched, this can result in death or severe injury.

- Ensure compliance with the limit values specified in the technical data during transport, storage and operation.
- Do not use any damaged devices.



⚠ WARNING

Electric shock due to unconnected cable shields

Hazardous touch voltages can occur through capacitive cross-coupling due to unconnected cable shields.

- As a minimum, connect cable shields and the cores of cables that are not used at one end at the grounded housing potential.



⚠ WARNING

Electric shock if there is no ground connection

For missing or incorrectly implemented protective conductor connection for devices with protection class I, high voltages can be present at open, exposed parts, which when touched, can result in death or severe injury.

- Ground the device in compliance with the applicable regulations.

NOTICE

Damage to equipment due to unsuitable tightening tools.

Unsuitable tightening tools or fastening methods can damage the screws of the equipment.

- Only use screw inserts that exactly match the screw head.
- Tighten the screws with the torque specified in the technical documentation.
- Use a torque wrench or a mechanical precision nut runner with a dynamic torque sensor and speed limitation system.
- Adjust the tools used regularly.

⚠ CAUTION

Symptomatic respiratory and skin reaction to chemicals

A newly purchased product might contain traces of substances that are identified as sensitizers.

Sensitizers are substances which can cause sensitization in the lungs and skin after exposure to them.

Once sensitized, individuals can have severe reactions to further exposure, even in small amounts. In the most extreme cases, individuals might develop asthma or dermatitis respectively.

- If the product has a strong smell, keep it in a well-ventilated area for 14 days.

⚠ WARNING

Unexpected machine movement caused by radio devices or cellphones

Using radio devices, cellphones, or mobile WLAN devices in the immediate vicinity of the components can result in equipment malfunction or faults and damage to the devices. Malfunctions may impair the functional safety of machines and can therefore put people in danger or lead to property damage.

- Avoid operating radio devices, cellphones and mobile WLAN devices in the direct vicinity of converters and operating units.
- Scan the machine readable code, e.g. a QR code, from a greater distance or switch off the converter power supply before scanning.
- Only operate built-in devices with the control cabinet doors closed.
- When control cabinet doors are open, only qualified electrical personnel are allowed to carry out service and maintenance work.

⚠ WARNING

Fire due to inadequate ventilation clearances

Inadequate ventilation clearances can cause overheating of components with subsequent fire and smoke. This can cause severe injury or even death. This can also result in increased downtime and reduced service lives for devices/systems.

- Ensure compliance with the specified minimum clearance as ventilation clearance for the respective component.

NOTICE

Overheating due to inadmissible mounting position

The device may overheat and therefore be damaged if mounted in an inadmissible position.

- Only operate the device in admissible mounting positions.

⚠ WARNING

Unexpected movement of machines caused by inactive safety functions

Inactive or non-adapted safety functions can trigger unexpected machine movements that may result in serious injury or death.

- Observe the information in the appropriate product documentation before commissioning.
- Carry out a safety inspection for functions relevant to safety on the entire system, including all safety-related components.
- Ensure that the safety functions used in your drives and automation tasks are adjusted and activated through appropriate parameterizing.
- Perform a function test.
- Only put your plant into live operation once you have guaranteed that the functions relevant to safety are running correctly.

Note

Important Safety instructions for Safety Integrated

If you want to use Safety Integrated functions, you must observe the Safety instructions in the Safety Integrated documentation.

⚠ WARNING

Malfunctions of the machine as a result of incorrect or changed parameter settings

As a result of incorrect or changed parameterization, machines can malfunction, which in turn can lead to injuries or death.

- Protect the parameterization against unauthorized access.
- Handle possible malfunctions by taking suitable measures, e.g. emergency stop or emergency off.

2.2 Equipment damage due to electric fields or electrostatic discharge

Electrostatic sensitive devices (ESD) are individual components, integrated circuits, modules or devices that may be damaged by either electric fields or electrostatic discharge.



NOTICE

Equipment damage due to electric fields or electrostatic discharge

Electric fields or electrostatic discharge can cause malfunctions through damaged individual components, integrated circuits, modules or devices.

- Only pack, store, transport and send electronic components, modules or devices in their original packaging or in other suitable materials, e.g conductive foam rubber of aluminum foil.
- Only touch components, modules and devices when you are grounded by one of the following methods:
  - Wearing an ESD wrist strap
  - Wearing ESD shoes or ESD grounding straps in ESD areas with conductive flooring
- Only place electronic components, modules or devices on conductive surfaces (table with ESD surface, conductive ESD foam, ESD packaging, ESD transport container).

2.3 Warranty and liability for application examples

Application examples are not binding and do not claim to be complete regarding configuration, equipment, or any eventuality which may arise. Application examples do not represent customer-specific solutions, but merely serve to provide assistance with typical tasks.

As the user you yourself are responsible for ensuring that the products described are operated correctly. Application examples do not relieve you of your responsibility for safe handling when using, installing, operating and maintaining the equipment.

2.4 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

Further information is provided on the Internet:

Industrial Security Configuration Manual (https://support.industry.siemens.com/cs/ww/en/view/108862708)

⚠ WARNING

Unsafe operating states resulting from software manipulation

Software manipulations, e.g. viruses, Trojans, or worms, can cause unsafe operating states in your system that may lead to death, serious injury, and property damage.

- Keep the software up to date.
- Incorporate the automation and drive components into a state-of-the-art, integrated industrial cybersecurity concept for the installation or machine.
- Make sure that you include all installed products in the integrated industrial cybersecurity concept.
- Protect files stored on exchangeable storage media from malicious software by with suitable protection measures, e.g. virus scanners.
- Carefully check all cybersecurity-related settings once commissioning has been completed.

2.5 Residual risks of power drive systems

When assessing the machine or system-related risk in accordance with the respective local regulations (e.g. EC Machinery Directive), the machine manufacturer or system integrator must take into account the following residual risks emanating from the control and drive components of a drive system:

1. Unintentional movements of driven machine or system components during commissioning, operation, maintenance, and repairs caused by, for example,
   - Hardware faults and/or software errors in the sensors, control system, actuators, and connections
   - Response times of the control system and of the drive
   - Operation and/or environmental conditions outside the specification
   - Condensation/conductive contamination
   - Parameterization, programming, cabling, and installation errors
   - Use of wireless devices/mobile phones in the immediate vicinity of electronic components
   - External influences/damage
   - X-ray, ionizing radiation and cosmic radiation
2. Unusually high temperatures inside and outside the components, including open flames, as well as emissions of light, noise, particles, gases, etc. due to fault conditions, e.g.:
   - Component failure
   - Software errors
   - Operation and/or environmental conditions outside the specification
   - External influences/damage
   - Short circuits or ground faults in the intermediate DC circuit of the converter
3. Hazardous shock voltages caused by, for example:
   - Component failure
   - Influence during electrostatic charging
   - Induction of voltages in moving motors
   - Operation and/or environmental conditions outside the specification
   - Condensation/conductive contamination
   - External influences/damage
4. Electrical, magnetic and electromagnetic fields generated in operation that can pose a risk to people with a pacemaker, implants or metal replacement joints, etc., if they are too close
5. Release of environmental pollutants or emissions as a result of improper operation of the system and/or failure to dispose of components safely and correctly

6. Influence of network-connected and wireless communications systems, e.g. ripple-control transmitters or data communication via the network or mobile radio, WLAN or Bluetooth.
7. Motors for use in potentially explosive areas:
   When moving components such as bearings become worn, this can cause enclosure components to exhibit unexpectedly high temperatures during operation, creating a hazard in areas with a potentially explosive atmosphere.

For more information about the residual risks of the drive system components, see the relevant sections in the technical user documentation.

Overview

3

3.1 Overview of information relevant to commissioning for SINUMERIK MC

Steps for commissioning SINUMERIK MC

Commissioning a SINUMERIK MC (MCU 1720) is performed in two basic steps:

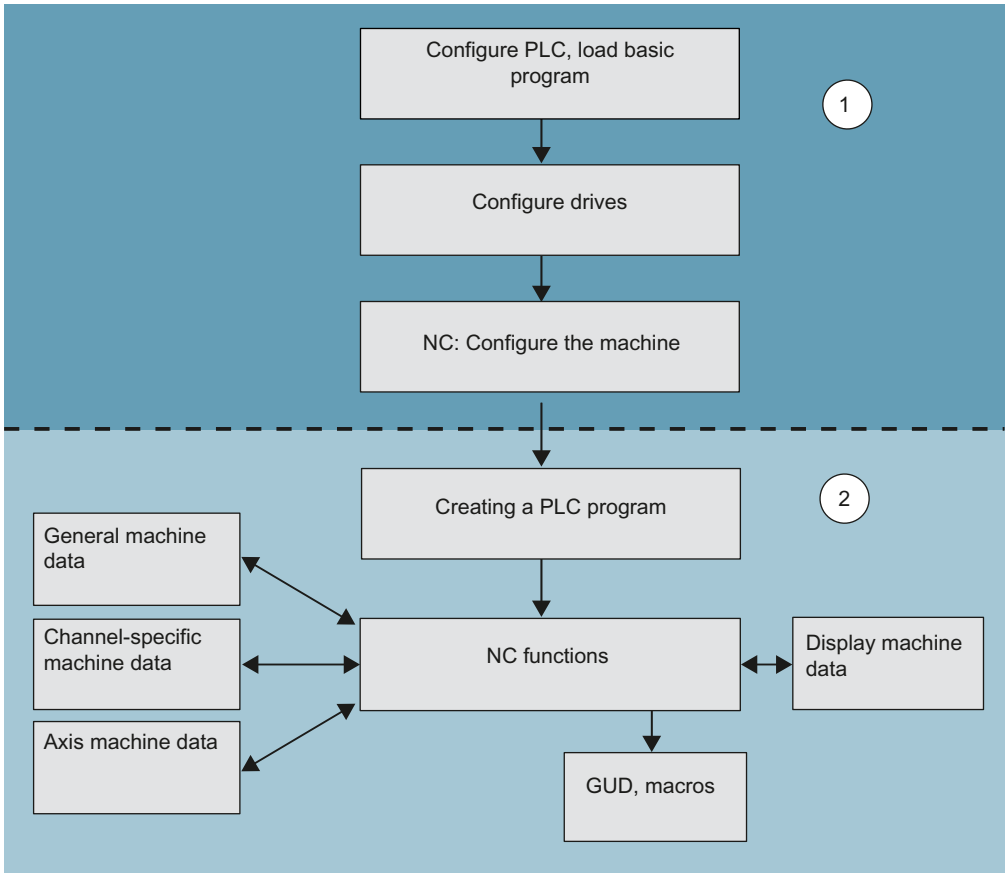


Figure 3-1 Commissioning process

Step 1: Commissioning the MCU, PLC, drive

- Commissioning Manual: MCU commissioning: NC, PLC, drive
- Function manuals: Basic functions, axes and spindles, transformations, tools, monitoring and offsets, technologies, PLC
- Commissioning Safety Integrated: Commissioning with Safety Integrated

Step 2: Commissioning NC functions, PLC program and machine data

- SINUMERIK STEP 7 Toolbox
- List manuals: Machine data, alarms

3.2 Configuration SINUMERIK MCU 1720

Configuration SINUMERIK MCU 1720 with SINAMICS S120 and S210

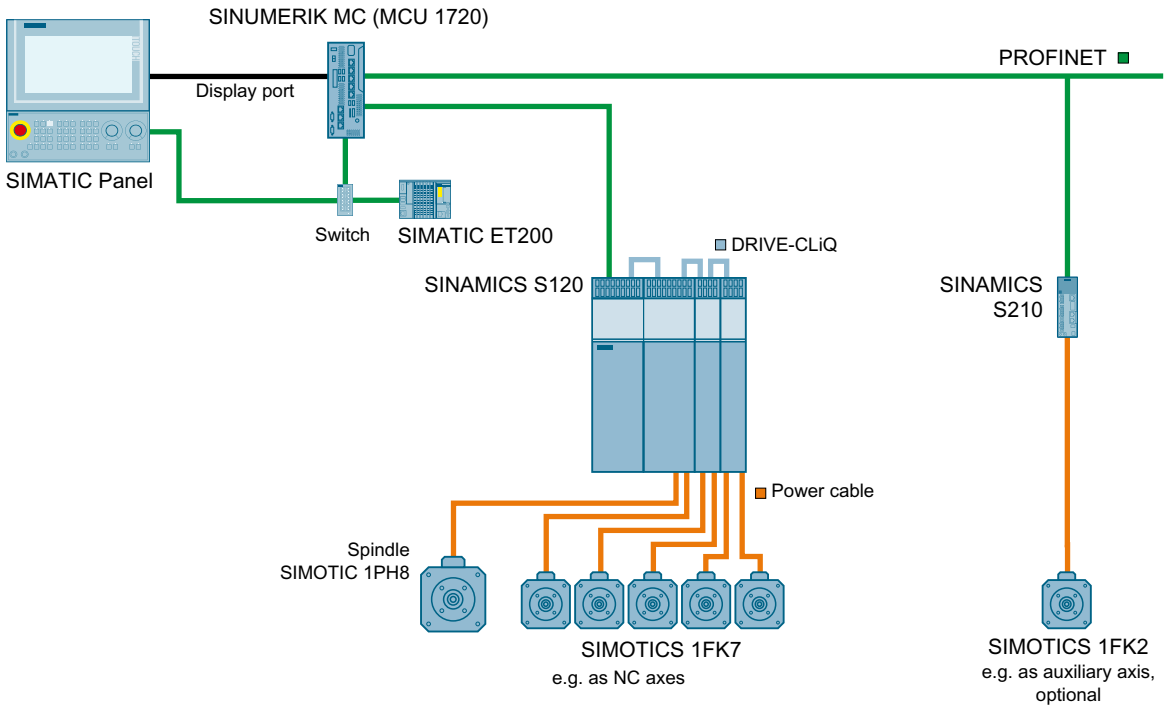


Figure 3-2 Example: Simplified schematic of a SINUMERIK MCU configuration

3.3 Procedure for the initial commissioning

Checking the system

The mechanical and electrical installation of the system must be completed.

The following is important when starting commissioning:

- The control system with its components boots error-free.
- The EMC guidelines were carefully maintained when configuring the system.

Variants for the commissioning process

When commissioning the system for the first time, the following dependencies with respect to the CNC software on the SD Card are considered:

- SD Card with the current CNC software
- SD Card without a CNC software ⇒ **new installation**
- SD Card with older CNC software ⇒ **upgrade**

Commissioning with current CNC software

Sequence		Reference to Chapter
①	Power up the control system with reset NC/PLC	→ Resetting NC/PLC (Page 41)
②	Commission the PLC	→ PLC commissioning (Page 71)
③	Commission the SINAMICS drive system	→ Commissioning NC-controlled drives (Page 119)
④	Commission the NC: • Assign the NC machine data for the communication • Scale the machine data • Parameterize the axis data • Parameterize the spindle data • Parameterize the measuring systems	 → NC commissioning (Page 163) → Procedure when commissioning the NC (Page 165)

Reinstallation of the CNC software

Sequence		Reference to Chapter
①	Install the CNC software on the SD Card: • Bootable USB flash drive • VNC viewer on PC/PG or IPC	→ New installation / upgrade (Page 189)
②	Power up the control system with reset NC/PLC	→ Resetting NC/PLC (Page 41)
③	Commission the PLC	→ PLC commissioning (Page 71)

Sequence		Reference to Chapter
④	Commission the SINAMICS drive system	→ Commissioning NC-controlled drives (Page 119)
⑤	Commission the NC: • Assign the NC machine data for the communication • Scale the machine data • Parameterize the axis data • Parameterize the spindle data • Parameterize the measuring systems	→ NC commissioning (Page 163) → Procedure when commissioning the NC (Page 165)

Upgrading the CNC software

Sequence		Reference to Chapter
①	Archive data from NC and PLC	→ Save data (Page 185)
②	Upgrade the CNC software using the VNC viewer on the PC/PG or internal MCU-IPC:	→ New installation / upgrade (Page 189)
③	Load archived NC and PLC data	→ Load data (Page 183)

Requirements for commissioning 4

4.1 General prerequisites

Preconditions for components involved

The complete system is connected mechanically and electrically, and has been verified in the following points:

- All ESD measures are observed for the design of the components.
- All screws are tightened with their prescribed torque.
- All connectors are plugged correctly and locked/screwed.
- All components are grounded and connected to shields.
- The load capacity of the central power supply is taken into account.

Limit values

All components are dimensioned for defined mechanical, climatic and electrical environmental conditions. No limit value may be exceeded, neither during operation, nor during transportation.

Special attention must be paid to the limit values:

- Power supply conditions
- Pollution burden
- Function-impairing gases
- Ambient environmental conditions
- Storage/transport
- Shock stressing
- Vibration stressing
- Ambient temperature

Further information

You can find further information for installing and connecting drive components and their interfaces in:

- SINAMICS S120 Equipment Manual
- SINAMICS S210 Operating Instructions
- SINUMERIK MC Equipment Manual MCU 1720

4.2 Software and hardware preconditions

Requirements for commissioning

To commission the SINUMERIK MC, the following requirements must be met:

- Hardware requirements
  - SINUMERIK MCU 1720
  - SD card
  - PC (Microsoft Windows 10), with monitor, mouse, and keyboard
- Connections to MCU
  - Monitor on X70/X71
  - Mouse and keyboard on X60 to X63
  - PG or company network on X127/X130
- Software requirements
  - CNC software V1.24
  - Commissioning tool SINUMERIK ONE Commissioning V6.24

    Note

    SINUMERIK ONE Commissioning does not support an OPC UA server connection.

  - SIMATIC STEP 7 Professional (TIA Portal) V19
  - SINUMERIK STEP 7 Toolbox V19 SP1

    Note

    The part numbers of the SINAMICS drives, encoders and motors should be available for parameterization.

  - SINUMERIK PCU-Basesoftware /IPC V15.0 SP3

    Note

    As of SINUMERIK PCU-Basesoftware /IPC V15.0 SP1, the use of the handheld terminals HT 2 and HT 10 is supported.

- Optional software
  - SINUMERIK Integrate Create MyHMI /WinCC V19
  - SINUMERIK Integrate Create MyHMI /3GL V6.24
  - SINUMERIK MC Operate /PCU Modular V1.24 operating software

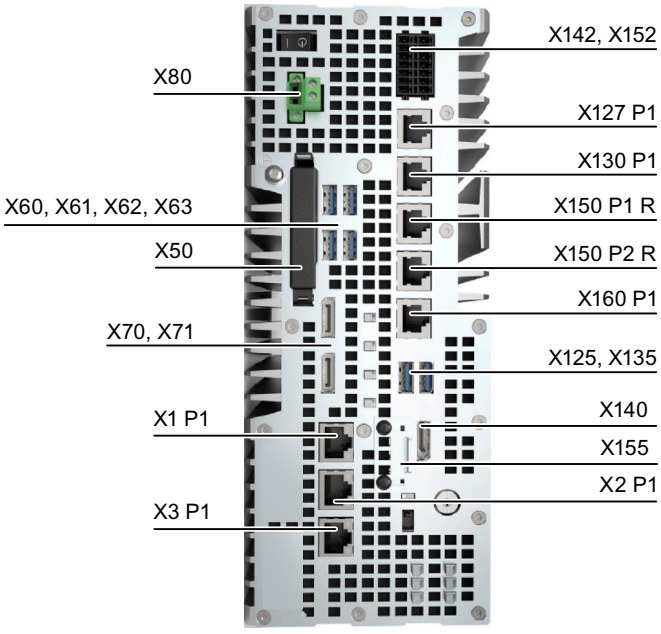
    Note

    The connection of an OPC UA server is supported with SINUMERIK MC Operate / PCU Modular.

4.3 Position of the interfaces

Interfaces on the MCU

The MCU has the following interfaces:



X1 P1	Industrial Ethernet	Ethernet interfaces (e.g. for system and company network)
X2 P1		
X3 P1		X3 (optional)
X50		Slot for the CFast card with cover
X60, X61, X62, X63	USB	Connections for peripheral devices (e.g. for keyboard, mouse, or external drives)
X70, X71	DisplayPort	Connections for digital monitors (e.g. for a SIMATIC operator panel)
X80	+24 V DC	external power supply
X125, X135	USB	only for commissioning and servicing
X127 P1	Industrial Ethernet	MCU service interface
X130 P1		for connection to a company network
X140	DisplayPort	for service purposes only
X142, X152		Digital inputs/outputs, NC
X155		Slot for the SD card with cover
X150 P1 R	PROFINET IO	IRT PROFINET components (e.g. for SINAMICS drive components S120 and S210)
X150 P2 R		
X160 P1		PROFINET connection (e.g. for a system network with SIMATIC ET200 SP)

Pin assignment X142/X152

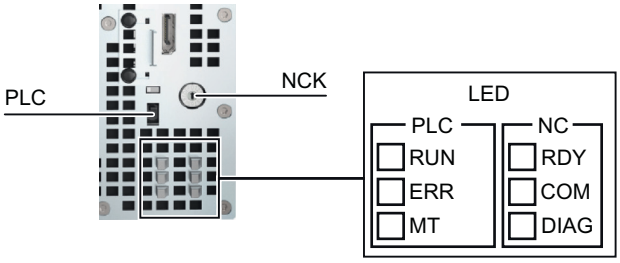
X142	**7**	6	5	**4**	3	**2**	**1**
	0/GND	$A_IN[4]	$A_IN[3]	**0/GND**	$A_IN[2]	**$A_IN[1]**	**+24V**
X152	7	6	5	4	3	2	1

4.4 Power-On and boot-up

4.4.1 Resetting the NC and PLC

NCK rotary switch and PLC toggle switch

The MCU is equipped with an NCK rotary switch and a PLC toggle switch in the lower area of the interface front:



The settings on the NCK switch have the following meaning:

Switch position	NC operating mode
0	NC normal run-up, setting in normal operation
1	General reset (NC run-up with default values)
2	The NC powers up with the data that was saved at the last shutdown.
7	Debug mode (NC is not started); the SSH port tcp/22 is open at X130
8	IP address for X130 of the MCU is displayed on the 7-segment display; the NC is not started; the PLC remains at STOP
9	SSH port tcp/22 is open at X130 (without any entry in file basesys.ini)
All others	Not relevant

Switch position	Operating mode of the PLC
RUN	Places the PLC in the RUN operating state.
STOP	Places the PLC in the STOP operating state.
MRES	Initiates a factory reset.

Note

To activate MRES, keep the switch position pressed.

More information

Information regarding the meanings of the various LEDs is provided in the

SINUMERIK MC Equipment Manual MCU 1720.

Reset for commissioning

In order to achieve a defined state of the complete system, when commissioning the MCU, an NC general reset and a PLC reset must be performed.

Note

In the following cases, the PLC must always be restored to its factory settings:

- First commissioning
- Module replacement
- Reset request from the PLC
- Upgrading the PLC

Procedure:

1. Set the NCK rotary switch to switch position 1.
2. Press the power-on or reset key.
   The MCU is restarted with the request for an NC general reset.
3. If you want to reset the PLC, wait until LEDs RUN and ERR alternate between flashing green and yellow.
4. Keep the toggle switch pressed in the MRES position.
5. Wait until the RUN LED remains permanently lit yellow.
6. Within approx. 4 seconds, move the toggle switch into the STOP position and then back to MRES.
   The RUN LED flashes for approx. 3 seconds at high frequency.
7. Move the toggle switch back into the STOP position.
   The factory settings of the PLC have been restored.
8. Move the PLC toggle switch back to RUN.
9. Turn the NCK rotary switch back to the 0 position.

Result

The NC has now been generally reset and is in the following state:

- NC
  - The user data is deleted.
  - The system data is initialized.
  - The standard machine data is loaded.
- PLC
  Restoring the factory settings puts the PLC into a defined initial state:
  - The PLC data have been deleted from the SD card.
  - The retentive data are initialized.
  - The IP address assigned via TIA Portal has been cleared.
  - The password for protecting confidential PLC configuration data has been deleted.

Note

The PLC can only be restored to the delivery condition with the toggle switch position MRES while the control system is running up

4.4.2 Resetting the NC and PLC separately

General reset of the NC

Carry out the following actions to perform an NC general reset:

1. Turn the NCK commissioning switch on the interface front to position 1.
2. Initiate a power-on reset by switching the control system off and on or by pressing the reset button.
   The system is restarted with the request for a general reset of the NC.
3. After the system has run up, turn the NCK commissioning switch back to position 0.
   Effect:
   - The number 6 and a flashing point are output on the 7-segment display on the front of the MCU.
   - The RUN LED lights up.

After an error-free run-up, the NC is in the following state:

- The NC is in cyclic operation.
- The static memory of the NC is deleted.
- The machine data is preassigned standard values.

Resetting the PLC to its factory settings

Perform the following actions to reset the PLC:

1. Press the power-on or reset key.
   The MCU is restarted with the request for an PLC reset.
2. Wait until LEDs RUN and ERR alternate between flashing green and yellow.
3. Keep the toggle switch pressed in the MRES position.
4. Wait until the RUN LED remains permanently lit yellow.
5. Within approx. 4 seconds, move the toggle switch into the STOP position and then back to MRES.
   The RUN LED flashes for approx. 3 seconds at high frequency.
6. Move the toggle switch back into the STOP position.
   The factory settings of the PLC have been restored.
7. Move the PLC toggle switch back to RUN.

Restoring the factory settings puts the PLC into a defined initial state:

- The PLC data has been cleared from the SD Card.
- The retentive data are initialized.
- The IP address assigned via TIA Portal has been cleared.
- The password for protecting confidential PLC configuration data has been deleted.

4.4.3 Boot completed

Run-up completed without error

After an error-free run-up of the MCU, the following status is displayed:

- The number 6 and a flashing point.
- RUN LED is continuously lit green.

Next steps:

- Configure and check the NC and IPC connection of the MCU.
- Commission the PLC using the TIA Portal.

4.5 Check the NC and IPC connection of the MCU and configure

When supplied from the factory, the NC/PLC and IPC components of the SINUMERIK MCU have no network settings. The MCU components are integrated in the internal network; however, they still do not have a valid IP address to establish communication.

Note

If you install PCU-Basesoftware /IPC, the network settings for the MCU components NC/PLC and IPC with IP address 192.168.214.241 are automatically configured.

Further information for installing PCU Base is provided in Chapter "Installing and setting up PCU-Basesoftware /IPC (Page 195)".

Use the Siemens communication settings application to check or configure network settings.

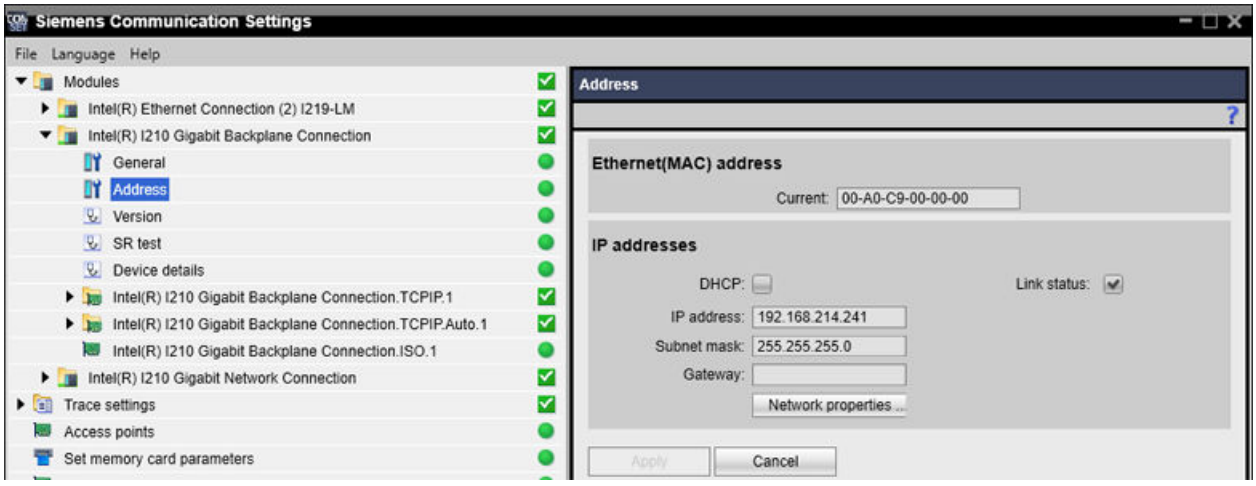


Figure 4-1 Checking or configuring MCU components using Siemens communication settings

Requirement

The Siemens communications settings application is installed on the MCU IPC system.

Note

The application is a system tool and is part of the SINUMERIK ONE Commissioning installation.

This is how you check or configure the network settings of MCU components using the Siemens communication settings application

1. Under Windows, select "Start > Control panel" > "All control panel elements".
2. Click "Communication settings".
   The "Siemens communication settings" window opens.
3. In the navigation, click on
   "Modules > Intel (R) I210 Gigabit Backplane Connection > Address".
   The available network data is displayed in the right-hand area.

4. Check or configure the following settings:
   – The DHCP server function is deactivated.
   – The standard IP address 192.168.214.241 has been entered.
5. Click "Apply".
6. Select "File > Exit" in the menu to close the window.

Result

The NC/PLC and IPC components of the SINUMERIK MCU have now been configured and connected for internal network communication.

4.6 Installing SINUMERIK ONE Commissioning or Operate /PCU Modular

4.6.1 Installing SINUMERIK ONE Commissioning

Description

The SINUMERIK ONE Commissioning installation package is located on the installation medium supplied.

Note

The term "installation medium" is synonymous with USB, download, or other supplied media.

Requirement

- The hardware and software of the PC meet the system requirements.
- You have administrator rights on your computer.
- All running programs are closed.

How to install SINUMERIK ONE Commissioning

1. Navigate to the setup files on the installation medium of SINUMERIK ONE Commissioning.
2. Double-click "SINUMERIK_Commissioning.exe". The installation wizard opens.
3. Follow the wizard's instructions and confirm the prompts.
4. You must restart the computer once the installation has been completed.

SINUMERIK ONE Commissioning is now installed.

Further procedure

Set the PG/PC interface (Page 53) so that communication between SINUMERIK ONE Commissioning and the MCU is possible.

4.6.2 Operating software SINUMERIK Operate /PCU Modular

SINUMERIK MC Operate /PCU Modular or generally **SINUMERIK Operate /PCU Modular** enables you to use individual operating areas and to utilize them via the MCU IPC system. Use the operating software such as **SINUMERIK ONE Commissioning** for complex commissioning, diagnostics and archiving tasks. Develop your own operating dialogs and images for individual requirements.



Software option

You require the following software option in order to use SINUMERIK Operate /PCU Modular for MC:

- 6FC5800-0CQ11-0YB0 (print license CoI) or
- 6FC5800-0CQ11-0YH0 (electronic license eCoI)

SINUMERIK Operate /PCU Modular is an expandable basic application with the following operating areas:

- Commissioning
- Diagnostics

Note

Application does not include a program editor

A program cannot be used with SINUMERIK Operate /PCU Modular. Part programs and subprograms can neither be edited nor executed in operating area "Commissioning > System data".

4.6.2.1 Installing SINUMERIK Operate /PCU Modular

The **SINUMERIK Operate /PCU Modular** installation package is on the installation medium provided.

Note

The term "installation medium" is synonymous with USB, download, or other supplied media.

Requirement

- The hardware and software of the MCU IPC meet the system requirements.

  Note

  PCU-Basesoftware /IPC is installed.

- You have administrator rights on your MCU-IPC system.
- All running programs are closed.

How to install SINUMERIK Operate /PCU Modular

Navigate to the setup files on the installation medium of SINUMERIK Operate.

Perform the following installation options:

For a standard guided installation, double-click the *.exe setup file, follow the wizard's instructions and configure Autologon mode (Page 50).

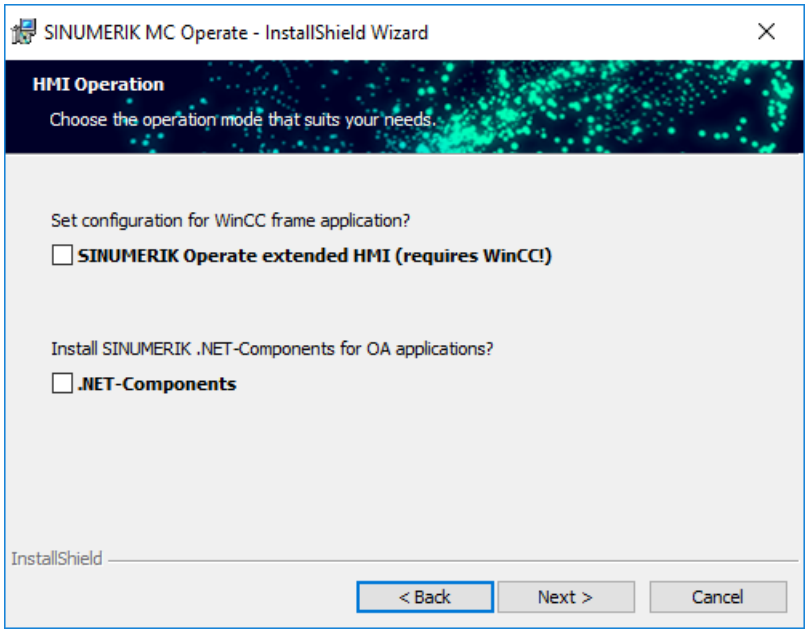


Figure 4-2 SINUMERIK Operate Installer - default setting

After successful installation, you must restart the MCU IPC system.
SINUMERIK Operate is now installed.

Note

Parallel SINUMERIK Operate installations on a PC system

It is possible to install further versions of the operating software on the MCU IPC system, e.g. for test purposes.

- During the installation of another version, change the main directory via the wizard:
  `C:\Program Files(x86)\Siemens\MotionControl\...`
  e.g. to
  `C:\Program Files(x86)\Siemens\MotionControl_V622\...`
- Avoid malfunctions between the versions. Only operate one SINUMERIK Operate application at a time.

Further procedure

- Configure the communication settings (Page 53) (PG/PC interface) on the MCU IPC system to enable communication between the PLC and SINUMERIK Operate.
- If required, set up the MCU connection (Page 55) so that communication between SINUMERIK Operate and the MCU is possible.
- Adjust the display size of (Page 53) SINUMERIK Operate, e.g. to improve operation on an external monitor.

4.6.2.2 Setting up SINUMERIK Operate for autologon mode

If you want the MCU-IPC system to start automatically in SINUMERIK Operate after switching on without having to make any further entries, set up the autologon mode.

When installing SINUMERIK Operate /PCU Modular, you can define an existing user account as an autologon account. The MCU IPC system then starts without the password for this user account being entered. SINUMERIK Operate is then started automatically because a link is created in the "Startup" Autostart folder.

For security reasons, you should use a special user account without administrator rights.

You can also configure the key filter and deactivate certain keyboard entries (Page 253), e.g. to prevent a switchover from SINUMERIK Operate to the Microsoft Windows desktop.

Requirement

- A Microsoft Windows user account without administrator rights is set up.
- SINUMERIK Operate /PCU Modular is not installed.
- You are logged on as an administrator or you know the password of the administrator account.
- The keyboard layout of the system (Page 206) is set to English.

Procedure

To set up autologon mode, proceed as follows:

1. Start installation of SINUMERIK Operate /PCU Modular and, in the installation wizard, proceed to step "Autologon".

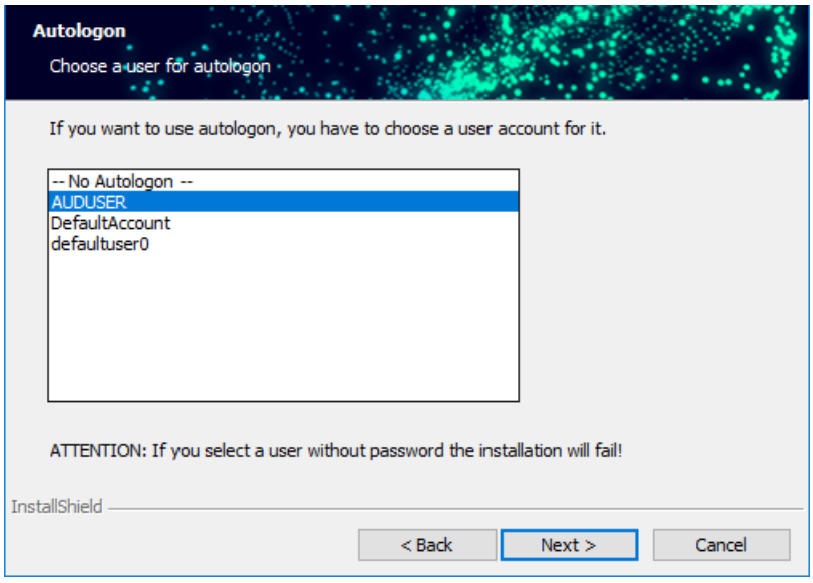


Figure 4-3 SINUMERIK Operate Installer - Autologon

2. In the list, select the user account to be logged on automatically.
3. Confirm with "Next", then in the next steps of the installation wizard make all the necessary settings and confirm the installation with "Finish".

Result

SINUMERIK Operate /PCU Modular is installed and autologon mode of the MCU IPC system is set up. During this process the password of the autologon user account is stored encrypted in Microsoft Windows, and SINUMERIK Operate is linked with the autostart folder "Startup".

Autologon mode is active at the next startup. The autologon user account is automatically logged on and SINUMERIK Operate is started.

4.6.2.3 Switching to the Service Desktop during autostart / autologon operation

If you have set up the autologon operation and the autostart of SINUMERIK Operate with the activated keyboard filter, the MCU IPC system runs up with SINUMERIK Operate after being switched on.

To be able to switch to the Windows desktop in this case, interrupt the run-up of SINUMERIK Operate with an entry, as described here.

Requirement

- SINUMERIK Operate /PCU Modular is installed and autologon mode is set up.
- The MCU IPC system is switched off.

Procedure

To switch to the desktop when the autostart/autologon mode is activated, proceed as follows:

1. Switch on the MCU IPC system and wait until the "SINUMERIK" splash screen is displayed.
2. While the "SINUMERIK" welcome screen is being displayed, make one of the following entries:
   - Press the key 3 on your keyboard.
   - Click or tip the copyright information.

   The counter for starting SINUMERIK Operate is suspended and you can select one of three options:

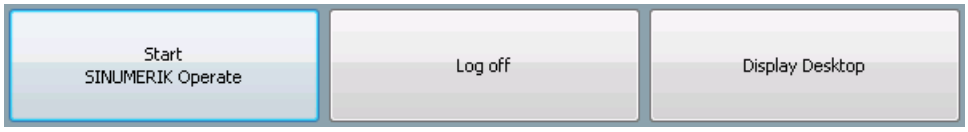


Figure 4-4 Welcome screen "SINUMERIK" after key input

3. Select the "Display Desktop" option.

Result

The Service Desktop opens.

4.6.2.4 Modifying the user account for autologon mode.

Because of the way autologon works, only one user account can ever be set up for autologon mode.

If you set up autologon mode during installation of SINUMERIK Operate /PCU Modular for one particular user account, but now want to use another user account for autologon mode, you can change this manually in the Service Desktop.

Requirement

- SINUMERIK Operate /PCU Modular is installed and autologon mode is set up.
- The Service Desktop is active.

Procedure

To change the user account that is used for automatic run-up in autologon mode, proceed as follows:

1. To open the "User Accounts" dialog box, proceed in one of the following ways:
   - On the Desktop, double-click the "Netplwiz" icon.
   - In the search field of the Start menu, enter `netplwiz` and confirm the entry.
   - At the prompt, enter `control userpasswords2`.

   The "User Accounts" dialog box opens.
2. Activate the "Users must enter a user name and password to use this computer" checkbox.

3. In the "Users for this computer" list, select the user account to be used for autologon mode.
4. Deactivate the "Users must enter a user name and password to use this computer" checkbox. You may be prompted to enter a password.
5. Confirm these settings in the "User Accounts" dialog box with "OK".
6. In the Autostart folder of the autologon mode user account, create a link to SINUMERIK Operate.

4.6.2.5 Configuring the SINUMERIK Operate display size

Adjust the SINUMERIK Operate display size, e.g. to improve the user interface operation on an external monitor with higher image resolution.

Procedure

Proceed as follows to configure the display size of SINUMERIK Operate:

1. Open the configuration file `slrs.ini` in the directory `...\MotionControl\user\sinumerik\hmi\cfg\`.
2. In the `[Global]` section, change the display size in the following lines:
   - `Resolution=`
     Sets the display size of the user interface
   - `DisplayResolution=`
     Sets the display size of the window area when the window mode is activated

   The following values are permissible: `640x480`, `800x600`, `1024x768` or `1280x1024`
3. Save and close the `slrs.ini` file.

Result

The display size is configured when you restart SINUMERIK Operate.

Note

Avoid display errors in the window mode of SINUMERIK Operate. Set at least the same value for `DisplayResolution` as for `Resolution`.

4.6.3 Configuring the PG/PC interface

Description

You must set the PG/PC interface to enable communication between TIA Portal respectively SINUMERIK ONE Commissioning or SINUMERIK Operate /PCU Modular and the MCU. To make the configuration, use the Siemens communication settings application.

If you select an interface parameter assignment, then assign this to the access point. This means that you establish the connection between the access point, the interface parameter assignment and the interface itself.

Requirement

The Siemens communications settings application is installed on the MCU IPC system.

Note

The application is a system tool and is part of the SINUMERIK ONE Commissioning or Operate / PCU Modular installation.

This is how you configure the PG/PC interface using the Siemens communication settings application

1. Under Windows, select "Start > Control Panel" > "All control panel elements"
2. Click "Communication settings".
   The "Siemens communication settings" window opens.
3. Click "Access points" in the navigation.
   The available access points (S7ONLINE, SINUMERIK_CP) are displayed in the right-hand area.
4. Click the arrow in front of "S7ONLINE" to display the settings.
5. In the "Used interface parameter assignment" field, select the "<network adapter>.TCPIP.1" entry. <network adapter> is a placeholder for the interface name of your deployed hardware.
6. Click "Apply".
7. Click the arrow in front of "SINUMERIK_CP1543" to display the settings.
8. In the "Assigned interface parameter assignment" field, select the "<network adapter>.TCPIP.1" entry. <network adapter> is a placeholder for the interface name as used previously.
9. Click "Apply".
10. Select "File > Exit" in the menu to close the window.

Note

If you have installed SINUMERIK ONE Commissioning or SINUMERIK Operate /PCU Modular on the MCU, then use the interface "Intel(R) I210 Gigabit Backplane Connection" in the access point.

Result

You have now configured the access points for the application. The user interface can be used.

4.6.4 Starting and setting up SINUMERIK ONE Commissioning or Operate /PCU Modular

Description

- When you start SINUMERIK ONE Commissioning on the PC, the application initially opens without the MCU connection.
- When you start SINUMERIK ONE Commissioning on the MCU, then the application is opened with the preset MCU IPC connection.
- When you start SINUMERIK Operate /PCU Modular on the MCU, then the application is opened with the preset MCU-IPC connection.

Note

Use the applications in the same way as the user interface of SINUMERIK Operate familiar to you.

Starting SINUMERIK ONE Commissioning

1. Select "Start > Siemens Automation > SINUMERIK ONE Commissioning"
   The user interface of SINUMERIK ONE Commissioning is displayed.
2. Select the "Commissioning" operating area and press the "Change language" softkey.
   The language selection opens.
3. Select your language and click "OK".
4. In the "Commissioning" operating area, press the "Password" softkey.
5. Press the "Set password" softkey, enter the manufacturer password and confirm with "OK".
   A valid password is acknowledged as set and the manufacturer access level is set.

Starting SINUMERIK Operate /PCU Modular

1. Select "Start > Siemens Automation > SINUMERIK MC Operate"
   The user interface of SINUMERIK Operate is displayed.
2. Select the "Commissioning" operating area and press the "Change language" softkey.
   The language selection opens.
3. Select your language and click "OK".
4. In the "Commissioning" operating area, press the "Password" softkey.
5. Press the "Set password" softkey, enter the manufacturer password and confirm with "OK".
   A valid password is acknowledged as set and the manufacturer access level is set.

More information

More information on access levels is provided in Chapter "Access levels (Page 57)".

Changing the user interface connection with MCU manually

1. In the "Commissioning" operating area, select the softkeys "HMI > cursor key > NCU Connection".
   The "NCU Connection" dialog box opens.
2. Select address type "IP Address", enter the value for MCU connection X130 (company network) and confirm with "OK".
   The user interface connects to the MCU after a restart.

On this user interface, you parameterize the machine data and drives that you need for your SINUMERIK MC environment.

Note

Alternatively, you can also configure the connection between the user interface and the MCU via the file `mmc.ini`.

Copy of the file from directory `.../siemens/sinumerik/hmi/cfg` and insert the copy below `user` or `oem` with the same path. Change the IP addresses and start the application.

4.7 Access levels

Access to functions and machine data

The access concept controls access to functions and data areas. Access levels 1 to 7 are available, where 1 represents the highest level and 7 the lowest level. Access levels 1 to 3 are locked using a password and 4 to 7 using the appropriate key-operated switch.

Access level	Locked by	Area	Data class
1	Password: SUNRISE	Manufacturer	Manufacturer (M)
2	Password: EVENING	Service	Individual (I)
3	Password: CUSTOMER	User	User (U)
4	Key-operated switch setting 3	Programmer, machine setter	User (U)
5	Key-operated switch setting 2	Qualified operator	User (U)
6	Key-operated switch setting 1	Trained operator	User (U)
7	Key-operated switch setting 0	Semi-skilled operator	User (U)

The password remains valid until it is reset with the "Delete Password" softkey. The passwords can be changed after activation.

If, for example, the passwords are no longer known, reinitialization (boot-up with "NCK default data") must be carried out. This resets all passwords to the default (see table). A power-on reset does not reset the password.

Key-operated switch

Access levels 4 to 7 require a corresponding key-operated switch setting on the machine control panel. Three keys of different colors are provided for this purpose. Each of these keys only provides access to certain areas.

Access level	Switch position	Key color
4-7	0 to 3	Red
5-7	0 to 2	Green
6-7	0 and 1	Black
7	0 = Key removal position	No key inserted

The position of the key-operated switch can be processed by the PLC program, and appropriately transferred to the NC/PLC interface .

Password security

Note

Assigning secure passwords

Observe the following rules when assigning new passwords:

- When assigning new passwords, never choose passwords that can be easily guessed, e.g. simple words, sequences of consecutive keys on the keyboard, etc.
- Passwords must always contain a combination of upper-case and lower-case letters as well as numbers and special characters. Passwords must comprise at least 8 characters. PINS must comprise an arbitrary sequence of digits.
- Wherever possible and where it is supported by the IT systems and the software, a password must always have a character sequence as complex as possible. You can use a password management program to assist you when dealing with passwords. With its help, you can save passwords and PINs in encrypted form, manage them and generate secure passwords.

Note

Changing passwords between SINUMERIK ONE Commissioning and NC

The access levels for SINUMERIK ONE Commissioning and the NC have been merged. If you change a password for SINUMERIK ONE Commissioning, this simultaneously changes the corresponding NC password and vice versa. It is important to note the following behavior:

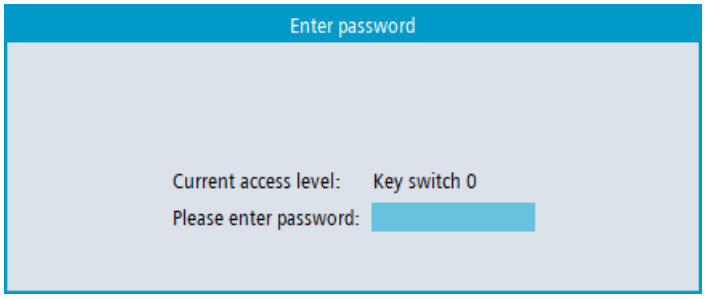
- When a general NC reset is performed, no passwords are reset to the default passwords.
- Following a software update, the SINUMERIK ONE Commissioning passwords apply to the NC.
- Once changed, a password can no longer be reset - not even by SIEMENS service. Therefore, make sure that you store the changed password in a safe place.

Entering the password

Procedure:

1. Open the SINUMERIK ONE Commissioning application.
2. Select the "Commissioning" operating area and press the "Password" softkey.

3. Press the "Enter password" softkey. The current key-operated switch setting is displayed first:



4. Enter the password for the desired access level and confirm this input with "OK" or with the <INPUT> button.
   A valid password is acknowledged as set and the access level is set. Invalid passwords will be rejected.

Pressing the "Delete password" softkey deletes the last valid password and displays the current key-operated switch setting again.

Note

Delete password

The password can also be deleted via the → PI service: LOGOUT

Further information on the PI service LOGOUT is provided in Function Manual Reference to the PLC basic program.

Rules relating to the password structure

Note

Invalid passwords are rejected by the operating software. Note the rules for strong passwords:

- A password must contain at least 8 and can contain up to 32 characters.
- Permissible characters are:
  - Uppercase characters
  - Lowercase characters
  - Numbers
  - Special characters (ASCII 0x20 - 0x7E)
- The character combination of a password must contain:
  - At least one number
  - At least one uppercase letter
  - At least one lowercase letter
- A password must not be too similar to the following names:
  - User names (manufacturer, service, user)
  - Computer name
  - The additional values that can be stored for a user in the Linux password file (so-called GECOS data)

We recommend that you confine yourself to the characters available on the operator panel front when selecting a password.

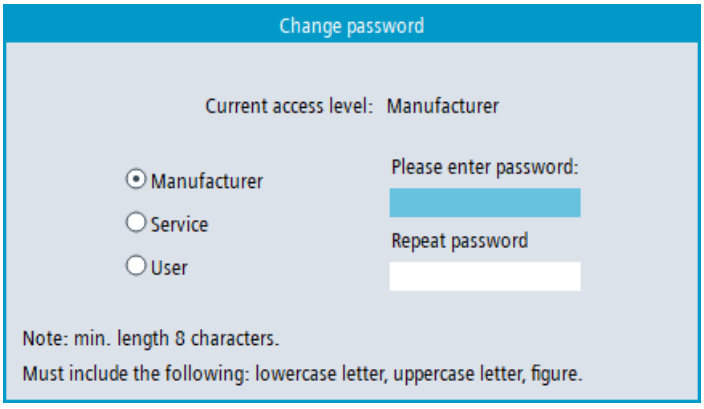


This information can also be found in the online help of SINUMERIK ONE Commissioning.

Change password

Procedure:

1. To change the default password from the delivery condition, press the "Change password" softkey.
2. The previous password must first be confirmed. After successful authentication, you are forwarded automatically to the following dialog:



3. Enter the new password and the repetition, and then confirm with the "OK" softkey. If both passwords match, the new password becomes valid and is adopted by the system.

4.8 Read-out the MCU serial number for the TIA Portal configuration

The serial number automatically read-out in the TIA Portal does not correspond to the MCU1720 nameplate serial number. In order to guarantee a unique assignment, the serial number of the F-PLC (internal MCU-NC board) must be read out when commissioning.

Possibilities

There are two ways in which you can read-out the serial number:

1. Read-out the serial number via the service system (USB flash drive) in menu item: "Show Status > Mainboard/SerialNo"
2. Read-out the serial number via SINUMERIK ONE Commissioning in operating area: "Diagnostics > Version > Hardware"

More information is available in the TIA Portal help, e.g. for configuring a Safety Integrated safety solution (F-PLC).

Licensing 5

5.1 SINUMERIK License Key

Basic information on license keys

If a license is required for a product, the purchaser receives a CoL (Certificate of License) with the purchase of the license as proof of the right to use this product together with a corresponding license key as the "technical representative" of this license. In conjunction with software products, the license key usually must be available on the hardware on which the software product is executed.

Note

Trial License

A trial license supports "short-term use" of the software in a non-productive context, e.g. use for testing and evaluation purposes; it can be transitioned into another license.

SINUMERIK license keys

Depending on the software product, there are license keys with different technical properties. The essential properties of a SINUMERIK license key are:

- Hardware serial number
  Via the hardware serial number contained in the SINUMERIK License Key, there is a direct relationship between the License Key and the hardware on which it may be used. That means that a license key that was generated for the hardware serial number of a certain SD Card is also only valid on this SD Card and rejected as invalid on another SD Card.
- Total number of assigned licenses
  A SINUMERIK license key not only refers to a single license, instead it is the "technical representative" of all licenses that are assigned to the hardware at the time of its generation.

Content of the SD Card

The SD Card contains the system and user software, the retentive system and user data, along with the data relevant for the license management of SINUMERIK software products of a control system:

- Hardware serial number
- License information including the license key

This means that the SD Card represents the identity of a SINUMERIK control system. This is the reason that licenses are always assigned to a control using the hardware serial number of the SD Card.

This has the advantage that in the event of the failure of the MCU, the SD Card can be inserted into a replacement MCU, and all data is retained.

SD Card as spare part

If the SD Card of a SINUMERIK control is replaced, for example, because of defective hardware, the license key loses its validity and the system is no longer operational.

Contact "Technical Support" if you have an SD Card with a hardware defect. They will then send you a new license key without delay. The following data is required:

- Hardware serial number of the defective SD Card
- Hardware serial number of the new SD Card

Note

Only SD Cards that have been released as a spare part can be used, as only these are known to the license database.

Determining the hardware serial number

The hardware serial number is a permanent part of the SD Card. It is used to identify a control system uniquely. The hardware serial number can be determined by:

- Certificate of License (CoL Print license, eCoL electronic license)
- SINUMERIK user interface
- Print on the SD Card

Note

Hardware serial number and CoL

The hardware serial number is located only on a CoL of the system software or if the license was ordered bundled, in other words the system software came together with options.

5.2 Web License Manager

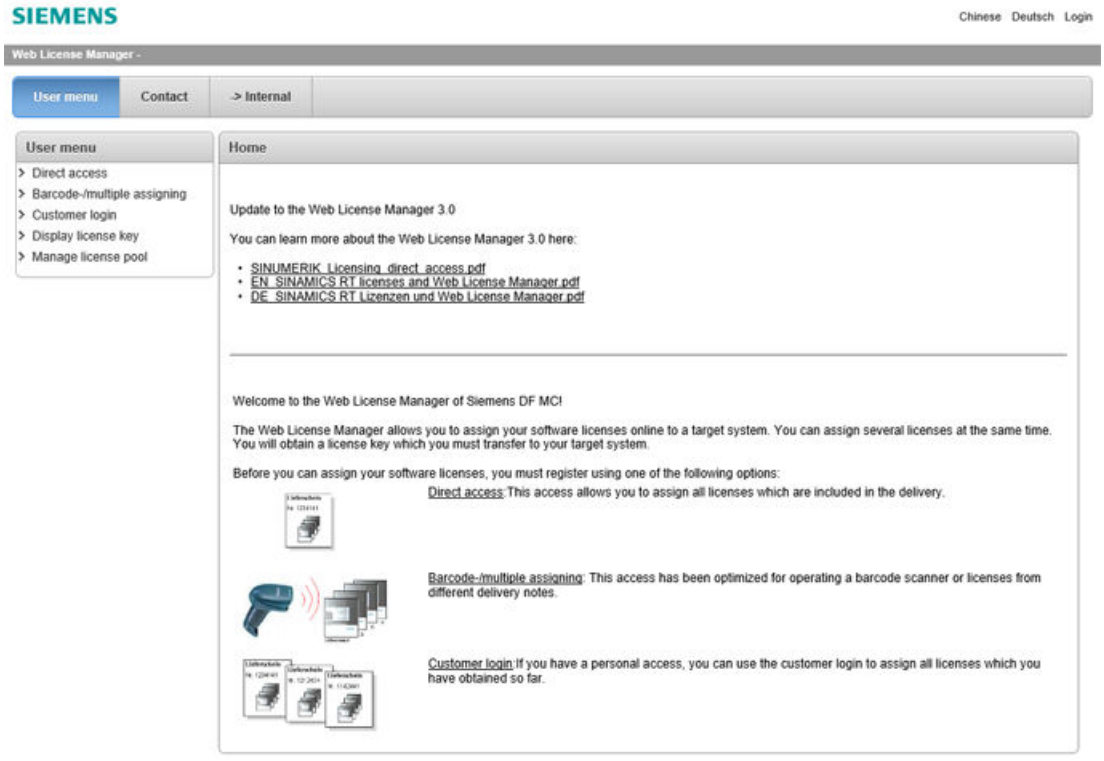
Overview

The use of the installed system software and the options activated on a SINUMERIK control system require that the licenses purchased for this purpose are assigned to the hardware. In the course of this assignment, a license key is generated from the license numbers of the system software, the options, as well as the hardware serial number. Here, a license database administered by Siemens is accessed via the Internet. Finally, the license information including the license key is transferred to the hardware.

The license database can be accessed using the Web License Manager.

Web License Manager

By using the Web License Manager, you can assign licenses to the hardware in a standard Web browser. To conclude the assignment, the license key must be entered at the controller via the user interface.



Internet links

Web License Manager (http://www.siemens.com/automation/license)

Siemens Industry Mall (http://mall.automation.siemens.com)

5.3 License database

License database access

The license database contains all relevant license information required for the license management of SINUMERIK software products. The central management of the license information in the license database ensures that the existing license information regarding a piece of hardware is always up to date.

Direct access

The direct access in the Web License Manager is made with:

- License number
- Delivery note number

The direct access enables the direct assignment of licenses for which the license numbers are available, e.g. in the form of a CoL.

Direct access with barcode scanner

The direct access in the Web License Manager is made with:

- Hardware serial number
- Product selection

The direct access enables the assignment of licenses with a barcode scanner for which the license numbers are available as a barcode, for example in the form of a CoL.

Customer login

The customer login in the Web License Manager is made with:

- User name
- Password

The customer login allows the assignment of all licenses available to the machine OEM that have been provided up to the instant of login, and which have not yet been assigned to any hardware serial number (SD Card). Here, the license numbers of licenses that can still be assigned need not be directly at hand, instead these are displayed from within the license database.

Note

Obtaining access data

You can obtain the address data for the customer login from the Siemens Industry Mall under the associated selected region with: "> Register" (top).

5.4 How to perform the assignment

Assigning a license to a piece of hardware

1. Determine the hardware serial number and the product name ("type of hardware") on the user interface via the licensing dialog:
   Commissioning > menu forward key > Licenses > Overview operating area

   Note

   Ensure that the hardware serial number displayed is also really the one you want to make the assignment for. The assignment of a license to a piece of hardware cannot be reversed via the Web License Manager.

2. Go to the Internet page of the Web License Manager.
3. Click the appropriate access to the license database:
   - Direct access
   - Direct access (barcode scanner)
   - Customer login
4. Follow the instructions in the Web License Manager.
   A progress bar shows you the individual steps:

5. Check the details of the selected licenses before confirmation of the assignment process.

   Note

   After confirmation, the generated license key irrevocably links the selected licenses with the specified hardware.

6. Confirm the assignment process.
7. After completing the assignment process, enter the license key displayed on the Web License Manager into the license dialog of the user interface.
   Commissioning > menu forward key > Licenses > Overview operating area
8. Press the <INPUT> button to confirm the input of the new license key.

Displaying the license key and sending via e-mail

For archiving or for documentation of the associated machine, you can also send a license report with the grouping of all assigned licenses. Follow the instructions in the Web License Manager under "Display License Key".

5.5 Important licensing terms

Certificate of License (CoL Print license, eCoL electronic license)

The CoL or eCoL is the proof of a → license. The product may only be used by the holder of the → license or authorized persons. The CoL includes the following data relevant for the license management:

- Product name
- License number
- Delivery note number
- Hardware serial number

SD Card

As the carrier of all retentively saved data of a SINUMERIK control system, the SD Card represents the identity of this control system. The SD Card is a memory card that can be inserted into the → MCU from the outside. The SD Card also contains the following data relevant for the license management:

- Hardware serial number
- License information including the → license key

Hardware

In the context of license management of SINUMERIK → software products, hardware refers to the component of a SINUMERIK control to which → licenses are assigned on the basis of its unique identifier. The license information is also retentively saved on this component, e.g. on an → SD Card.

Hardware serial number

The hardware serial number is a permanent part of the → SD Card and cannot be changed. It is used to identify a control system uniquely. The hardware serial number can be determined by:

- → Certificate of License
- User interface
- Print on the → SD Card

License

A license gives the user the legal right to use a → software product. Evidence of this right is provided by the following:

- → Certificate of License (CoL)
- → License key

License key

The License Key is the "technical representative" of the sum of all the → licenses that are assigned to one particular piece of → hardware, which is uniquely identified by its → hardware serial number.

License number

The license number is the feature of a → license used for its unique identification.

Option

An option is a SINUMERIK → software product that is not contained in the basic version and which requires the purchase of a → license for its use.

Product

A product is marked by the data below within the license management of SINUMERIK → software products:

- Product designation
- Article number
- License number

Software product

The term software product is generally used to describe a product that is installed on a piece of → hardware to process data. Within the license management of SINUMERIK software products, a corresponding → license is required to use each software product.

PLC commissioning

6

6.1 PLC commissioning: Overview

The PLC of a SINUMERIK MCU is always installed in the TIA Portal.

You commission the PLC by performing the following work steps (Page 31):

1. Configuring the PLC
   - Create a project
   - Insert an MCU
   - Configure network settings
   - Establish the communication connection
   - Load hardware configuration into the PLC
2. Creating and loading the PLC program
   - Create the PLC basic program and insert it into the project
   - Edit the blocks
   - Load the PLC program into the PLC
   - Complete first commissioning of the PLC

6.2 Starting the TIA Portal

Requirement

- TIA Portal is installed.
- SINUMERIK STEP 7 Toolbox is installed.

Procedure

1. Start the TIA Portal by double-clicking the link to the Windows desktop or from the start menu under "All Programs > Siemens Automation > TIA Portal".

Result

The TIA Portal opens. The functions of a SINUMERIK MCU are now available to you in the TIA Portal.

6.3 Configuring the PLC

6.3.1 Create a project

Introduction

You create a new project in the following. Within a project, all of the automation tasks required, for example the hardware configuration and the PLC programming, are performed.

Precondition

- The TIA Portal has been started.

Procedure

1. Click "Create new project" in the portal view.



2. Assign a project name and select the storage location of the project (path).
3. Click "Create".

Result

A new, empty project has been created.

6.3.2 Inserting an MCU

Introduction

A SINUMERIK MCU comprises an open-loop control-specific part (PLC, CP and NCK) and a PC-specific part (PC system).

When creating a SINUMERIK MCU in the TIA Portal, all subcomponents and the PC system are simultaneously created.

Ethernet is used for the internal communication between the various components.

Precondition

- A project is open in the TIA Portal.
- The project view is active.

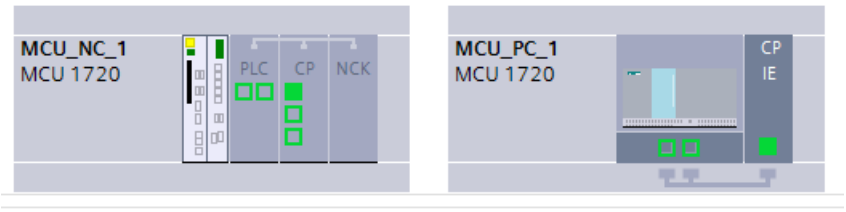
Procedure

To insert an MCU into the project, follow these steps:

1. Click "Add new device" in the project tree.
2. Click the "Controllers" button.
3. In the folder structure under "Controller", expand the corresponding SINUMERIK device family and then select the MCU 1720.
   The firmware version of the MCU is displayed in the "Version" drop-down list.
4. Confirm your selection with "OK".

Result

The SINUMERIK MCU 1720 is created as new device.



Note

You can connect distributed PROFINET I/O devices at interface X150 or X160.

PROFINET I/O devices, which are to be accessed by the NCK, must be connected to X150.

To exchange distributed data, assign the process image PIP NCK to the I/O device.

If additional PROFINET I/O devices are connected to X150 and commissioning is to be performed via SINUMERIK ONE Commissioning on the IPC, the CP interface must be set up. Configure the subnet of the CP interface in the TIA Portal, e.g. under the tab "Devices & Networks".

6.3.3 Configuring the PC system

Introduction

When creating a SINUMERIK MCU in the TIA Portal, all subcomponents and the PC system are simultaneously created.

Install WinCC RT Advanced on the PC system if you wish to use the PC system for using the customized user interfaces.

You can configure and customize the operating area.

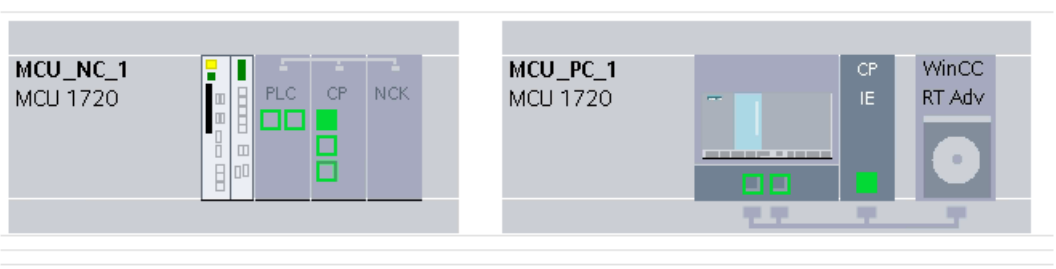
Further information on this topic is provided in the TIA Portal help in Chapter "SINUMERIK user interfaces".

Precondition

- A project is open in the TIA Portal.
- A SINUMERIK MCU has been created.
- The device view is active.

Procedure

1. Double-click "Device configuration" under "PC system" in the project tree.
   The device configuration for the PC system is displayed.
2. In the Hardware catalog, select the runtime software under "SIMATIC HMI application > WinCC RT Advanced" and drag it to a free slot of the device in the Network view.



Result

In the project tree, the configured Runtime "HMI_RT_1 [WinCC RT Advanced]" is added to the created PC system.

This view provides the following configuration editors, among others:

- "Connections"
- "HMI variables"
- "HMI messages"
- "Screens"

6.3.4 Configuring PROFINET for SINUMERIK MCU

Introduction

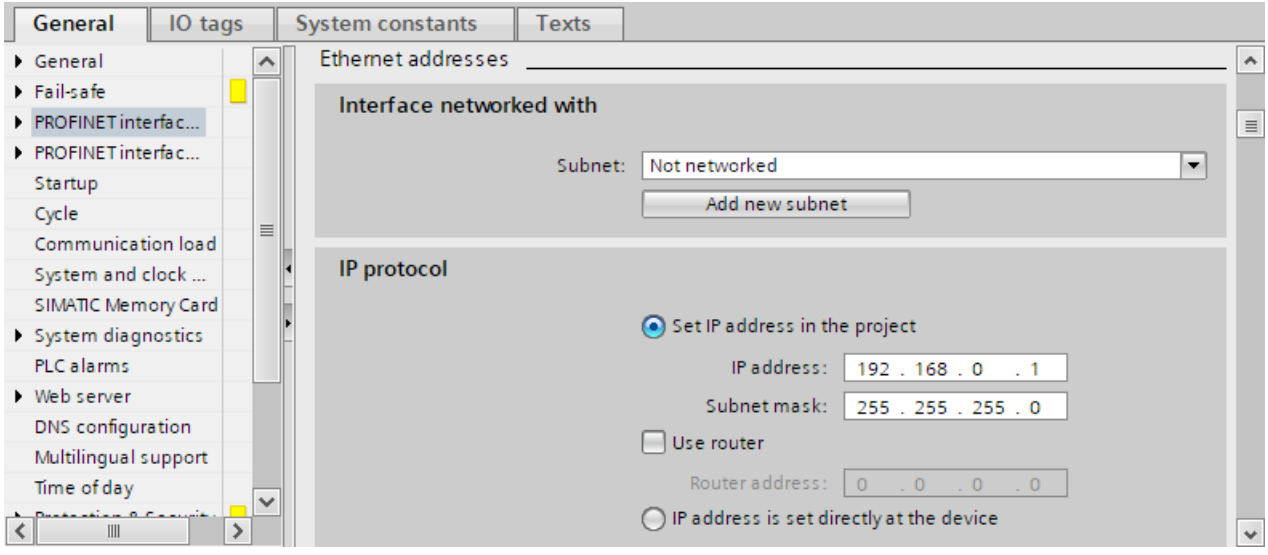
Internal and external communication between the devices involved is established via the PROFINET interfaces.

In order that PROFINET participants can be correctly addressed, the configured addresses must be set at the various participants.

Procedure

Proceed as follows to configure the PROFINET interface of the SINUMERIK MCU:

1. In the network view, click the PLC in the basic rack of the SINUMERIK MCU.
2. Switch to the inspector window "Properties > General".
   You can configure the IP addresses of the various PROFINET interfaces in the respective associated properties:
   - PROFINET interface [X150]
   - PROFINET interface [X160]



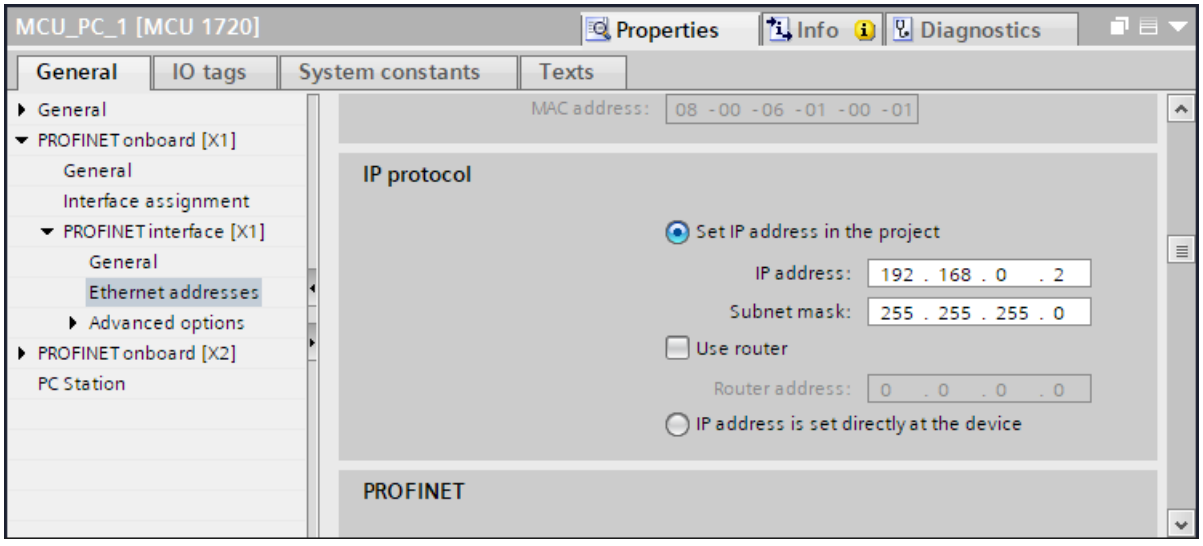
3. Under "IP protocol", in each case check as to whether the correct IP address is set ("192.168.0.1" for X150 in the example).

You can find **more information**, e.g. external drive devices/I/O devices (RT/IRT) connected at X160, which can be assigned to the NCK and the process image partition (TPA NCK), in the TIA Portal help.

6.3.5 Configuring PROFINET on the PC system

Procedure

1. In the network view, click on the PC system in the basic rack of the SINUMERIK MCU.
2. Switch to the inspector window "Properties > General".
   You can configure the IP addresses of the various PROFINET interfaces in the respective associated properties:
   - PROFINET onboard [X1]
   - PROFINET onboard [X2]



3. Under "PROFINET onboard > PROFINET interface > Ethernet addresses", in the "IP protocol" area, set the IP address of the interface on the PC system under "Address".

6.3.6 Compile hardware configuration

Introduction

For a SINUMERIK MCU and the associated PC system, you compile and load separately and in any sequence.

Procedure

To compile the configured hardware configuration, proceed as follows:

1. In the project tree, right-click on the SINUMERIK MCU, and select the "Hardware" command in the "Compile" shortcut menu.
2. To compile the PC system, right-click on "PC-System_1" and, in the "Compile" shortcut menu, select command "Hardware".
   The consistency of the hardware configuration is tested in the compilation process. Remedy any errors that may occur and compile the project again.

Result

The PC system and the SINUMERIK MCU, with the integrated subcomponents PLC, CP and NCK, have been compiled.

6.3.7 Establish the communication connection

Introduction

To be able to load the configuration to the PLC, a communication connection (Ethernet) must be established between the PG/PC and the PLC.

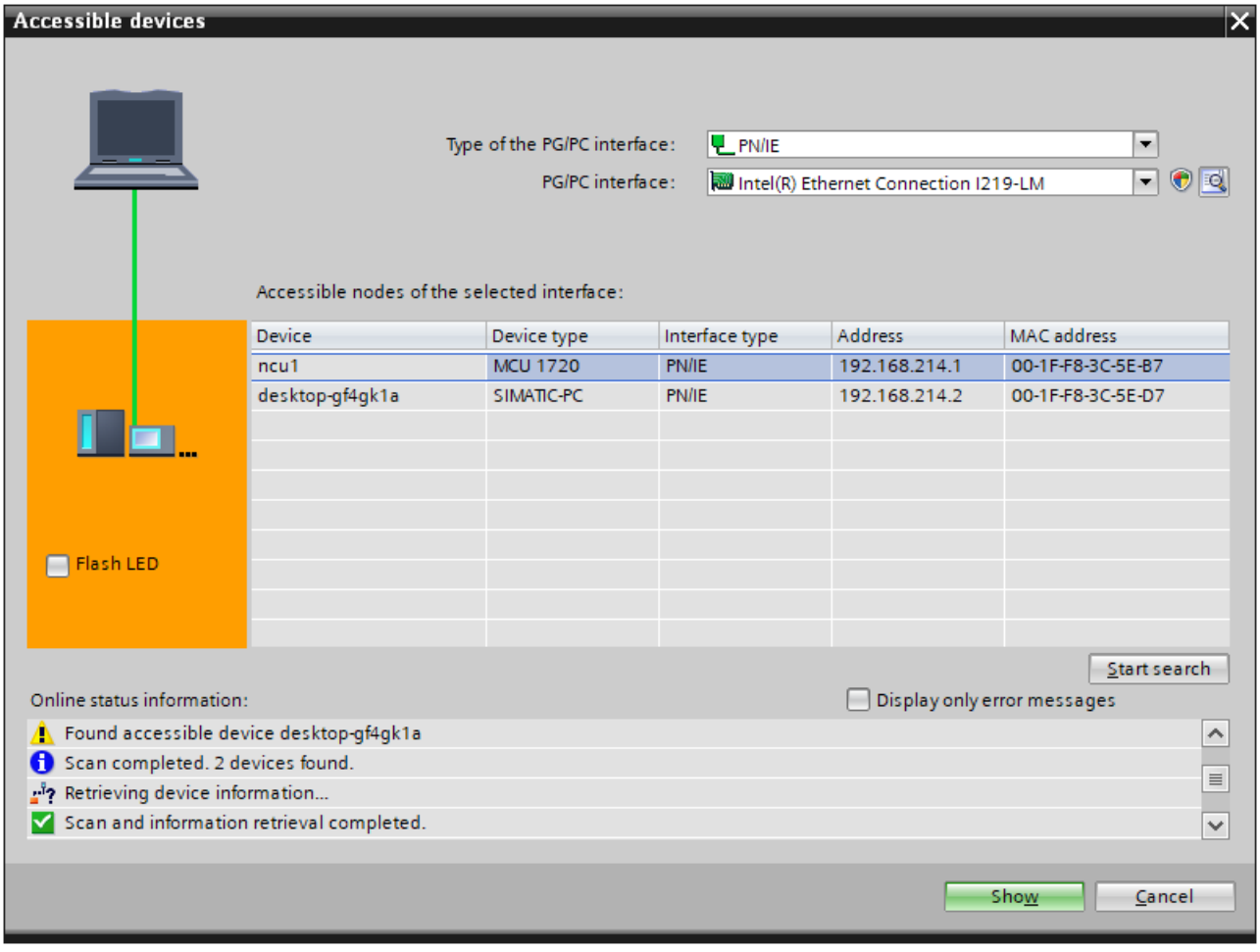
You can use one of the following interfaces or ports to load the configuration to the PLC.

- X127
- X130 (if port 22 is open)
- X150.P1 PN
- X150.P2 PN
- X160 PN

Procedure

To establish a communication connection between two devices, proceed as follows:

1. In the "Online" menu, select the "Accessible nodes" command.
2. In the drop-down lists "Type of PG/PC interface" and "PG/PC interface", search for the interface used.
   If no devices are accessible at an interface, the connecting line between the PG/PC and the device is interrupted. If devices are accessible, the connecting line is shown, and the accessible nodes at the selected interface of the PG/PC are displayed in a list.



Note

The PC system is also displayed as a communication node.

3. If you have connected a new device in the meantime, click the "Refresh" button to refresh the list of accessible nodes.
4. Using "Display", transfer to the project tree the device that has been found in the "Online accesses" folder.
   The subfolder of the interface to which the selected device is connected is selected in the project tree.

Note

Several identical devices

If several identical devices can be accessed from the PG, by clicking on the "Flash LED" button you can then display which device corresponds to the entry in the list of accessible nodes.

6.3.8 Load hardware configuration into the PLC

Introduction

The project must be saved and compiled before the system data is created for the PLC and the complete configuration can be closed.

Precondition

- The hardware configuration is compiled.
- A communication connection exists between the PG/PC (TIA Portal) and the SINUMERIK MCU.

Procedure

Proceed as follows to load the configured hardware configuration to the MCU:

1. In the project tree, right-click the device name, e.g. "MCU", and select the "Download to device > Hardware configuration" command in the shortcut menu.

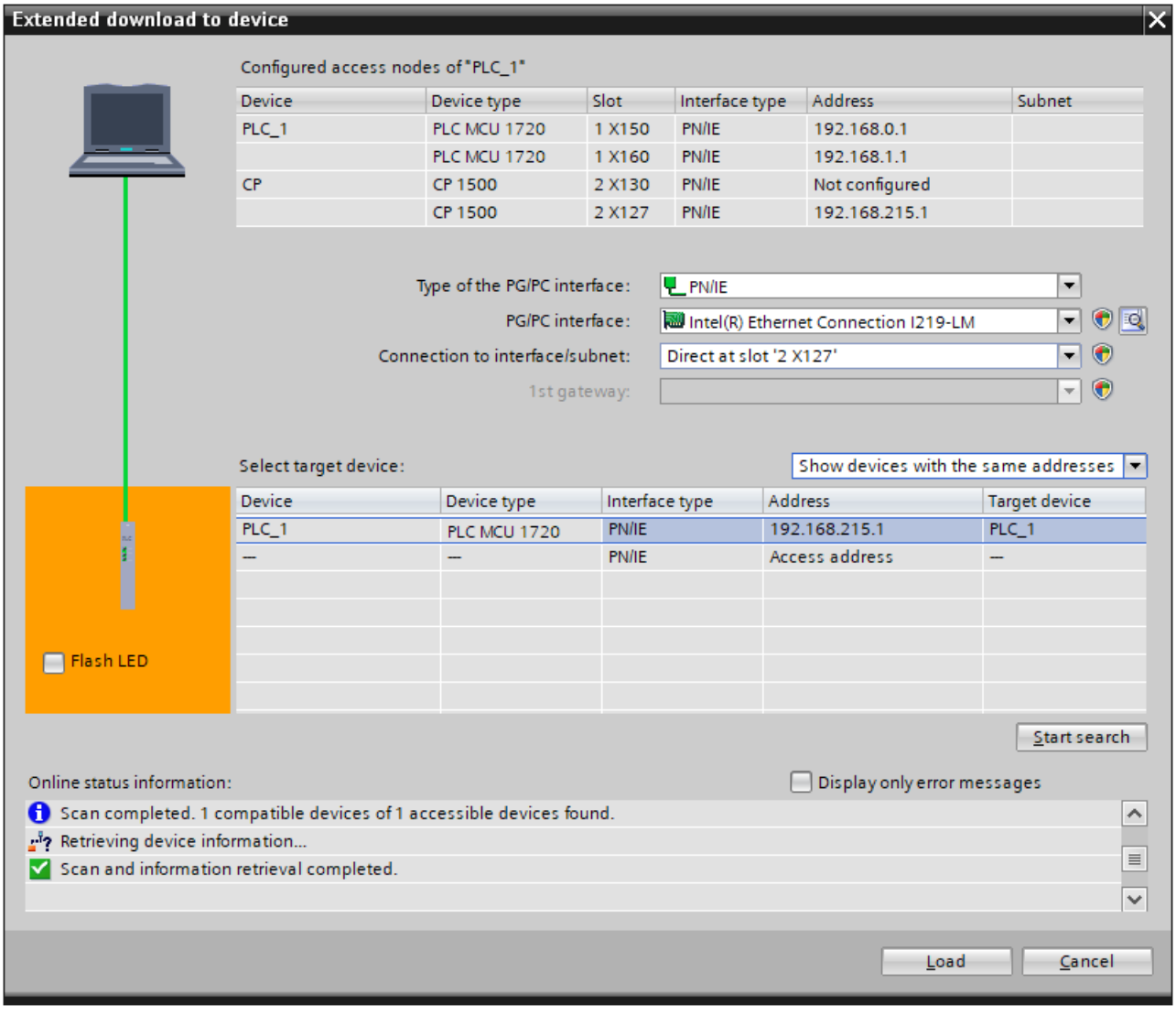
   Note

   Scope of the data to be downloaded

   Alternatively, you can select one of the other commands to start downloading additional data to the MCU in this step.

   See TIA Portal help, keyword "General information on downloading".

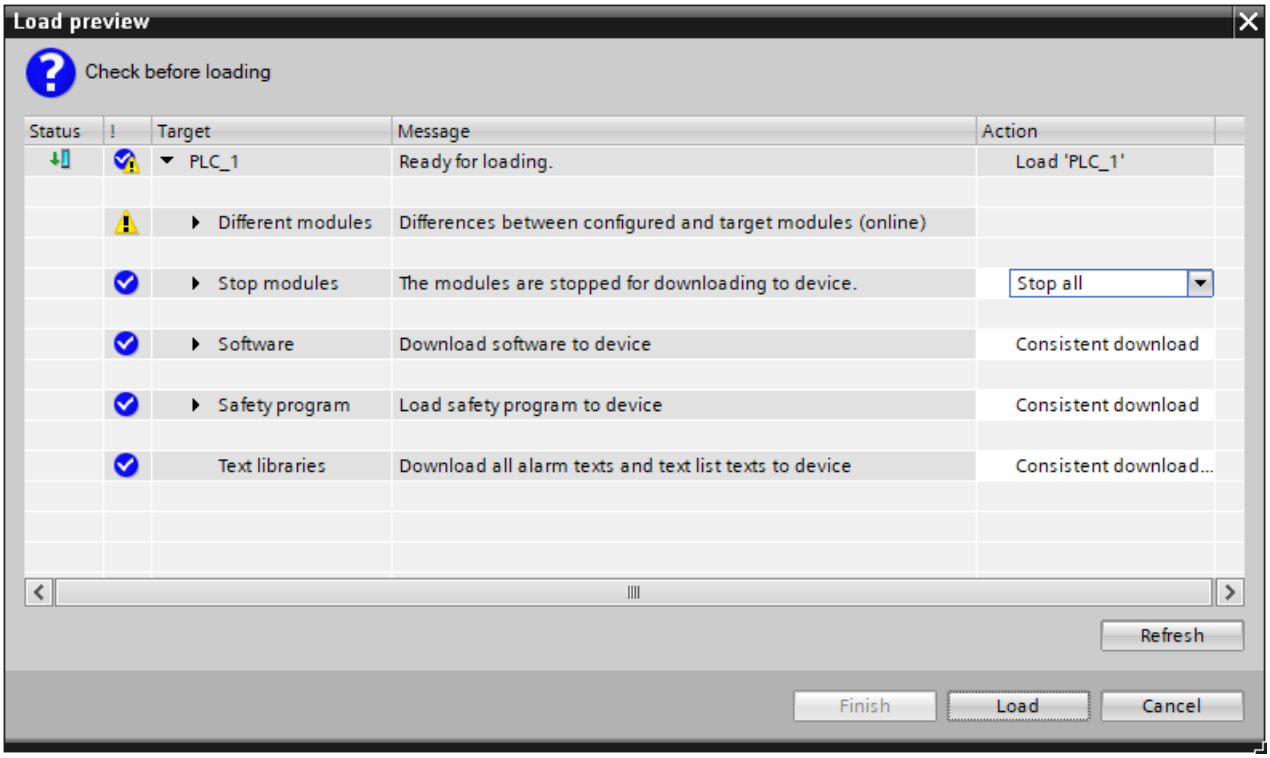
   The "Extended download" dialog opens.



2. Make the following settings in the "Extended download" dialog:
   – PG/PC interface: Network card used, e.g. "Intel[R] Ethernet Connection I217-V"

– Connection with interface/subnet: Specific interface on the MCU or "Try all interfaces"

3. Click on "Start search" and then select the found PLC from "Compatible nodes in the target subnet". Alternatively, you can specify an IP address directly in the "Compatible nodes in the target subnet" list in the "Address" column.
4. Confirm the download with "Load".
   The "Download preview" dialog opens.



Note

Consistency check

Before the loading, the consistency of the download is checked. This means that a check is performed as to whether the parameterized hardware of the TIA Portal project matches the hardware that has actually been installed.

Note

Adapt the IP address?

If the IP address of your PG/PC is located in a different subnet than the PLC, a dialog box is displayed as to whether the IP address in the PG/PC should be adapted.

5. In the "Download preview" dialog, check the settings and click "Load" to confirm the input.

Result

The PLC is stopped and the configuration is loaded to the PLC. The "Results of the loading action" dialog opens and displays the status of the loading action. The dialog restarts the PLC after completion provided the "Start" checkbox has not been disabled.

6.3.9 Loading the WinCC runtime project into the PC system

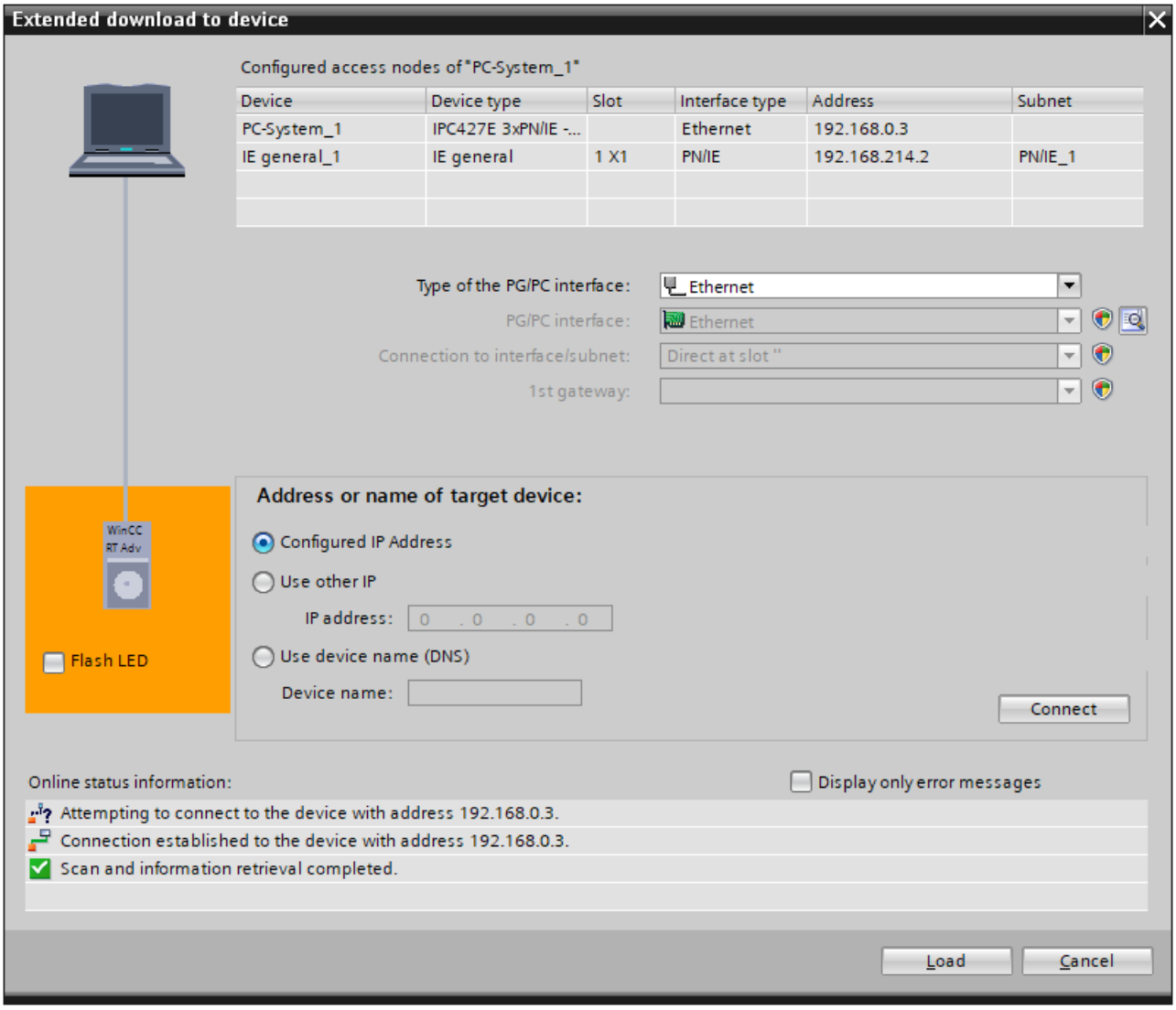
Precondition

- The project has been compiled.
- A communication connection exists between the PG/PC (TIA Portal) and the PC system.
- You have started the WinCC Runtime Loader.

Procedure

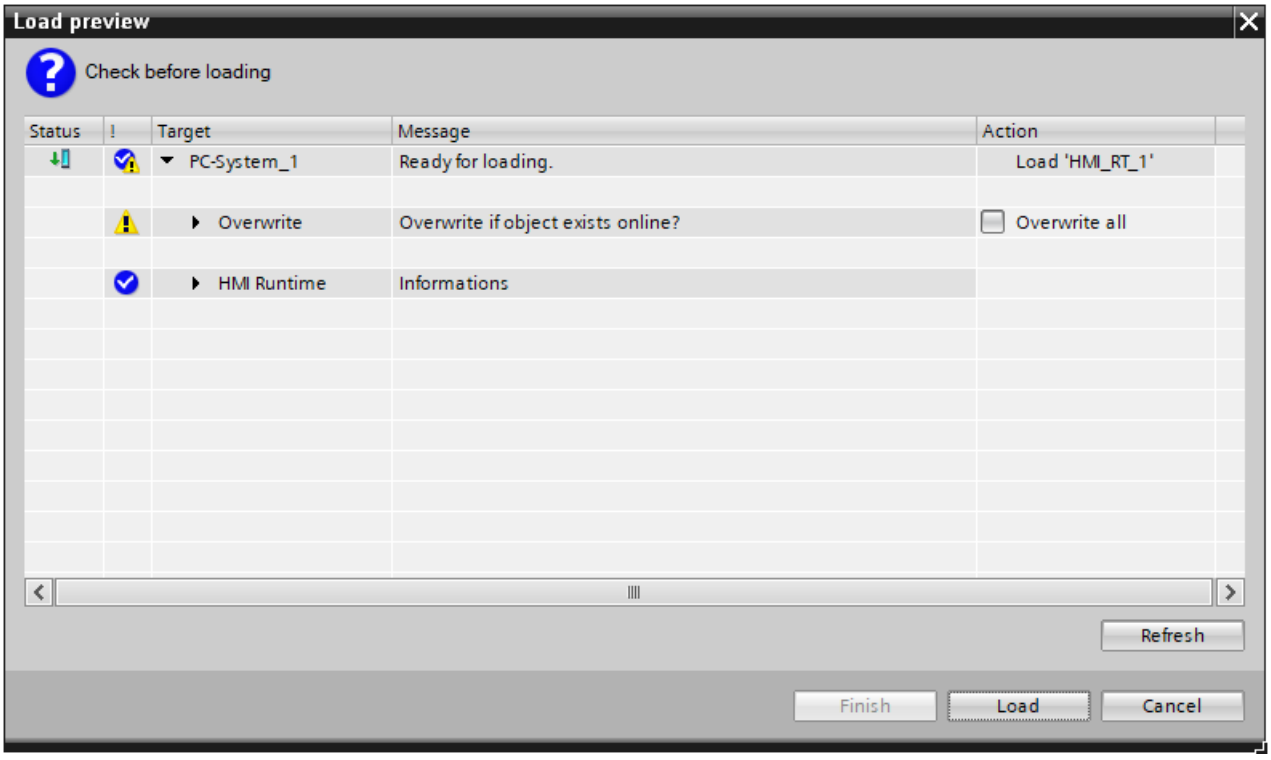
Proceed as follows to load the configured hardware configuration to the PC system:

1. In the project tree, right-click the device name, e.g. "PC system_1", and select the "Hardware configuration" command in the "Download to device" shortcut menu.
   The "Extended download" dialog opens.



2. Make the following settings in the "Extended download" dialog:
   – PG/PC interface: Network card used, e.g. "Intel[R] Ethernet Connection I217-V"
3. Click on "Start search" and then select the found IPC from "Compatible nodes in the target subnet". Alternatively, you can specify an IP address directly in the "Compatible nodes in the target subnet" list in the "Address" column.

4. Confirm the download with "Load".
   The "Download preview" dialog opens.



Note

Consistency check

Before the loading, the consistency of the download is checked. This means that a check is performed as to whether the parameterized hardware of the TIA Portal project matches the hardware that has actually been installed.

Note

Adapt the IP address?

If the IP address of your PG/PC is located in a different subnet than the IPC, a dialog box is displayed indicating whether the IP address in the PG/PC should be adapted.

5. In the "Download preview" dialog, check the settings and click "Load" to confirm the input.

Result

The software configuration is loaded to the IPC. The "Results of the loading action" dialog opens and displays the status of the loading action.

6.4 Creating a PLC program

6.4.1 Overview of the PLC program

The PLC program of a SINUMERIK MCU is modular and comprises the following parts:

- Organization blocks (OB)
  The SINUMERIK basic PLC program must be opened and initialized in the respective organization blocks (OB) of the PLC program. You also call your PLC user program in these organization blocks.
- Basic PLC program
  The basic PLC program organizes the exchange of signals and data between the PLC user program and the NCK.
- PLC user program
  The PLC user program is the user-specific part of the PLC program by which the basic PLC program has been augmented or extended.
- Safety program of the F-PLC: Safety Integrated (F-PLC) is activated as standard in the properties of the MCU.
  If you want to use the safety functions of the F-PLC, add a safety program to the PLC program (see the Safety Integrated Commissioning Manual).

Note

The system library of the TIA Portal contains the SINUMERIK basic PLC program and data types as templates. You can edit the individual blocks of the basic PLC program directly in the TIA Portal using the STEP 7 editors.

6.4.2 Execution structure PLC program

Overview

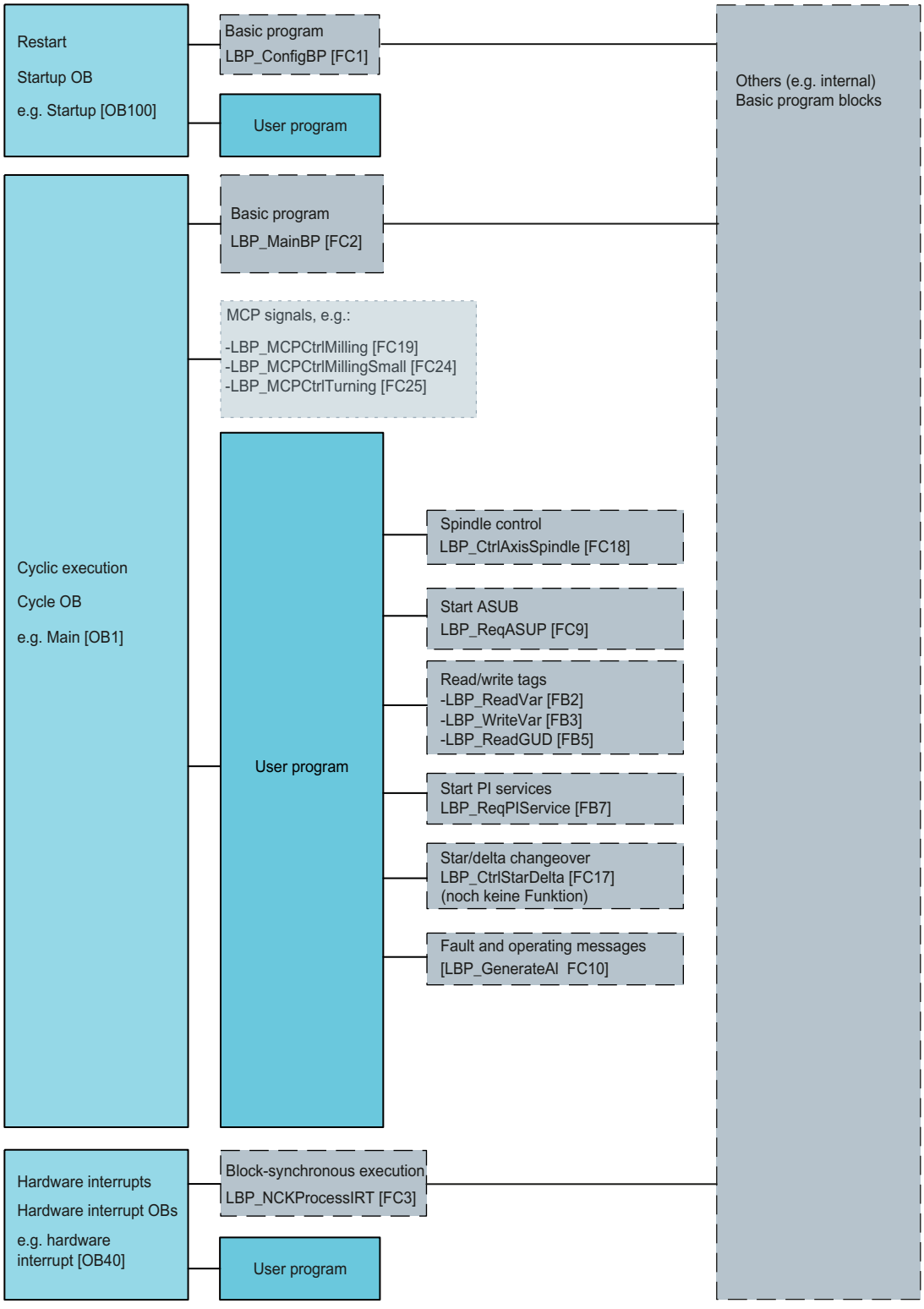
The basic PLC program of a SINUMERIK MCU comprises various function blocks (FB), functions (FC), and data blocks (DB). These blocks are called by various parts of the PLC program and organize the exchange of signals and data between the PLC user program and the NCK, HMI, and machine control panel components. From a chronological viewpoint, the main part of the basic PLC program runs before the PLC user program, but must partly be called via the same organization blocks.

The following figure and associated description illustrate the structure of the PLC program:

Note

Information on the basic PLC program blocks required in the project

The following description does not list all basic PLC program blocks individually that are required for an executable project. Refer to the overview tables of the basic PLC program reference for this kind of information or for the dependencies between the individual basic PLC program blocks.


Restart
Startup OB
e.g. Startup [OB100]
Basic program
LBP_ConfigBP [FC1]
User program
Cyclic execution
Cycle OB
e.g. Main [OB1]
Basic program
LBP_MainBP [FC2]
MCP signals, e.g.:
-LBP_MCPCtrlMilling [FC19]
-LBP_MCPCtrlMillingSmall [FC24]
-LBP_MCPCtrlTurning [FC25]
User program
Spindle control
LBP_CtrlAxisSpindle [FC18]
Start ASUB
LBP_ReqASUP [FC9]
Read/write tags
-LBP_ReadVar [FB2]
-LBP_WriteVar [FB3]
-LBP_ReadGUD [FB5]
Start PI services
LBP_ReqPIService [FB7]
Star/delta changeover
LBP_CtrlStarDelta [FC17]
(noch keine Funktion)
Fault and operating messages
[LBP_GenerateAl FC10]
Hardware interrupts
Hardware interrupt OBs
e.g. hardware interrupt [OB40]
Block-synchronous execution
LBP_NCKProcessIRT [FC3]
User program
Others (e.g. internal)
Basic program blocks

The PLC always starts up in the RESTART mode, i.e. the PLC operating system runs through block **Startup [OB100]** after initialization:

- In the startup [OB100], first call **LBP_ConfigBP [FC1]**, which configures and initializes the basic PLC program.
  - LBP_ConfigBP [FC1] calls further basic PLC program blocks internally.
- In addition, you need to insert the respective calls for your **PLC user program** in Startup [OB100] after LBP_ConfigBP [FC1].

Once Startup [OB100] has completed, the PLC commences cyclic mode at the beginning of **Main [OB1]**:

- In cyclic mode, the basic PLC program is called with **LBP_MainBP [FC2]** in Main [OB1]. Complete processing of the NCK-PLC interface is carried out. A cyclic monitoring function is activated between PLC and NCK once boot-up and the first OB cycle have been completed. LBP_MainBP [FC2] calls further basic PLC program blocks internally.
- In addition, you need to insert the respective calls for your **PLC user program** in Main [OB1].
  - You configure the transfer of machine control panel signals (e.g. MCP) in this part of your user program and call the respectively required basic program block, e.g. **LBP_MCPCtrlMilling [FC19]**.
  - From the PLC user program, you can call various basic PLC program blocks yourself at any point, e.g. to start ASUB or PI services.

If a hardware interrupt is triggered during runtime due to a configured hardware event, cyclic program processing is interrupted and the corresponding hardware interrupt OB is triggered.

- If a command that requires a synchronous reaction in the PLC program is processed during runtime in an NC part program, this reaction is executed in the part of the basic program that is synchronous with the block (LBP_NCKProcessIRT [FC3]). You configure the signal exchange and the hardware interrupt required for it in the NCK properties and you call the **LBP_NCKProcessIRT [FC3]** in the corresponding hardware interrupt OB, e.g. in **Hardware Interrupt [OB40]**. LBP_NCKProcessIRT [FC3] calls further basic PLC program blocks internally.
- In addition, you insert the respective calls for your **PLC user program** in this and/or in different hardware interrupt OBs and define the associated events in the properties of the corresponding device or module.

A PLC failure produces the "2000 PLC sign-of-life monitoring" alarm in the SINUMERIK ONE Commissioning Tool. No return is made to the interruption point (for example, in the event of a power failure). Some data of the basic PLC program is stored in a retentive memory area.

6.4.3 Relevant organization blocks

Below, you will find a list of all of the organization blocks from which the basic SINUMERIK PLC program must be called.

The organization blocks are not available as a copy template in the system library because you can also insert calls of your user program in the OBs.

Instead, add these organization blocks yourself and insert call and initialization of the basic program at the beginning of each OB.

Table 6-1 Organization blocks of the basic SINUMERIK PLC program

Name (default setting)	Address (default setting)	Description	PLC basic program block to be called
Startup	OB100	Startup OBs are processed once when the mode of the CPU switches from STOP to RUN. After execution of the startup OB, execution of the cycle OB starts.	LBP_ConfigBP [FC1]
Main	OB1	Cycle OBs are higher-level logic blocks in the program that are cyclically processed and in which you can program instructions or call additional blocks.	LBP_MainBP [FC2]
Hardware interrupt	OB40	Hardware interrupt OBs interrupt the cyclic program processing due to a hardware event. You define the event in the hardware properties.	LBP_NCKProcessIRT [FC3]

6.4.4 Inserting program code for calling the basic program

Because the organization blocks of the PLC program must contain both calls of the SINUMERIK PLC basic program and calls of your PLC user program, these organization blocks are not available as copy templates in the system library.

Instead, add these organization blocks yourself and then insert the program code for calling and initializing the PLC basic program.

For example, you can type these calls directly in the editor, copy them from a program example (SCL) and paste them into the editor or create them with drag and drop.

Requirement

- The respective organization block is added.

  Note

  Selecting the programming language for Main [OB1]

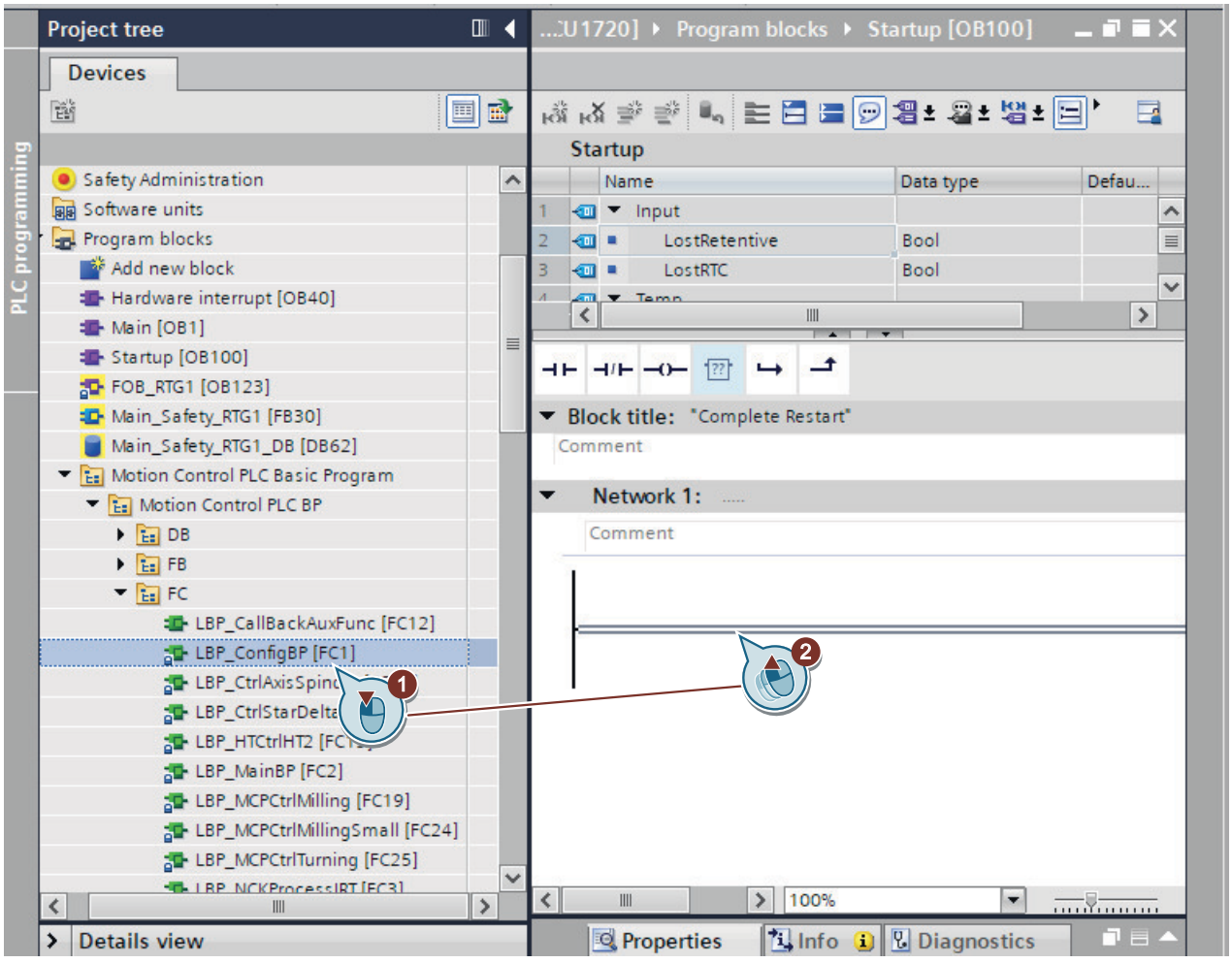
  A newly added MCU already contains Main [OB1] in the LAD programming language. You can change the programming language to FBD in the block properties or delete the existing block and add it back again as an STL block or SCL block.

- The basic SINUMERIK PLC program blocks that are to be called from the respective organization block are added in the "Program blocks" folder of the project tree.

Procedure

To insert the program code for calling and initializing the basic SINUMERIK PLC program, proceed as follows:

1. In the project tree, double-click the relevant organization block, e.g. "MCU_1 > PLC_1 > Program blocks > OB > Startup [OB100]".
   The organization block is opened.
2. Drag the basic program block to be called from the program blocks folder and drop it in Network 1 of the relevant organization block.
   - The startup OB, e.g. Startup [OB100], must include the call of LBP_ConfigBP [FC1] in network 1.
   - The cycle OB, e.g. Main [OB1], must include the call of LBP_MainBP [FC2] in network 1.
   - The hardware interrupt OB, e.g. Hardware interrupt [OB40], must include the call of LBP_NCKProcessIRT [FC3] in network 1.



Result

The calls of the SINUMERIK PLC basic program have been added. For the hardware interrupt OB or the call of LBP_NCKProcessIRT [FC3], the event-driven signal exchange NCK to PLC must be configured in addition.

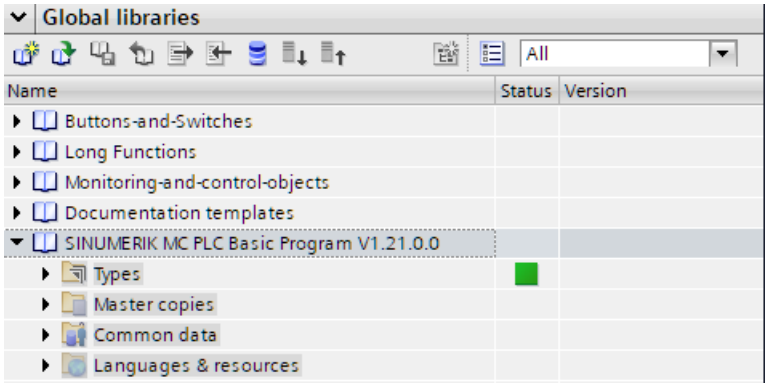
6.4.5 Inserting the basic PLC program into the project

6.4.5.1 Opening the PLC basic program system library

Procedure

Proceed as follows to open and display the system library of the SINUMERIK PLC basic program:

1. Switch to the "Libraries" task card.
2. Under "Global libraries", select the PLC basic program that matches the firmware version of the inserted MC, e.g. the library "SINUMERIK MC PLC Basic Program V1.21.0.0".



Result

The library is opened. In the subfolders, you will find the components of the PLC basic program structured in the following way:

Folder	Purpose	Content
"Copy templates > Motion Control PLC Basic Program > Motion Control PLC BP"	Use this "Copy templates" folder when you insert a new SINUMERIK Motion Control.	Contains all the blocks required for the maximum configuration (8 axes, 4 channels) of a SINUMERIK Motion Control. The individual blocks are sorted into the subfolders "DB", "FB", "FC" and "Internal".
"Copy templates > Motion Control PLC Basic Program (upgrade) > Motion Control PLC BP"	Use this copy template folder when you upgrade or migrate from an older version of the PLC basic program.	Contains all the knowhow-protected blocks required for the maximum configuration (8 axes, 4 channels) of a SINUMERIK Motion Control. Blocks that are supplemented with user-specific adaptations are not included. The individual blocks are sorted into the subfolders "DB", "FB", "FC" and "Internal".
"Copy templates > Motion Control PLC Basic Program > Motion control PLC BP data types"	The content of this copy template folder is used by the PLC basic program and must be copied into the "PLC data types" folder.	Contains all PLC data types (UDT) that are used by the PLC basic program.

You can copy and paste these block copy templates (Page 97) and PLC data types copy templates (Page 93) directly or together with the folder structure into your project.

6.4.5.2 Inserting PLC data types

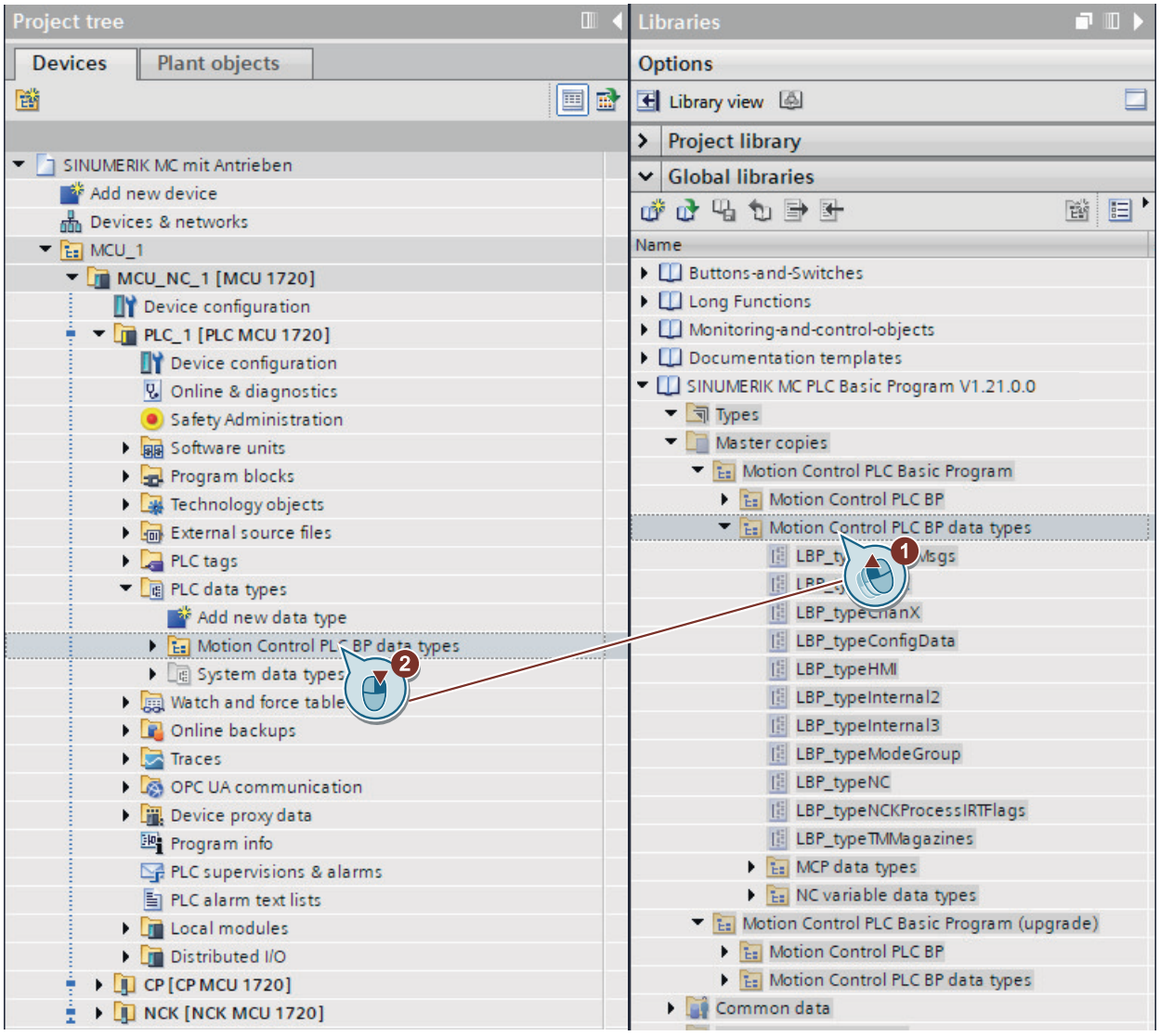
The PLC interface data blocks of the basic program make it possible to access various interfaces and data (axes/spindles, channels, mode groups, alarms/messages, PLC/HMI, MCP/HT) from the PLC program.

PLC data types (UDT), which define the content of the data blocks, are available in the system library of the SINUMERIK Motion Control PLC Basic Program. Copy these PLC data types into your project.

Procedure

Proceed as follows to copy the PLC data types into your project:

1. Switch to the "Libraries" task card and open the system library "SINUMERIK MC PLC Basic Program V1.21.0.0", for example.
2. Drag the folder "Copy templates > Motion Control PLC Basic Program > Motion Control PLC BP data types" into folder "PLC data types" of your project (e.g. under "MCU_1 > PLC_1 > PLC data types").



Result

The data types were copied into your project and assigned to the corresponding blocks of the PLC basic program.

6.4.5.3 Inserting PLC basic program blocks

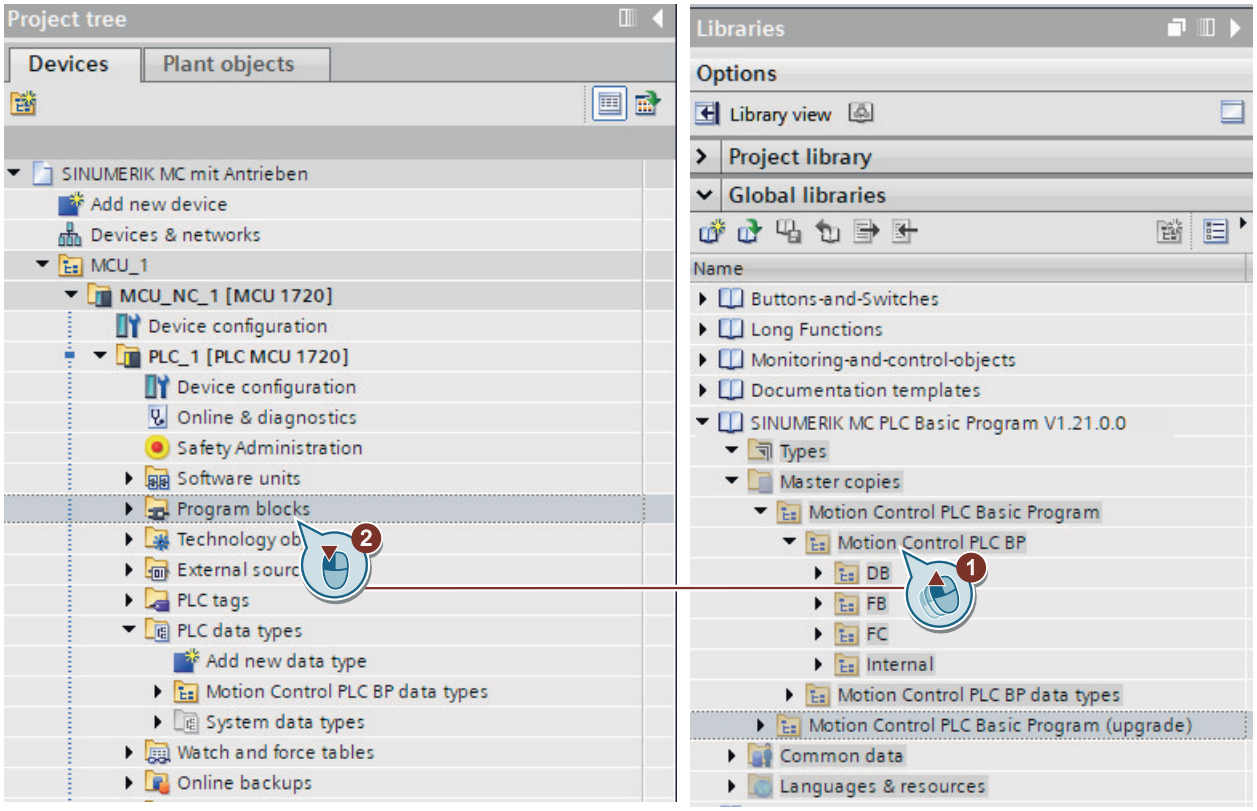
Requirement

- A SINUMERIK MCU has been created.
- The data types of the PLC basic program blocks are inserted (Page 93).

Procedure

To copy program blocks of the basic program from a copy template to the program blocks folder of the project tree, proceed as follows:

1. Switch to the "Libraries" task card and open the system library "SINUMERIK MC PLC Basic Program V1.21.0.0", for example.
2. Drag the folder "Motion Control PLC BP" into the "Program blocks" folder, e.g. under "MCU_1 > PLC_1 > Program blocks":



Note

Copying this folder changes the user-defined folder structure

Copying the "Motion Control PLC BP" folder automatically creates new groups (subfolders) in your "Program blocks" folder and moves the existing blocks into them.

If you have already organized the PLC basic program into separate groups and would like to keep this structure, copy the individual block copy templates from the lower-level folders or select multiple block copy templates using multiple selection instead.

The blocks are copied to your project. A check is made for duplicate block names and, if applicable, the "Conflicts when copying" (Page 107) dialog is displayed.

3. In the project tree, right-click "Program blocks" and in the "Compile" shortcut menu select the command "Software (compile all)".
   The PLC program is compiled and a check is made for duplicate block addresses, for example. You can check whether the PLC program has been successfully compiled in the inspector window under "Info > Compile".

Result

The blocks of the SINUMERIK PLC Basic Program have been copied to your project. The folder structure of the copied elements is taken over.

Now you can check the copied blocks and, if applicable, manually delete the PLC basic program blocks that you do not require (e.g. unused axis DB, channel DB, FB or FC).
If you have unused blocks in your project, user memory is also assigned for these blocks that are not being used.

6.4.5.4 Edit blocks

The individual blocks of the PLC basic program or the user program can be edited directly in the TIA Portal Portal using the STEP 7 editors.

Information about these functions and editors is available in the higher-level help "Programming the PLC" and in the STEP 7 Professional System Manual.

6.4.5.5 Blocks with user-specific adaptations

In the following, you will find a list of all of the blocks of the SINUMERIK basic program that can contain user-specific adaptations and therefore cannot be automatically upgraded. These blocks are not included in the copy template "UpgradeProject".

Table 6-2 PLC basic program blocks with user-specific adaptations

Block	Name	Description
DB5	LBP_ParamAlarmMsgs	Interface between user program and LBP_GenAlarmMsgs [FC10], contains the parameter assignment of the alarms for the bit fields in the LBP_AlarmMsgs [DB2] as error or operating message.
DB75	LBP_MFuncDecList-Config	Decoding list for M decoding according to list.
DB78	LBP_PowerrideConfig	Global data block containing two example configurations for a Powerride rotary/push switch using UDT78 and UDT79.
FC12	LBP_CallBackAuxFunc	Call interface for users for auxiliary functions, the block is called on an event-driven basis in the basic program when new auxiliary functions are available.

6.4.5.6 Retentivity behavior of the PLC basic program

The following data of the PLC basic program is stored in a retentive memory area to avoid data loss in the event of a voltage failure.

Name	Block address/number:
LBP_AlarmMsgs	DB2
LBP_ParamAlarmMsgs	DB5
LBP_ConfigData	DB7
LBP_InternalDB8	DB8
LBP_NC	DB10
LBP_ModeGroup	DB11

Name	Block address/number:
LBP_HMI	DB19
LBP_Chan1, ... LBP_Chan4	DB21, ... DB24
LBP_Axis1, ... LBP_Axis8	DB31, ... DB38
LBP_TMLoad	DB71
LBP_TMSpindle	DB72
LBP_TMTurret	DB73
LBP_MFuncDecListConfig	DB75

6.4.5.7 Programming examples (SCL)

Example for calling LBP_ConfigBP [FC1]

In the startup [OB100], LBP_ConfigBP [FC1] must be called in which the basic PLC program is initialized and configured.

You can copy or input the call in the editor or create it with drag and drop.

SCL

```
"LBP_ConfigBP"(MCPNum := 1,
MCP1In := P#I0.0,
MCP1Out := P#Q0.0,
MCP1BusAdr := 6,
MCP1Timeout := S5T#700MS,
MCP2In := NULL,
MCP2Out := NULL,
MCP2BusAdr := 0,
MCP2Timeout := S5T#700MS,
MCP1Stop := FALSE,
MCP2Stop := FALSE,
MCP1NotSend := FALSE,
MCP2NotSend := FALSE,
MCPBusType := B#16#6,
HTIf := 0,
HTIn := NULL,
HTOut := NULL,
HTAdr := 2,
HTStop := FALSE,
HTNotSend := FALSE,
NCCyclTimeout := S5T#200MS,
NCRunupTimeout := S5T#50S,
ListMDecGrp := 0,
MMCToIF := TRUE,
HWheelMMC := TRUE,
MCP_IF_TCS := FALSE,
```

SCL

```
ExtendChanAxMsg := FALSE,
HMIAxisSel := FALSE,
MsgUser := 10,
IRAuxfuT := FALSE,
IRAuxfuH := FALSE,
IRAuxfuE := FALSE,
OpKeyNum := 0,
Op1KeyIn := NULL,
Op1KeyOut := NULL,
Op1KeyBusAdr := 0,
Op2KeyIn := NULL,
Op2KeyOut := NULL,
Op2KeyBusAdr := 0,
Op1KeyStop := FALSE,
Op2KeyStop := FALSE,
Op1KeyNotSend := FALSE,
Op2KeyNotSend := FALSE,
OpUnitCommId :=1,
OpUnitInterfaceId :=262,
MCP1ConnectionId :=1001,
MCP2ConnectionId :=1002,
HTConnectionId :=1003,
Op1KeyConnectionId :=1004,
Op2KeyConnectionId :=1005,
IdentConnectionId :=1006,
MCP1LocalUdpPort :=16001,
MCP2LocalUdpPort :=16002,
HTLocalUdpPort :=16003,
Op1KeyLocalUdpPort :=16004,
Op2KeyLocalUdpPort :=16005,
IdentLocalUdpPort :=16006,
MaxModeGroup => "LBP_ConfigData".MaxModeGroup,
MaxChan => "LBP_ConfigData".MaxChan,
MaxAxis => "LBP_ConfigData".MaxAxis,
ActiveChan => "LBP_ConfigData".ActiveChan,
ActiveAxis => "LBP_ConfigData".ActiveAxis,
MaxNumUserDataInt => "LBP_ConfigData".MaxNumUserDataInt,
MaxNumUserDataHex => "LBP_ConfigData".MaxNumUserDataHex,
MaxNumUserDataReal => "LBP_ConfigData".MaxNumUserDataReal,
UserDataIntArray => NULL,
UserDataHexArray => NULL,
UserDataRealArray => NULL,
TMMagazines => NULL);
//INSERT USER PROGRAM HERE
```

Examples for calling LBP_MainBP [FC2]

Call LBP_MainBP [FC2] in Main [OB1], thus starting cyclic processing of the SINUMERIK PLC basic program.

You can copy or enter the call in the editor or create it with drag and drop.

SCL

```
// Call of basic program as first FC
"LBP_MainBP"();
// Add user program here
```

Example for calling LBP_NCKProcessIRT [FC3]

If a command that requires a synchronous reaction in the PLC program is processed during runtime in an NC part program, this reaction is executed in the part of the basic program that is synchronous with the block (LBP_NCKProcessIRT [FC3]). You configure the signal exchange and the hardware interrupt required for it in the NCK properties. You call LBP_NCKProcessIRT [FC3] in the corresponding hardware interrupt OB, e.g. in Hardware Interrupt [OB40].

You can copy this call to the editor or enter it or create it with drag and drop.

Example 1 without transfer of the output parameters

SCL

```
//Call without output parameters
"LBP_NCKProcessIRT"(Flags=>NULL);
```

Example 2 with transfer of the output parameters

In this example, "LBP_NCKProcessIRT" is called directly in the hardware interrupt OB with the transfer of the output flags. The output flags are subsequently evaluated.

Variables to be declared in the "Temp" section of the hardware interrupt OBs

Temp	
GP	"LBP_typeNCKProcessIRTFlags"
NckEvent	Bool
Axis1InPos	Bool
Axis2InPos	Bool
Axis3InPos	Bool
AuxFunctionInChan1	Bool
AuxFunctionInChan2	Bool
TMCommand	Bool

Program code to be inserted into the hardware interrupt OB

SCL

```
// GP: "LBP_typeNCKProcessIRTFlags";
// NckEvent : Bool;
// Axis1InPos: Bool;
```

SCL

```
// Axis2InPos: Bool;
// Axis3InPos: Bool;
// AuxFunctionInChan1: Bool;
// AuxFunctionInChan2: Bool;
// TMCommand: Bool;
//Call with output parameters
"LBP_NCKProcessIRT"(Flags=>#GP);
//Use of the output parameters
IF #GP.IRFromNck THEN
#NckEvent := TRUE;
END_IF;
//Use of the flags for axis 1 to 3
IF #GP.InPosition[1] THEN
#Axis1InPos := TRUE;
END_IF;
IF #GP.InPosition[2] THEN
#Axis2InPos := TRUE;
END_IF;
IF #GP.InPosition[3] THEN
#Axis3InPos := TRUE;
END_IF;
//Use of the flags for channel 1 and 2
IF #GP.AuxFunction[1] THEN
#AuxFunctionInChan1 := TRUE;
END_IF;
IF #GP.AuxFunction[2] THEN
#AuxFunctionInChan2 := TRUE;
END_IF;
//Is a tool change pending?
IF #GP.TM THEN
#TMCommand := TRUE;
END_IF;
```

Example 3 - as nested call without transfer of the output parameters

In this example "LBP_NCKProcessIRT [FC3]" is called nested over an own FC (e.g. hardware interrupt [OB40] > MyProcessAlarmFC [FC30] > LBP_NCKProcessIRT [FC3]) without transfer of the output flags.

Hardware interrupt OB, e.g. Hardware interrupt [OB40]:

SCL

```
//Call own FCs
"MyProcessAlarmFC"();
```

Own FC, e.g. MyProcessAlarmFC [FC30]:

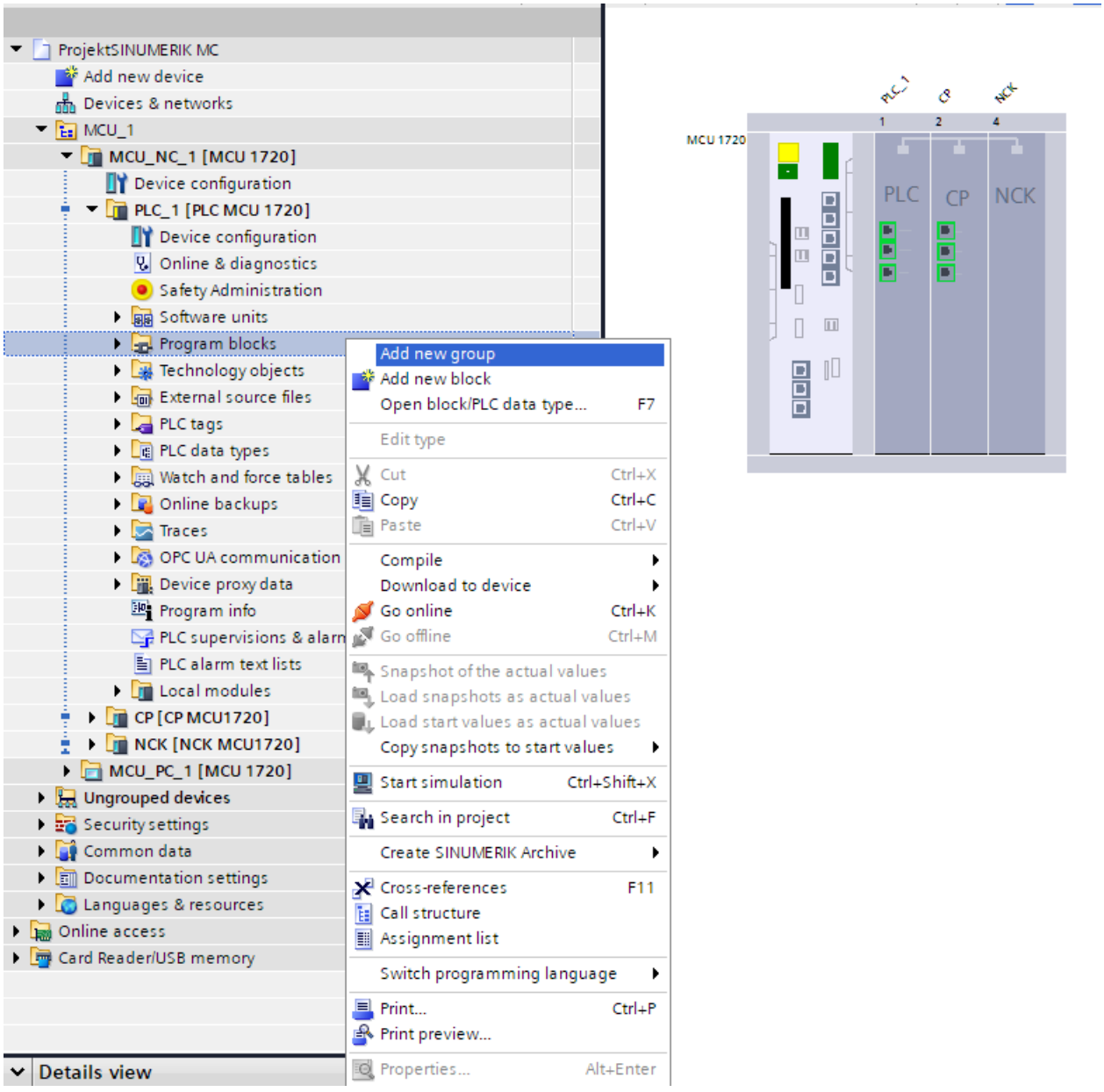
SCL

```
//Call without output parameters
"LBP_NCKProcessIRT"(Flags=>NULL);
```

6.4.6 Handling of blocks and libraries

6.4.6.1 Use and handling of groups

In the Program blocks folder in the project tree, you can call the command "Add new group" in the shortcut menu to create groups to organize your program blocks.



For example, this function is useful in the following situations:

- Creating a dedicated group for the blocks of the basic program and of the user program. This allows you to individually display the editable blocks of the user program.
- Organizing specific related program blocks (e.g. axis DBs).

To maximize the overview window, select the "Program blocks" folder and click the "Maximizes/minimizes the Overview" icon on the project tree toolbar.

6.4.6.2 Copying blocks into a project

Here the procedure how to copy blocks from one project to another is described.

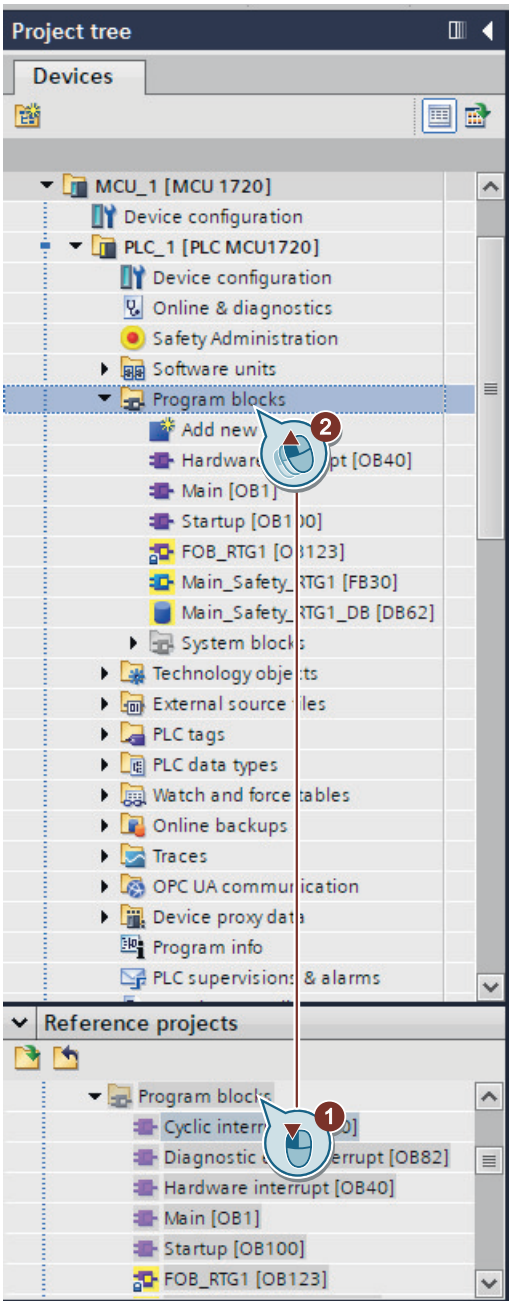
Alternatively, the library functionality in the TIA Portal can be used. Existing program modules can be provided, for example, in the form of copy templates or typified objects.

Procedure

Proceed as follows to import blocks from an existing project:

1. From the "View" menu, choose the command "Reference projects".
   The "Reference projects" palette is displayed under the project tree.
2. Click the "Open reference project" icon in the "Reference projects" palette, select the project, and confirm with "Open".
   The project is opened (write-protected) and the associated project structure is displayed in the "Reference projects" palette.

3. Navigate in the reference project to the "Program blocks" folder and select the blocks that you want to copy.
4. Drag-and-drop the blocks from the reference project to the "Program blocks" folder of your current project.



Note

Copy additional objects separately (e.g. variables or PLC data types)

When you copy the program blocks, objects that belong together, such as variables, PLC data types or technology objects, are not automatically included in the copy. This applies both to copying from reference projects and to copying to another PLC.

Error messages are issued during the compilation, e.g. if the variables used in the copied program block are not defined in the variable table.

Therefore, additionally copy the objects used by the copied blocks.

Note

Conflicts due to names, addresses or numbers that are used multiple times

When you paste objects from a reference project whose names have already been used in the project, these are automatically renamed under certain circumstances:

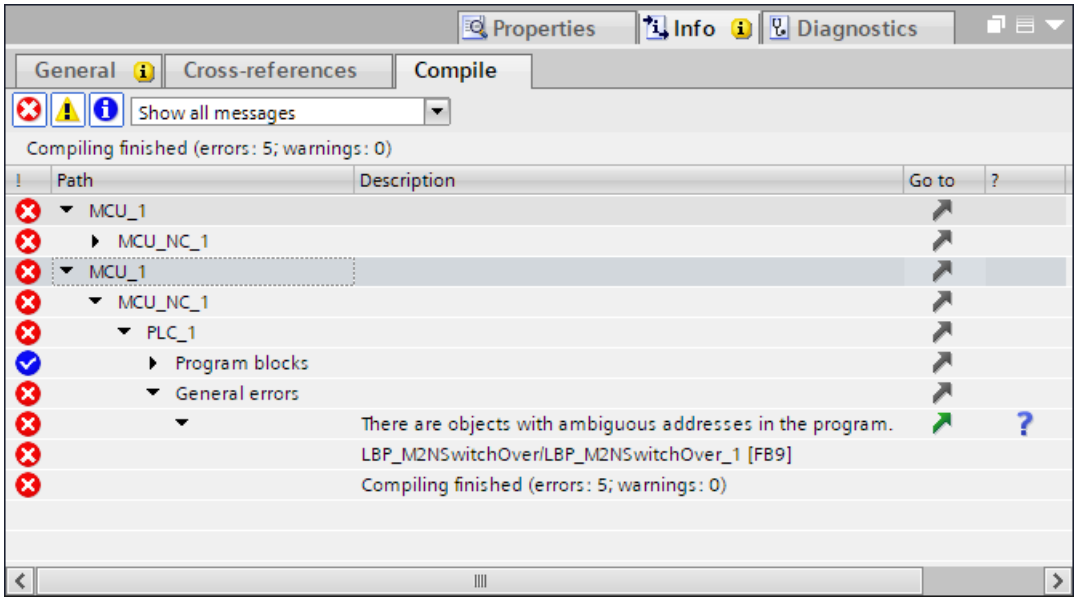
- If you copy objects with the same name into the same folder or the same group, the "Conflicts when copying" dialog (Page 107) is displayed.
- If you copy objects with previously assigned names to a different folder (or group), the newly inserted objects are renamed without asking.

A check for duplicate block numbers or addresses is, however, only performed during compilation.

6.4.6.3 Conflicts when copying blocks

Two different conflict types can occur during copying and pasting of program blocks:

- If several blocks with the same block numbers exist in the "Program blocks" folder, a message is not displayed immediately. As duplicate block numbers are not flagged until the during the compilation process,
  we recommend you compile your project after making a copy in order to detect any conflicts at an early stage.

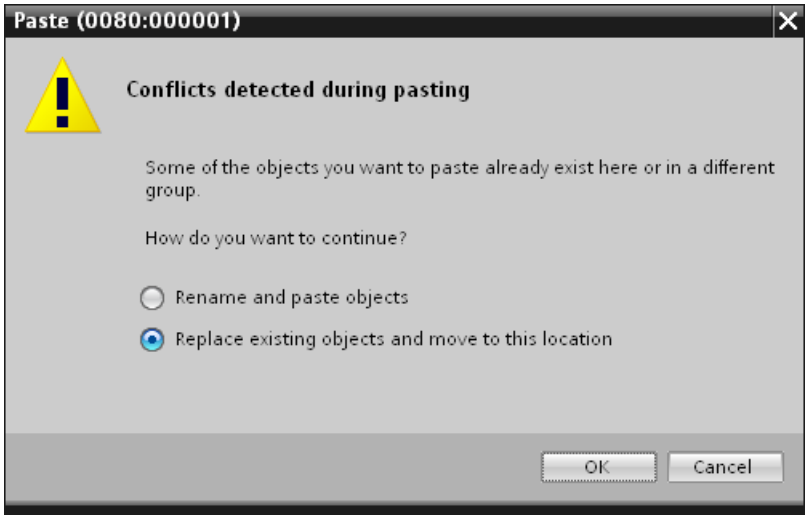


  If duplicate block numbers exist, proceed as follows:

  – If this involves one of the blocks of the basic program that you do not require (e.g. unused axis DB, channel DB, FB or FC), you can delete it.

  – If a user block has the same block number as a required basic program block, you must change the number of the user block.

- The presence of duplicate symbolic block names is already checked during the copying procedure. A message is issued if conflicts result because of existing symbolic names.



The dialog offers you the following ways of rectifying the conflict:

- You can cancel the copy process, search for the duplicate blocks in the project tree and delete them before you initiate the copy process again. In this case, click in the "Cancel" dialog box.
- You can copy the template to the project and overwrite duplicate blocks without knowing which blocks have caused the conflict. In this case, select in the dialog box "Replace existing objects and move to this location" and confirm with "OK".

The other option mentioned in the dialog, "Rename and add objects", does not resolve the conflict in this case.

6.4.6.4 Block address range for PLC user program

From the following block number assignment overview, you can find out whether a specific block number (or block address) is assigned or reserved by the basic PLC program, or whether it can be used for the PLC user program.

Table 6-3 Assignment overview of the DB numbers

DB number	Availability	Occupied by
1	Reserved	Siemens
2 ... 3	Occupied	Siemens (basic PLC program)
4 ... 7	Reserved	Siemens
8	Occupied	Siemens (basic PLC program)
9	Reserved	Siemens
10 ... 11	Occupied	Siemens (basic PLC program)
12	Occupied	Computer link and transport system interface
13 ... 15	Reserved	Siemens
16	Occupied	Siemens (basic PLC program)
17 ... 18	Reserved	Siemens
19	Occupied	Siemens (basic PLC program)

DB number	Availability	Occupied by
20	Reserved	Siemens
21 ... 24	Occupied[1]	Siemens (basic PLC program: interface for NC channels)
31 ... 38	Occupied[1]	Siemens (basic PLC program: interface for axes/spindles)
62 ... 70	Freely available (user program)	-
74	Reserved	Siemens
71 ... 73	Reserved	Siemens
75 ... 76	Occupied	Siemens (M group decoding)
77 ... 80	Reserved	Siemens
81 ... 999	Occupied or reserved	Siemens (ShopMill, ManualTurn)
1000 ... 1019	Reserved	Siemens
1020	Occupied or reserved	Siemens (basic PLC program)
1021 ... 1099	Reserved	Siemens
1100 ... 24999	Freely available (user program)	-
25000 ... 29999	Reserved	Siemens
30000 ... 59999	Reserved[2]	Standard number range for generated F-system blocks
60000 ... 60999	Occupied or reserved	CPU DBs

Table 6-4 Assignment overview of the FB numbers

FB number	Availability	Occupied by
0	Reserved	Siemens
1	Reserved	Siemens (basic PLC program)
2 ... 3	Occupied	Siemens (basic PLC program)
4	Reserved	Siemens
5	Occupied	Siemens (basic PLC program)
6	Reserved	Siemens
7	Occupied	Siemens (basic PLC program)
8	Reserved	Siemens
9	Occupied	Siemens (basic PLC program)
10 ... 29	Reserved	Siemens
15	Reserved	Siemens (basic PLC program)
16 ... 28	Reserved	Siemens
29	Reserved	Siemens (basic PLC program)
30 ... 999	Freely available (user program)	-
1000 ... 1019	Reserved	Siemens
1020	Occupied	Siemens (basic PLC program)
1021 ... 1023	Reserved	Siemens
1024 ... 24999	Freely available (user program)	-

FB number	Availability	Occupied by
25000 ... 32766	Reserved	Siemens (basic PLC program)
32767 ... 65535	Reserved[2]	Standard number range for generated F-system blocks

Table 6-5 Assignment overview of the FC numbers

FC number	Availability	Occupied by
0	Reserved	Siemens
1 ... 3	Occupied	Siemens (basic PLC program)
4	Reserved	Siemens
5	Reserved	Siemens (basic PLC program)
6 ... 29	Reserved	Siemens
30 ... 999	Freely available (user program)	-
1000 ... 1023	Reserved	Siemens
1024 ... 24999	Freely available (user program)	-
25000	Occupied	Siemens (basic PLC program)
25001 ... 32766	Reserved	Siemens (basic PLC program)
32767 ... 65535	Reserved[2]	Standard number range for generated F-system blocks

[1]Not recommended for use, but possible with limitations. Data blocks of channels and axes/spindles that have not been activated can be used by the user, but this can result in conflicts when upgrading or migrating the basic PLC program.

[2]If you use SINUMERIK Safety Integrated (F-PLC), this number range is used for automatically generated F-blocks by default. You can adapt the number range used by the F-system, but you must select a sufficiently large range of numbers.

6.4.7 NCK hardware interrupts

6.4.7.1 General information on hardware interrupt OBs

If a hardware interrupt is triggered by a module during runtime, the hardware interrupt OB defined in the associated event is triggered or entered in the queue depending on its priority.

- This allows you to react specifically in the PLC user program to events that are triggered by various modules.
  You can use the same or different hardware interrupt OBs for different hardware/module events. When you assign the same hardware interrupt OB to different events, you must distinguish between the triggering events in the program code of the hardware interrupt OB.
- The hardware interrupt mechanism is also used by the event-driven signal exchange (NC to PLC) to be able to respond to NC events (NCK events) in the PLC program.
  You must activate the event-driven signal exchange in the NC properties. You should assign an exclusive hardware interrupt OB during this. The hardware interrupt OB must contain the call of LBP_NCKProcessIRT [FC3] and the queries for the occurrence of the NC events.

6.4.7.2 Transfer and acknowledgment time of NCK signals

Various events in the NC (NCK) are transferred to the PLC. These are accessible at different times in the PLC user program, depending on their type, and are acknowledged at different times to the NCK again. You can reconfigure this behavior for auxiliary functions as described in the table.

When you activate hardware interrupts in the properties of the NCK and assign a hardware interrupt OB, this assigned hardware interrupt OB is called for all NC events. If several events occur simultaneously, then the events are combined and executed in a hardware interrupt OB.

All NC signals that are accessible in the PLC user program are listed in the table below.

Signal type	Handover to user	Acknowledgment to NCK	Remark
Standard auxiliary function	Cycle OB	After cycle OB	
Fast auxiliary function (user-defined auxiliary functions with fast acknowledgment)	Cycle OB	Immediately in the hardware interrupt OB (see note)	Fast auxiliary functions (user-defined auxiliary functions with fast acknowledgment) are auxiliary functions that are typically already acknowledged in the hardware interrupt OB in the NC before they are pending for processing in the cycle (cycle OB). This means the acknowledgment does not acknowledge the execution of the PLC user function in this case. Especially when fast auxiliary functions are output in consecutive part program blocks there is no guarantee that the reaction in the PLC user program is synchronous with the block. In such cases the first fast auxiliary function is acknowledged immediately in the hardware interrupt OB but the following fast auxiliary functions are treated like standard auxiliary functions and the acknowledgement takes place only after the next cycle OB.
Auxiliary function to be executed event-driven	Hardware interrupt OB	Immediately in the hardware interrupt OB	An auxiliary function can be defined as an auxiliary function that is executed event-driven by setting the corresponding parameter of the LBP_ConfigBP [FC1]: • T function: IRAuxfuT • H function: IRAuxfuH • DL function: IRAuxfuE
G commands	Hardware interrupt OB	Immediately in the hardware interrupt OB	
Auxiliary function axis signals	Hardware interrupt OB	Immediately in the hardware interrupt OB	
Signal from positioning axis	Next call of LBP_CtrlAxisSpindle [FC18]	Immediately in the hardware interrupt OB	
ASUP interrupt executed	Next call of LBP_ReqASUP [FC9]	Immediately in the hardware interrupt OB	Special type. No function but acknowledgment that ASUP interrupt was executed.
Compile cycles/data records	Hardware interrupt OB	Depending on programming in the compile cycle	Special type, is not evaluated.

6.4.7.3 Identification of an NCK event in the PLC program

A hardware interrupt OB should be assigned to the event-driven signal exchange from NC (NCK) to PLC that exclusively contains the call of LBP_NCKProcessIRT [FC3].

You will only need to distinguish between the triggering events in the program code of the hardware interrupt OBs if you did not follow this recommendation and have assigned the same hardware interrupt OBs to different events.

Whether or not an event was triggered by the NC can be queried as follows:

- LADDR in the start information of the hardware interrupt OB
  LADDR contains the hardware identifier of the module that has triggered the hardware interrupt. The HW identifiers that occur in your project can be viewed in the system constants.
- PointAddr in the start information of the hardware interrupt OB

Slice access	#PointAddr.B3			#PointAddr.B2			#PointAddr.B1			#PointAddr.B0		
Bit number	31	...	24	23	...	16	15	...	8	7	...	0
Meaning	currently not used (set to 0)			currently not used (set to 1)			Channel currently not used (set to 0)			Event that triggered the hardware interrupt. 10 or B#16#0A: Event-driven signal exchange NCK to PLC		

LBP_NCKProcessIRT [FC3] should only be called after such a successful query to avoid unnecessary calling.

Alternatively, you can call the LBP_NCKProcessIRT [FC3] without any distinction at the start of the hardware interrupt OB and then specifically query the pending individual NC signals in the output parameters of LBP_NCKProcessIRT [FC3].

6.4.7.4 Defining NCK hardware interrupt event

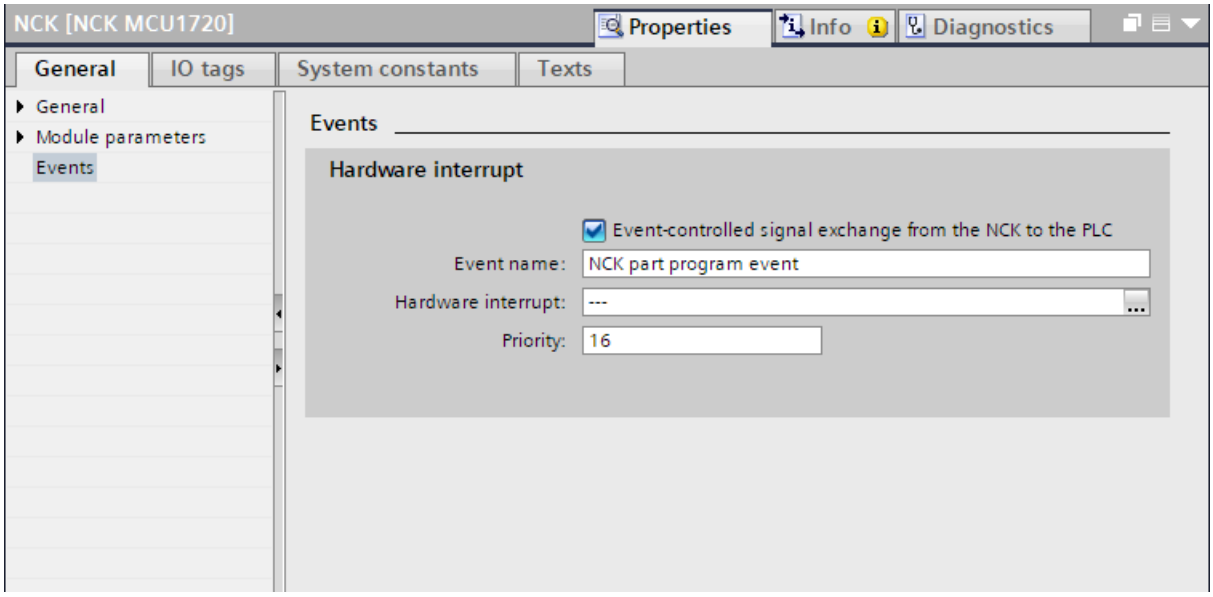
Precondition

- A SINUMERIK MCU has been created.

Procedure

Proceed as follows to configure process alarms in the properties of the NCK:

1. Click on the "NCK" module in the network view or device view.
2. In the "Properties" inspector window, select the "Events" entry.
   The hardware interrupt settings are displayed. The event-controlled signal exchange from the NCK to the PLC is activated by default and given a default priority.
   You must assign a hardware interrupt OB to the start event.



3. Make the following settings:

Settings	Purpose
Event name	Name for identification of the event, for example, in the list of the start events of assigned hardware interrupt OBs and the system constants. A language-neutral event name is set as default. You can change the event name as necessary and select a language-neutral name, for example.
Hardware interrupt	Select an existing hardware interrupt OB from the list and confirm with the check mark button or click on "Add" to add a new block and assign it to the event. In special applications (e.g. a modular machine) it may be useful to assign the hardware interrupt during runtime in the user program with an attach command instead.
Priority	Define the priority of this event in relation to other hardware interrupt OBs or the priority in the queue. The valid value range of the priority can be found in the tooltip. **The following applies:** • Small number value → low priority (e.g. 2) • Large numerical value → high priority (e.g. 26)

Note

Hardware interrupts: Response for NCK events

You must issue an attach command before an event occurs from the part program (by executing a command to output a fast help function). If you do not issue an attach command, then the NCU is brought into state "Wait for HiFu acknowledgment".

You must reset the NCU in order to exit state "Wait for HiFu acknowledgment".

Result

The properties of the NCK process alarm events have been specified and may have been assigned to a process alarm OB. The event is also listed in the properties of the selected hardware interrupt OB under "Start events". A corresponding system constant was added.

Note

Message: "Wait: AuxF acknowledgment missing"

If NCK events, auxiliary functions or NCK hardware interrupts are called without a hardware interrupt OB being assigned or before one is assigned, the channel message "Wait: AuxF acknowledgment missing" is issued.

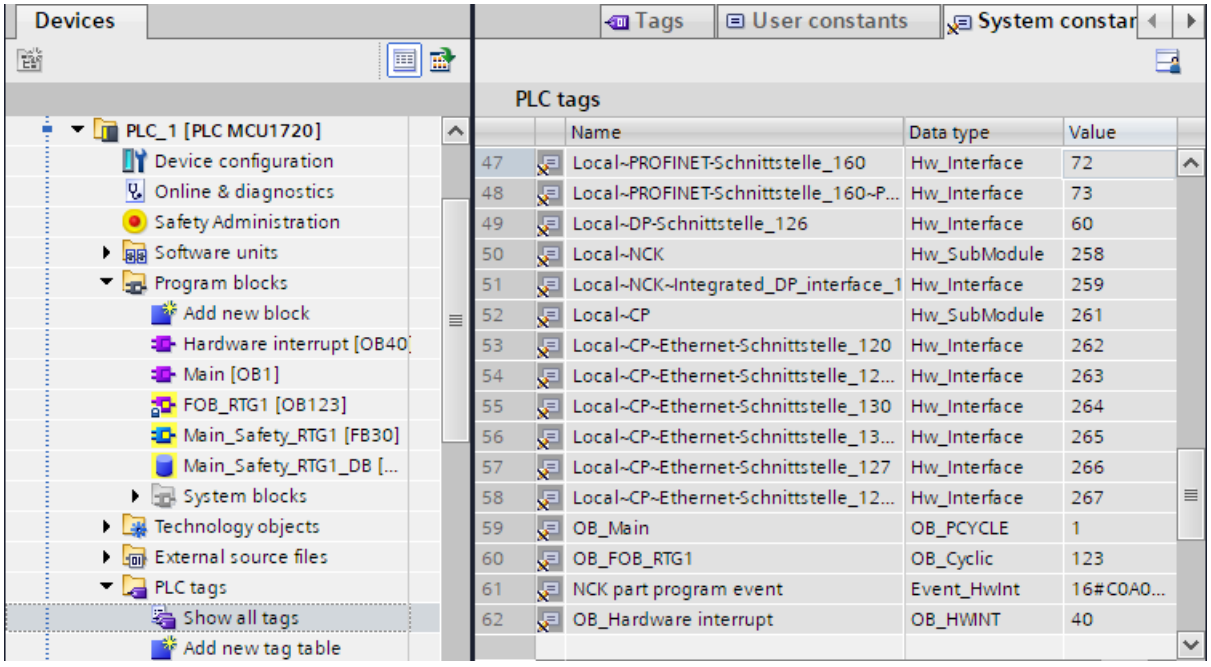
You can only leave this state if you trigger a "power-on reset" of the MCU.

For the NCK signals to be processed in the PLC basic program, you must call LBP_NCKProcessIRT [FC3] in the hardware interrupt OB (e.g. hardware interrupt [OB40]) next.

6.4.7.5 Use of the associated system constant

When you define the event for NCK hardware interrupts, a system constant is automatically added whose name corresponds to the associated event name. You can use the system constant to query in the PLC user program whether a hardware interrupt was triggered and by which module.

You can find the system constant in the "PLC variables" editor in the "System constants" tab.



The system constant with the data type "Hw_Interface" contains the HW identifier of the DP-Integrated interface on the NCK (initiating module for NCK events).

6.4.7.6 Assigning hardware interrupt OB during runtime

In special applications (e.g. modular machine) it probably makes sense not to select the hardware interrupt OB in the project in the NCK events, but during the runtime in the user program using an attach command instead.

- In the assigned hardware interrupt OB the block "LBP_NCKProcessIRT [FC3]" must be called in exactly the same way as when you define the hardware interrupt OB in the configuration.
- The assignment must take place in the user program before the call of the NCK hardware interrupt, i.e. before the call of a quick auxiliary function, for example
- The assignment of the hardware interrupt OB during runtime is not saved in the project data. The assignment must take place in the user program after each STOP-RUN transition of the PLC.

Note

Message: "Wait: AuxF acknowledgment missing"

If NCK events, auxiliary functions or NCK hardware interrupts are called without a hardware interrupt OB being assigned or before one is assigned, the channel message "Wait: AuxF acknowledgment missing" is issued.

You can only leave this state if you trigger a "Power On Reset" of the MCU.

6.4.8 Loading the PLC program to the PLC

Introduction

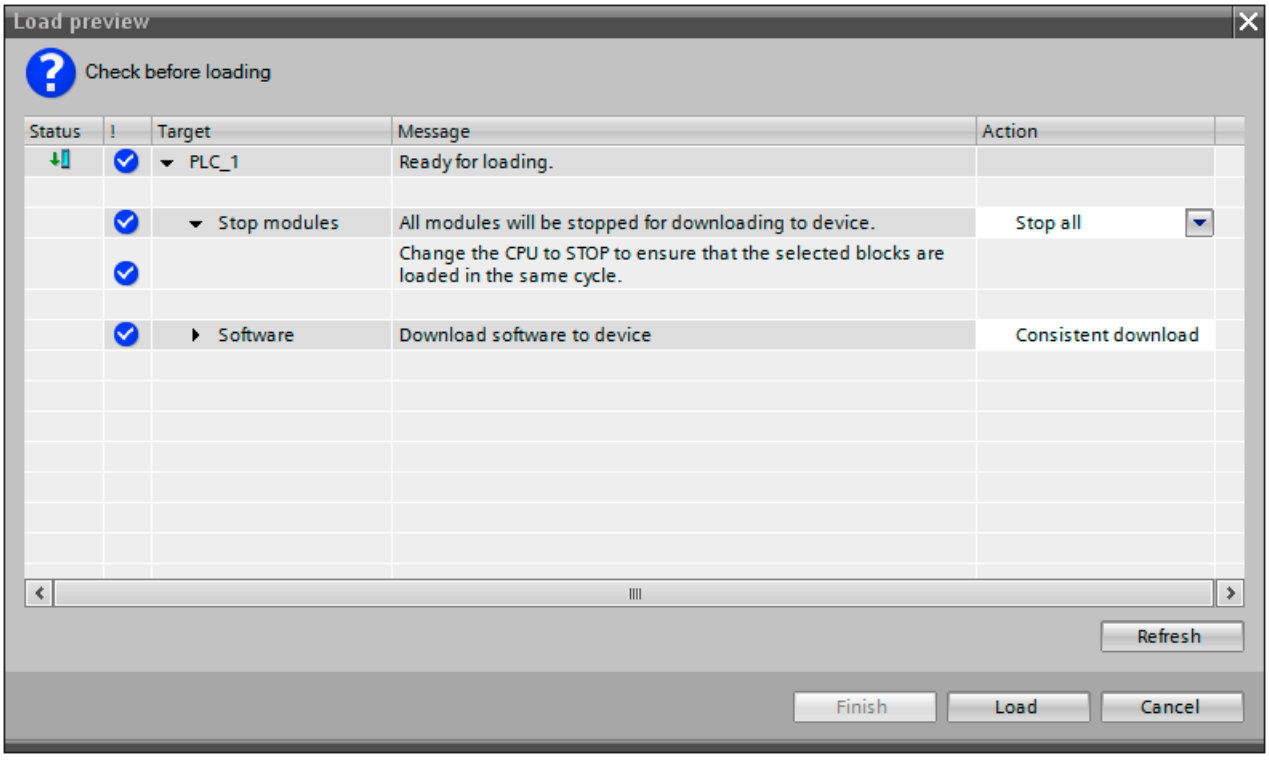
For loading the configured PLC project, the following preconditions must be fulfilled:

Precondition

- A network connection exists between the PG/PC and the PLC.
- The configuration to be loaded corresponds to the actual station configuration.
- You have loaded the hardware configuration into the module.
- The MCU is active:
  - NCK is in cyclic mode.
  - PLC in RUN or STOP mode.

Procedure

1. In the project tree, right-click "MCU_1 > PLC_1" and select "Load to device > Software (changes only)" from the shortcut menu.
   The "Load preview" dialog box opens.



2. In the "Download preview" dialog box, check the settings and then click "Load" to confirm the input.

Result

The PLC is stopped and the PLC program is loaded into the PLC. The "Results of the loading action" dialog opens and displays the status of the loading action. The dialog restarts the PLC after completion provided the "Start" checkbox has not been disabled.

6.5 First commissioning of the PLC completed

First commissioning of the PLC completed

Note

A reset (warm restart) of the NC is required for PLC-NC synchronization.

The PLC and NC are in the following state after a reset (warm restart):

- RUN LED is continuously lit green.
- Status display shows a "6" with a flashing point.
  ⇒ PLC and NC are in cyclic operation.

You have completed the first commissioning of the PLC.

Continue with the steps for "Guided commissioning" of SINAMICS drives.

You start with Reset (warm restart) for the NC and drive system.

Note

Response of the PLC in the case of an NC stop

For a stop of the NC, the PLC normally continues to run and the type of stop response is the user's responsibility depending on the machine situation. In this special case, the NC can no longer switch the outputs to zero and the current status is retained because the PLC is still running.

In order to switch off the outputs or to force a PLC stop, for example, the "NC READY" signal is evaluated in the PLC program.

Commissioning NC-controlled drives 7

7.1 Drive systems for SINUMERIK MC

Only external drive systems can be used when operating the SINUMERIK MC. The drive systems are configured and commissioned in the TIA Portal and in SINUMERIK ONE Commissioning.

A SINUMERIK MC is designed for use with the following drive systems:

- SINAMICS S120 (CU320-2)
- SINAMICS S210

You create the drive system suitable for your application and network it with a SINUMERIK MC.

Possible commissioning methods

- Basic commissioning using "SINAMICS Startdrive" in the TIA Portal, followed by fine parameterization in SINUMERIK ONE Commissioning
  Precondition: "SINAMICS Startdrive" option package in the TIA Portal
  With this method, the basic commissioning is carried out in the TIA Portal. The configuration data are loaded to the drive. The configuration of the telegram configuration, acceptance tests, and other detailed settings is then performed in SINUMERIK ONE Commissioning. SINUMERIK ONE Commissioning supports you with assignment of the components to the drive objects and axis assignment. This method is only available for S120 drives.
- Commissioning using "SINAMICS Startdrive" in the TIA Portal, followed by manual parameterization in SINUMERIK ONE Commissioning
  Precondition: "SINAMICS Startdrive" option package in the TIA Portal
  If a a MCU is used in conjunction with an S210 drive, this is the only method available to completely commission and configure the drive.
  In SINUMERIK ONE Commissioning, device configuration and axis assignment for S210 drives are performed manually.
- Commissioning using the device master data files in the TIA Portal
  Basic commissioning without the functions and optimization methods of the "Startdrive" application intended for the selected drive.

Note

You must install .NET Framework before installing SINUMERIK ONE Commissioning.

The USB flash drive containing the NET Framework software is included in the scope of delivery of the IPC.

7.2 Commissioning drives with "Startdrive"

7.2.1 Overview

You integrate drives of the SINAMICS family contained in the "SINAMICS Startdrive" option package in the TIA Portal using the "Startdrive" engineering tool.

You commission the SINAMICS S120 (CU320-2) and SINAMICS S210 drive systems via Startdrive by performing the following worksteps:

- Create or open a TIA Portal project
- Establish an online connection between Startdrive and the target device
- Create a device configuration in Startdrive offline or read one in from the drive (S120)
- Commission the drive via the control panel
- Set the basic parameters of the drive system in the SINUMERIK ONE Commissioning commissioning tool
- Load project data into the target device

Note

Perform device configuration detection for the drive system S120 in the TIA Portal. Startdrive in the TIA Portal automatically detects existing components and DRIVE-CLiQ interconnections, and creates the appropriate drive objects (DOs) and connections in the project.

The device configuration will only be detected for SINAMICS S120 drives if the drive is not assigned to a control system.

7.2.2 Reading out the device configuration from the drive

Introduction

The "Device configuration detection" function reads out the actual topology of your drive and uses this as the basis for the offline configuration in your TIA Portal project.

Note

The "Device configuration detection" function is available for the S120 drive system. The device configuration will only be detected for SINAMICS S120 drives if the drive is not assigned to a control system.

The wizard automatically identifies existing components and DRIVE-CLiQ interconnections, and creates the appropriate drive objects (DOs) and connections in the project.

The results of a detection run of the device configuration are listed in the dialog box "Device configuration detection".

All assignable components are listed in the table and are assigned as follows:

- Components are assigned to drive objects.
- Drive objects are assigned to drive units.

Note

Overwriting existing data in the device configuration

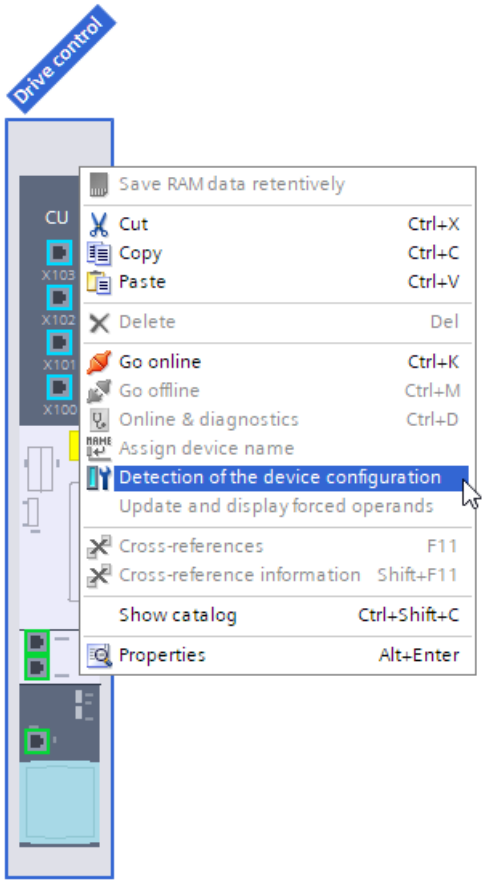
Existing components and their configuration are overwritten by the automatically detected device configuration.

Requirements

- A TIA Portal project is open.
- The device configuration contains a SINAMICS 120 Control Unit.
- There is a physical connection between the Ethernet interface of your PG/PC and the Ethernet or PROFINET interface of your drive.
- The drive is switched on.
- The drive is not yet connected to a control system.

Starting the device configuration detection

1. You can start device configuration detection in one of the following ways:
   - Project tree: In the shortcut menu of a drive unit or of a CU in the project tree, select the "Device configuration detection" entry.
   - Device view: In the device view in the shortcut menu of a CU, select the "Device configuration detection" entry.
   - Network view: In the network view in the shortcut menu of a CU, select the "Device configuration detection" entry.
   - Main menu: Run "Device configuration detection" in the "Online" menu.



Note

In order for you to be able to read the actual topology, there must be an online connection between the PG/PC and the drive unit. If a connection does not yet exist, the Connect devices online dialog box opens. In this dialog, establish a connection with the drive unit.

The topology of the drive unit is read out: Existing DRIVE-CLiQ interconnections are transferred directly from the actual topology of the drive unit.
The "Device configuration detection" dialog is displayed.
All located components are displayed in a tabular overview.

Components that cannot be assigned to any main component are displayed in the drop-down entry "Non-assignable components."

2. To cause an LED of a particular module in your actual topology to flash, select the "LED Flashing" option in the "Identification" column. This is how you can identify the module.
3. Assign non-assignable components to the main components. You have the following options for assigning the components:
   - Drag-and-drop: Drag the non-assignable components onto the main components. The system automatically observes the DRIVE-CLiQ interconnection rules. If the plug-in rules do not allow insertion into the component in question, a 'forbidden' cursor appears.
   - Shortcut menu: Right-click the component to be connected. All of the possible main components that are assignable as per the plug-in rules are listed in the shortcut menu of the components below the "Move" entry. Delete a component via the "Delete" menu entry. Change the name of a component via the "Rename" menu entry.

Selecting the drive object type of motor controllers

After the device configuration has been read out, the drive object type in the header of the dialog is automatically set to "High dynamic (servo)".

If you want to set another motor control, proceed as follows:

1. Presetting the drive object type:
   Select the option "Universal (vector)" or "High dynamic (servo)" to define the respective drive object type for all motor controllers. In this case, the drive object type can then no longer be changed in the tabular device overview.

   Note

   If one of the motor controllers does not support a control type as drive object type, this option can no longer be selected as a default setting. You must select the drive object type of each motor controller individually in this case.

2. Individually selecting the drive object type:
   Select the option "Can be selected" to individually define the drive object type for each motor control. Select the desired drive object type in the tabular device overview in the column "Drive object type" for each drive object in the drop-down list.

Assigning components

If all components found in the actual topology have been assigned, no further adaptations must be made in the "Device configuration detection"
dialog. The "Create" button can then be selected.
If the "Create" button cannot be selected (i.e. is grayed out), the topology of the components still has to be adapted:

1. All of the components that are found are displayed in a tabular overview in the lower area of the dialog.
   Components that are not assignable to a main component are displayed in the drop-down "Non-assignable components" entry.
2. To cause an LED of a particular module in your actual topology to flash, activate the "LED Flashing" checkbox in the "Identification" column. This is how you can identify the module.
3. Assign non-assignable components to the main components. You have the following options for assigning the components:
   - Drag-and-drop: Drag the non-assignable components onto the main components. The system automatically observes the DRIVE-CLiQ interconnection rules. If the plug-in rules do not allow insertion into the component in question, a 'forbidden' cursor appears. If components logically belong together, they are moved together and assigned.
   - Shortcut menu: Select the main component to be assigned in the shortcut menu of the component below the "Move" entry. Delete a component via the "Delete" menu entry. Change the name of a component with the "Rename" menu entry.

Using the parallel connection view

The parallel connection view supports you with parallel connection of components.

1. Activate the "Parallel connection view" checkbox.
   The "Connect in parallel at" shortcut menu is now available (see Step 2).
2. You have the following options for connecting components in parallel:
   - Drag-and-drop: Move the parallel interconnection-capable components together by dragging them to interconnect them in parallel.
   - Shortcut menu: In the shortcut menu, under menu item "Connect in parallel at" select the drive objects to which you want to connect the component in parallel.
   - The "All" entry connects the selected power unit to all of the interconnectable components in parallel.

   Any components which are hidden but associated with a component are automatically also interconnected in parallel.
3. Move the components via drag-and-drop to the higher-level drive unit to cancel a parallel connection. Alternatively, you can cancel the parallel connection via the "Undo parallel connection" menu entry in the shortcut menu. A new drive object appears as a result.

Cancelling a parallel connection

You can cancel an existing parallel connection as follows:

1. Drag components to the higher-level drive unit using drag-and-drop.
   - Or -
2. Select a component connected in parallel and select the "Disconnect parallel connection" shortcut menu.

Creating the configuration

After you have checked and, if required, corrected the topology determined in the configuration, you can transfer this topology to a Startdrive project.

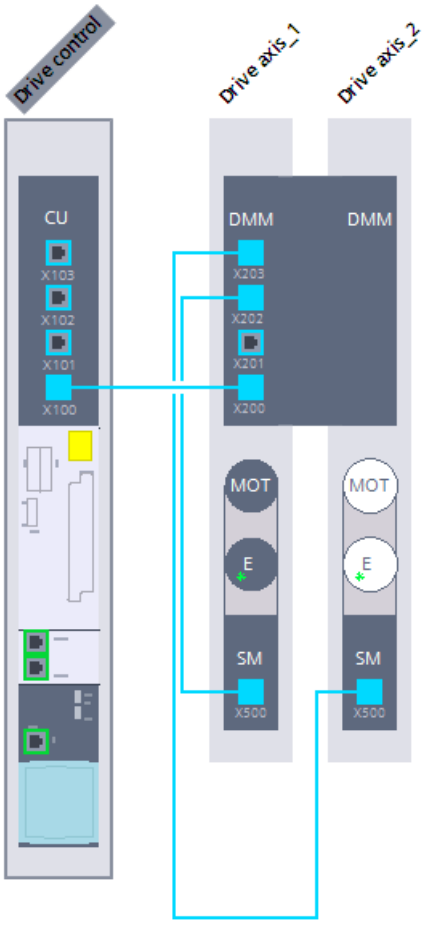
1. Make sure that there are no non-assignable components in the "Device configuration detection" dialog.
   Only when there are no non-assignable components is the "Create" button active.
2. Click the "Create" button.

The components are created in the offline condition. While the topology is being created, an interruptible progress dialog is displayed. If you interrupt the operation, the online connection is maintained. After creation, the topology is displayed in the device view.

Result

The topology is created in the device configuration of the selected drive unit. The view changes into the device view.

The online connection with the target device is automatically disconnected. As a consequence, you can immediately make changes to the specification or configuration of the components. This would not be possible in the online mode.



7.2.3 Inserting the drive offline

Introduction

You can also create drive units manually in the TIA Portal.

You configure your SINAMICS drive offline in the "Device view". You insert the individual components of the SINAMICS drive and connect them.

Preconditions

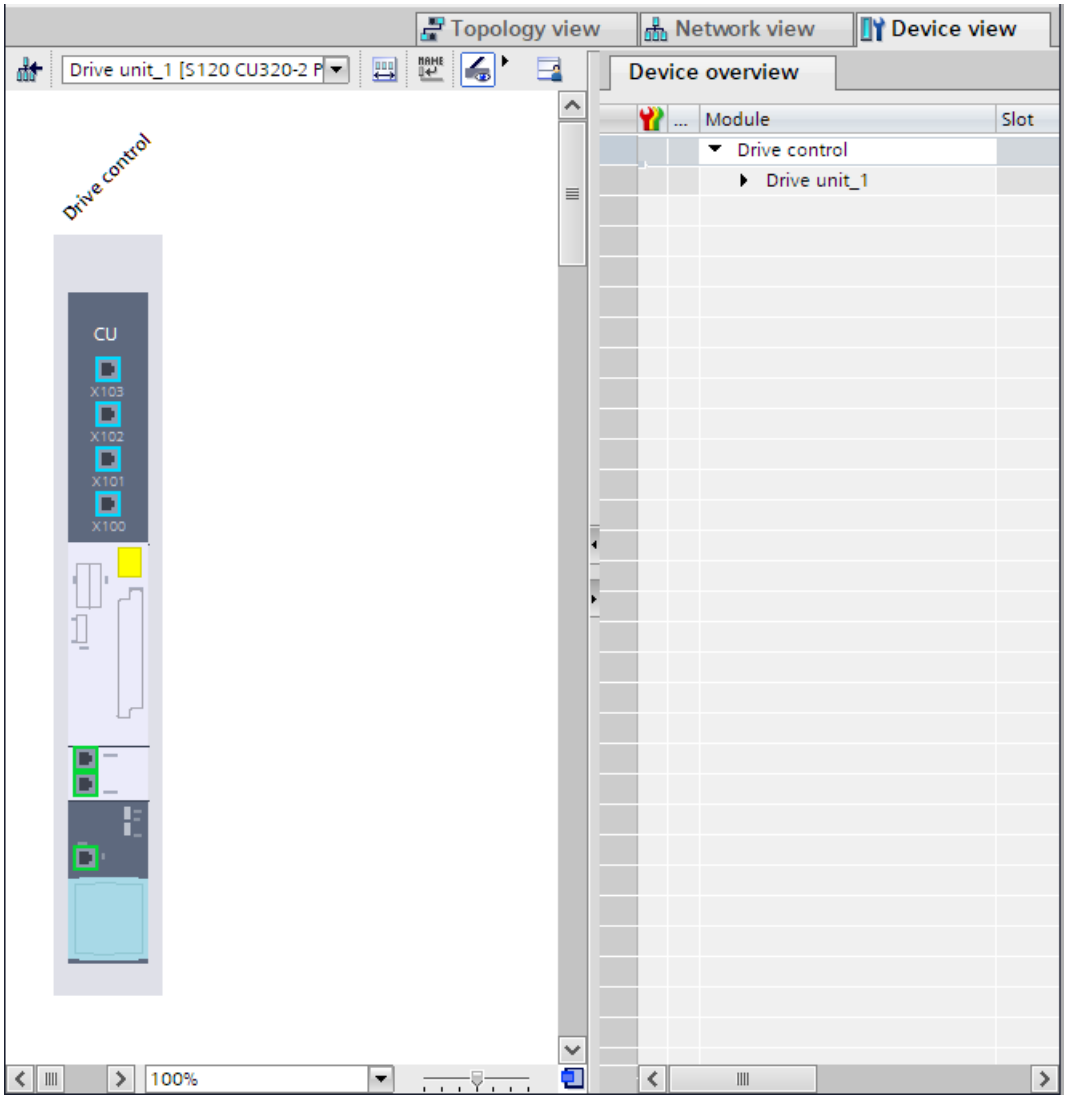
- A project is open in the TIA Portal.
- The device view is active.

Procedure

Proceed as follows to insert a SINAMICS S drive:

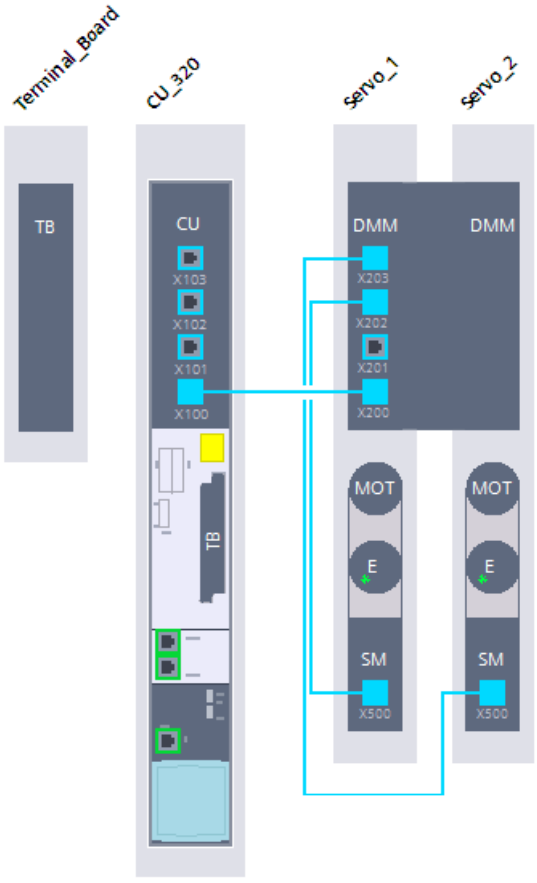
1. Double-click "Add new device" in the project navigation.
   The "Add new device" dialog box opens.
2. Click the "Drives" button to limit the list of devices to just drives.
   All of the available SINAMICS control modules are now displayed in the drop-down list.
3. Select the required SINAMICS drive from the list.
4. When required, assign a different device name for the drive - or change the suggested firmware version.

5. Click "OK" to confirm your settings.
   As soon as the "Open device view" option is activated, the SINAMICS drive is automatically created and displayed in the device view.



   The drive appears below "drive_unit_1" in the project navigator.

6. Supplement the drive with the other components required (S210: Motor, Encoder, S120: Line Module, Power Module, Motor, Encoder, etc.).



The components used by the SINAMICS drive are listed in the "Device overview".

Device overview

	...	Module	Slot	Type	Article no	Drive ...	Firmw..	HW ve..	Slot connectio...
		Drive control				1			
		Drive unit_1		CU320-2 PN	6SL3040-1MA01-0...	1	V5.2		
		Input/output object_1				2			
		Terminal Board_1		Terminal Board TB30	6SL3055-0AA00-2...	2			
		Drive axis_1				3			
		Motor Module_1		Single Motor Modu...	6SL3x2x-1xxxx-xxxx	3			

Result

As soon as the drive system has been created, it appears in the project navigator under "drive_unit_1" together with the following entries:

- Device configuration
- Online & diagnostics

- Parameter:
  - Function view: Parameter assignment on the graphical interface. The individual screen forms are based on the function diagrams and include the parameters required.
  - Parameter view: Clearly organized representation of the parameters available for the device.
- Commissioning
- Acceptance test
- Traces

For **further information** about configuring drives with Startdrive, see Commissioning Manual "SINAMICS S120 with Startdrive".

7.2.4 Networking the drive with the control system

Introduction

You can configure the telegrams and drive-integrated safety functions in the TIA Portal via the SINAMICS drives (S120 or S210). You can configure the MCU and the networked drives entirely in the TIA Portal and do not need to import configuration data from other previously parameterized engineering tools into the TIA Portal. The requirement for this is that the drive has also been created in the project and is networked with the MC.

Preconditions

- A project is open in the TIA Portal.
- A SINUMERIK MCU has been created.
- The device view is active.

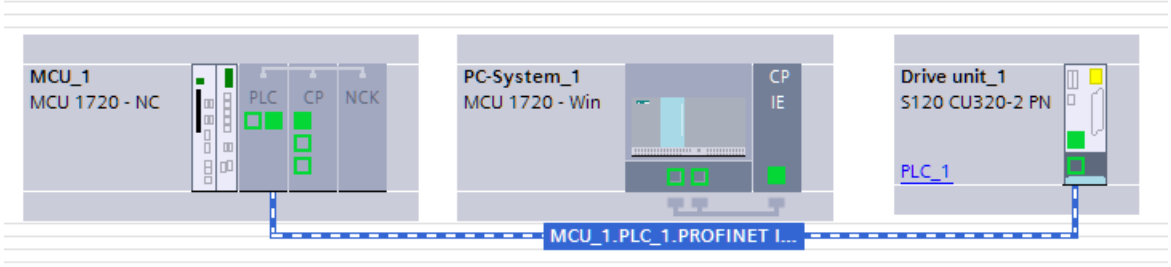
Procedure

Proceed as follows to establish the connection between the SINUMERIK MC and the SINAMICS drive:

1. Switch to the network view.
2. In the drive view, click "Not assigned" and under "Select IO controller" select "MCU_1.PLC_1.PROFINET_Interface_150".
   Alternatively, drag a connection between a PROFINET interface of the SINUMERIK MC (e.g. the PLC) and the PROFINET interface of the SINAMICS drive.
   The PROFINET IO system is created and the drive is assigned to the control.

Note

A PROFINET IO system and a sync domain with the two nodes are created automatically. If you assign another IO device to the IO system of the IO controller, the IO device is assigned automatically to the sync domain of the IO controller.



Note

You need a telegram for the communication between a control and a drive.

After inserting the IO device, you can configure the sync domain and the isochronous mode of the IO device. Isochronous mode is required for typical motion control applications.

7.2.5 Preparing communication via PROFINET IO

7.2.5.1 Configure sync domains and send clock

Configuring sync domains

A sync domain is needed for synchronizing PROFINET IO devices. The sync domain ensures that all nodes that belong to the domain are synchronized. After being inserted, the nodes of the sync domain are not synchronized. The drive and control together form a sync domain.

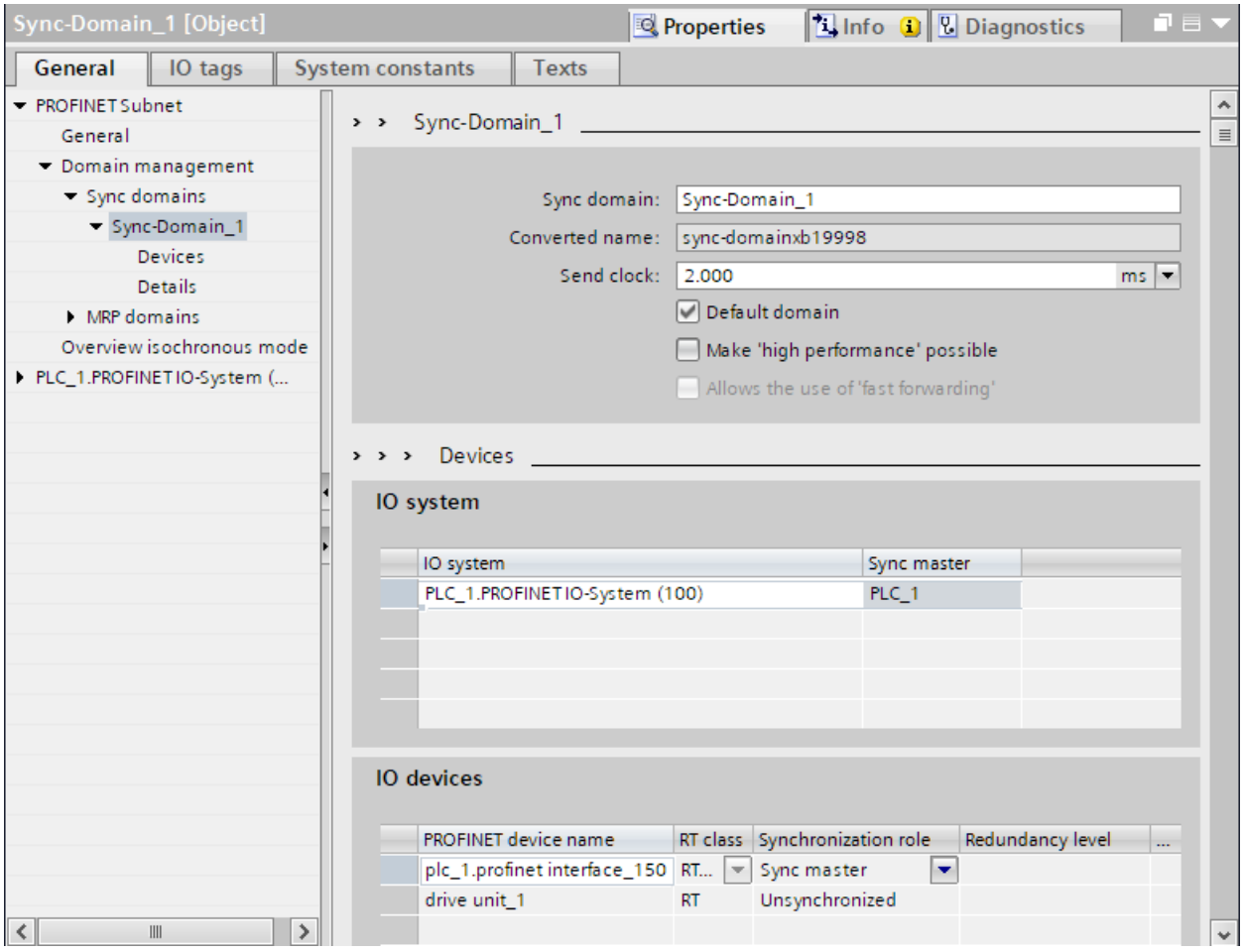
After you have inserted a control and a SINAMICS drive unit, you must first assign them to a subnet. Unassigned devices are displayed as "Not assigned".

To configure the sync domain, proceed as follows:

1. Select the PROFINET IO system in the network view.
2. In the Inspector window, click the "General" tab and select "Domain management > Sync domain > Sync domain_1" and make the necessary parameter settings.
   You can set a new name at "Sync domain". It is converted automatically to a conformant name that is displayed at "Converted name".
3. Under "IO-Devices" assign synchronization roles to the devices: role "Sync master" to the PLC of the MCU and the role "Sync slave" to the drive unit.
4. Select the "send clock" for the sync domain.

Note

You can set the send clock only when you have configured the synchronization role and the RT class at "IO devices".



Explanation of the parameters

Parameter	Description
Sync domain	Name of the sync domain. This name is converted automatically if it does not conform with the DNS conventions.
IO devices	Here, you can see a list of the IO devices of the sync domain. You can select the following parameters for the nodes: • RT class: Select either RT (Real Time) or IRT (Isochronous Real Time). • Synchronization role: Select sync master or sync slave. The synchronization role is displayed as "unsynchronized" by default, e.g. for devices in RT networks.
Send cycle	Select the send clock for the sync domain here.
Nodes	The nodes of the PROFINET IO system are listed here.

7.2.5.2 Configuring topology and ports

Interconnecting ports

Prerequisite for IRT is the topology configuration with the specification of which device is connected via which port to which other devices.

There are two options for defining the properties of the cables between the ports of the switches:

- Via the topology view
- Via the object properties

Using the topology view

With the topology view you have an overview of all ports in the project and can interconnect them centrally.

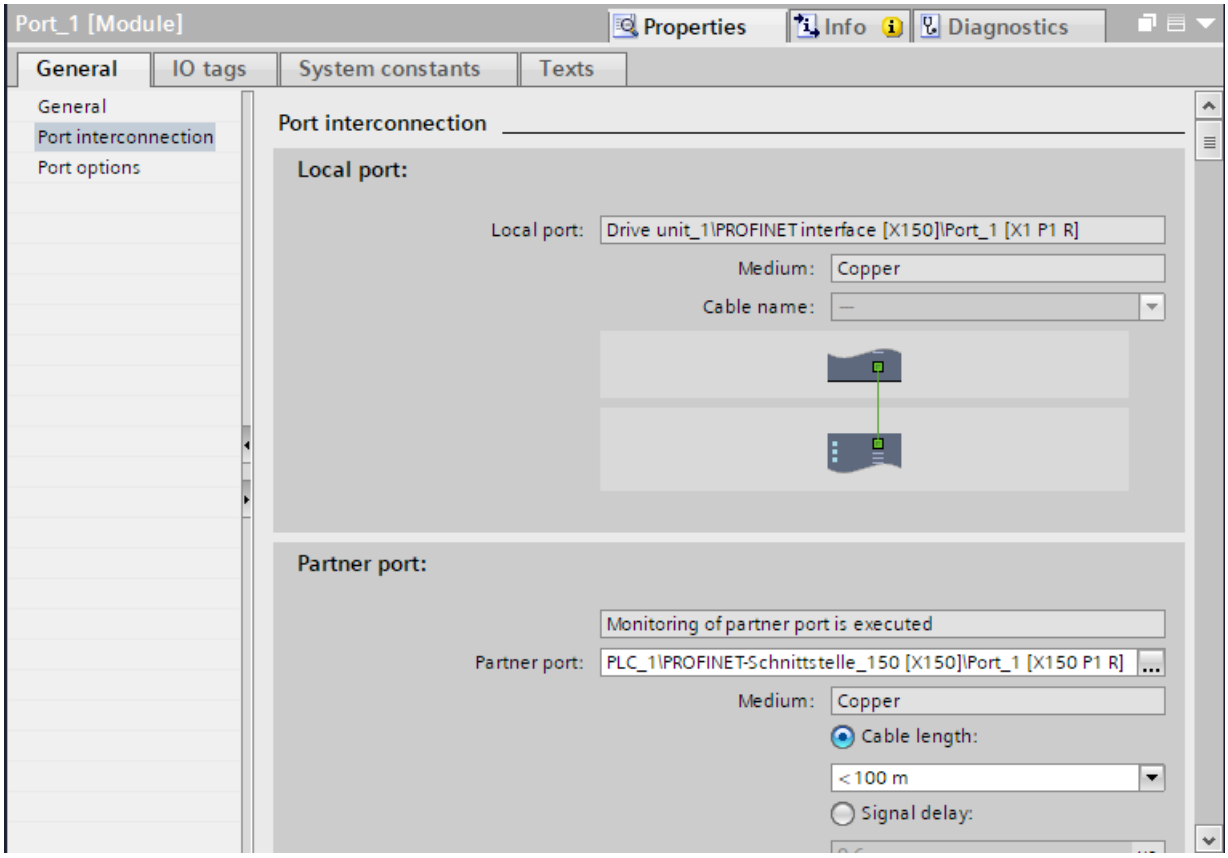
To configure the topology, proceed as follows:

1. Click the "Topology view" tab.
   You can perform the following in the topology view:
   - Interconnect ports
   - Modify the properties of the interconnection
   - Insert passive components
   - Arrange for an offline/online comparison to be displayed in online mode
2. If you hover the mouse over the ports, port names are displayed in the tooltip. In the Inspector window, the properties for each selected port/device are displayed.
3. Click the source port and drag the connection onto the target port.
   The topology view then shows the connection between the two ports.

Port interconnection via the properties

After the selection of a device or an interface, the entries for the ports are displayed in the Inspector window in the "General" tab at "PROFINET PN / IO interface > Advanced options" or "Advanced options".

1. Select the interface, whose ports you want to edit, from the Inspector window.
2. Select the interface you wish to interconnect.
3. Select the "Port interconnection" entry.
   The "Local port" and "Partner port" dialogs open.



4. Open the "Partner port" drop-down menu.
   All devices with their PROFINET interfaces are shown.
5. Below the respective interface, select the port you want to connect to the selected port.
   Ports that you cannot connect are marked in red. Ports that are already assigned are not displayed.
   The connection between the ports is displayed in the topology view.
6. If necessary, edit the other parameters of the port.

7.2.5.3 Set up the sync master and sync slave.

Preconditions

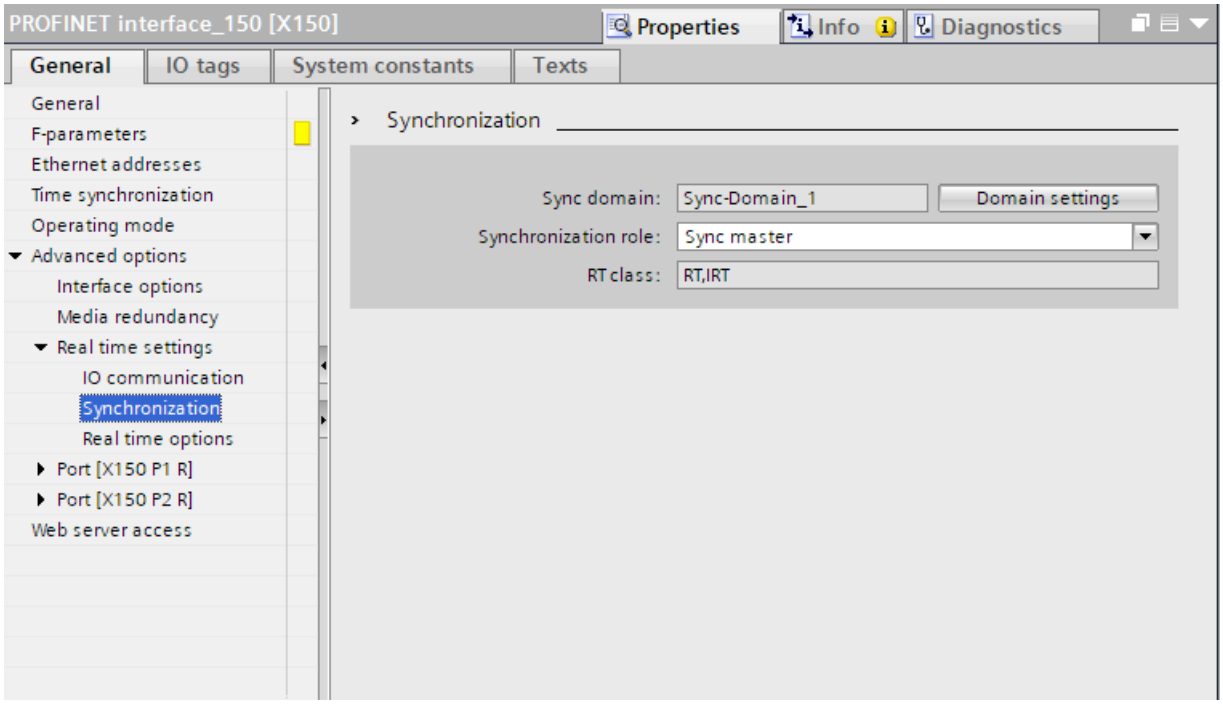
You have performed the following configuration steps:

- IO controller and IO device configured with RT
- Port interconnections are configured

Configuring the sync master

To configure a sync master, proceed as follows:

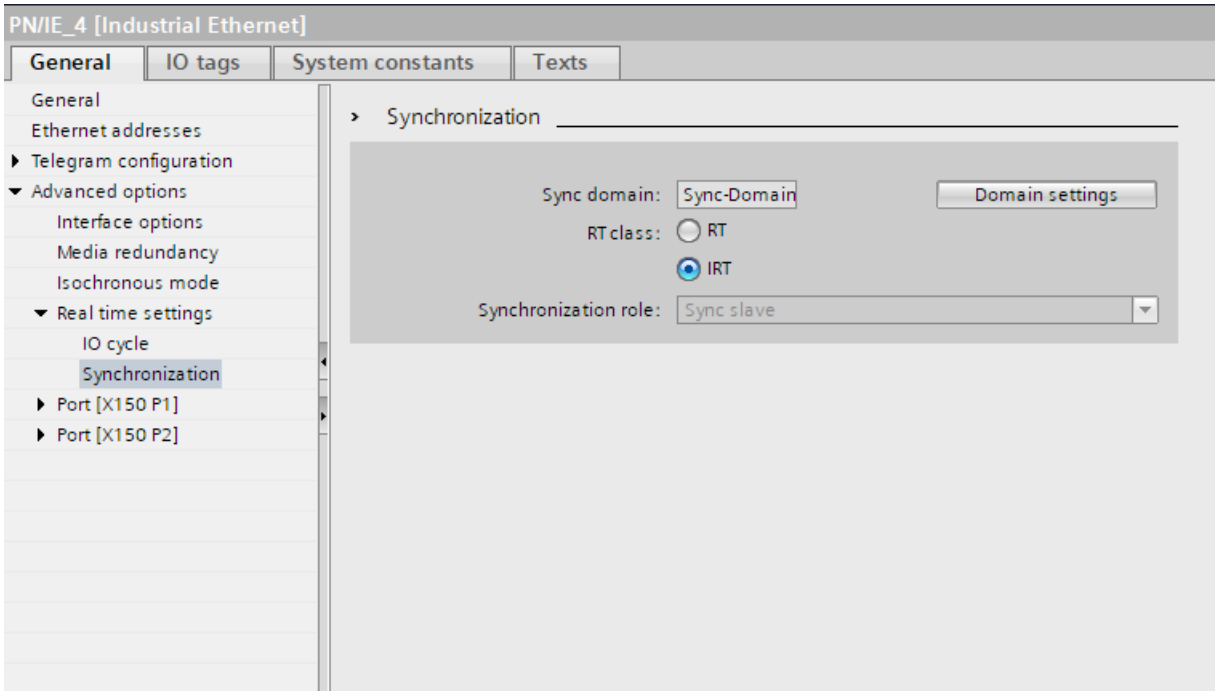
1. Select the PROFINET interface of the sync master in the network view, e.g. the PLC interface of the SINUMERIK MCU.
   The interface settings are displayed in the Inspector window.
2. Under "General", click "Extended options > Real-time settings > Synchronization".
3. Select the "Sync master" entry at "Synchronization role".



Configuring the IO device as a sync slave

To configure a device within a PROFINET IO system as a sync slave, proceed as follows:

1. Select the PROFINET interface for the sync slave in the network view, e.g. the interface of the drive system.
   The interface settings are displayed in the Inspector window.
2. Under "General", click "Extended options > Real-time settings > Synchronization".
3. Select RT class "IRT".
   The entry "Sync slave" is automatically selected under "Synchronization role".



7.2.5.4 Configure isochronous IO device

Configuring isochronous mode for IO devices

The drive and controller together form a sync domain. You must parameterize the IRT operating mode (for isochronous drives) and the PROFINET settings for motion control applications of the PROFINET IO system. Isochronous mode for the application on the bus is only possible for PROFINET IO with IRT. In the case of PROFINET IO with IRT, a sync master generates a synchronization telegram to which all sync slaves synchronize themselves. To use isochronous mode, you must configure it for the IO device.

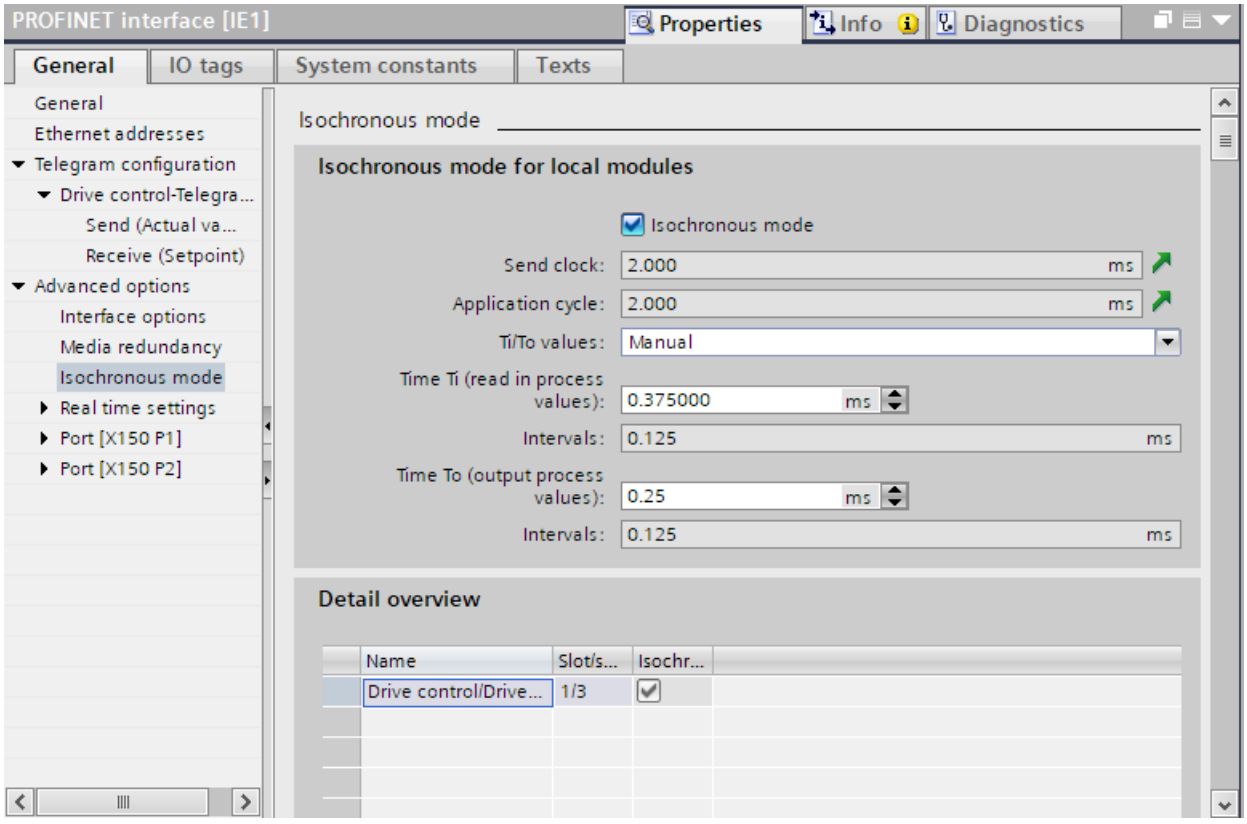
Note

Isochronous mode only applies if isochronous submodules are configured in the IO device so that the IO controller has isochronous IO submodules. Otherwise, the Save and compile in the TIA Portal will be terminated with an error message.

To configure isochronous mode in the TIA Portal, you should therefore have already configured the drive and an axis for the control and assigned it to a drive object in Startdrive.

To configure isochronous mode, proceed as follows:

1. Select the IO device in the network view and click the PN interface.
   The interface properties are displayed in the Inspector window.
2. In the Inspector window, under "General", click "Extended options > Isochronous mode".
3. Activate the "isochronous mode" option.
   In the "detailed overview", the drive objects are displayed with the appropriate telegrams. You must already have configured the objects and telegrams in Startdrive.
4. If necessary, activate the option "Isochronous mode" for the drive object in question. This setting cannot be changed for telegrams for which isochronous mode is essential (e.g. telegram 105).



Parameterizing isochronous mode

Isochronous mode can be activated and deactivated for each IO device or module in the IO device. You will find a more detailed description of the possible settings for isochronous mode in the following table.

Parameter	Description
Isochronous mode	Activate this option if you want to operate the drive (IO device) in isochronous mode with the PROFINET IO.
Send clock	Shows the send clock of the PROFINET IO system. Click the link to edit the setting.
Application cycle	Shows the application cycle (multiple of the data cycle).
Ti/To values	Three settings are possible for the Ti/To values: • Automatic: Ti/To is automatically calculated. • Manual: Ti/To can be edited. • Task: Ti/To values are transferred to the OB. Ti, To: can only be edited if "manual" is set. Ti_{Min}/Ti_{Max}: minimum or maximum time for Ti. To_{Min}/To_{Max}: minimum or maximum time for To. Interval: defined interval for Ti/To values.
Time Ti (actual value)	Specifies at what time Ti, the actual value will be read in before the cycle starts.
Intervals	Indicates in which interval the value will be read in. The value should not be changed.

Parameter	Description
Time To (setpoint)	Specifies at what time To, the setpoint will be read out after the end of the cycle.
Interval	Indicates in which interval the value will be read in. The value should not be changed.

7.2.6 Configuring telegrams

7.2.6.1 Overview of telegram configuration

Description

If communication is established between the drive and higher-level control system via PROFINET IO, the data (setpoints and actual values) are cyclically transferred using PROFIdrive telegrams.

Because SINUMERIK MCU does not have its own telegram configuring function, the telegram must be configured via a connected SINAMICS drive.

To configure a cyclic data transfer, proceed as follows:

- Insert and network the drive and control in the TIA Portal
- Insert the PROFINET subnet in the drive
- Check the PROFINET settings
- Parameterize the drive
  - SINAMICS S210 drives
    You must create telegrams for the drive control.
  - Multiple-axis drives (SINAMICS S120, S210)
    You must create telegrams for the relevant drive objects, such as drive axes, drive control or infeed
- Check and edit the telegram settings
  For all telegrams that are processed by the NCK (e.g. closed-loop control telegrams), you must choose process image partition "PIP_NCK".
- If you are controlling a drive with safety functions via PROFIsafe, you must insert the appropriate PROFIsafe telegram.

Telegram overview

The following table shows the telegrams for PROFIdrive communications:

Drive system	Designation	Purpose
S120	SIEMENS telegram 136	Manufacturer-specific telegram. Permits the use of the following data: • Dynamic Servo Control (DSC) • Torque feedforward control • 2 position encoders (encoder 1 and encoder 2) • 4 trace signals
S120	SIEMENS telegram 391	Manufacturer-specific telegram for PROFIdrive communication. Permits the use of the following data: • Access to onboard I/O of the CU • Use of the control and status word of the CU (CU_STW, CU_ZSW) • Central measuring probe evaluation of up to 2 probes This telegram is used by the MCU for PROFIdrive communication between the NC and DRIVE.
S120	SIEMENS telegram 370	Manufacturer-specific telegram for communication of the infeed (Infeed / Active Infeed (A_INF)).
S210	SIEMENS telegram 105	Manufacturer-specific telegram for PROFIdrive communication.

The telegram configuration (e.g. telegram address, telegram type) in the SINUMERIK ONE Commissioning Tool must match the configuration in the TIA Portal.

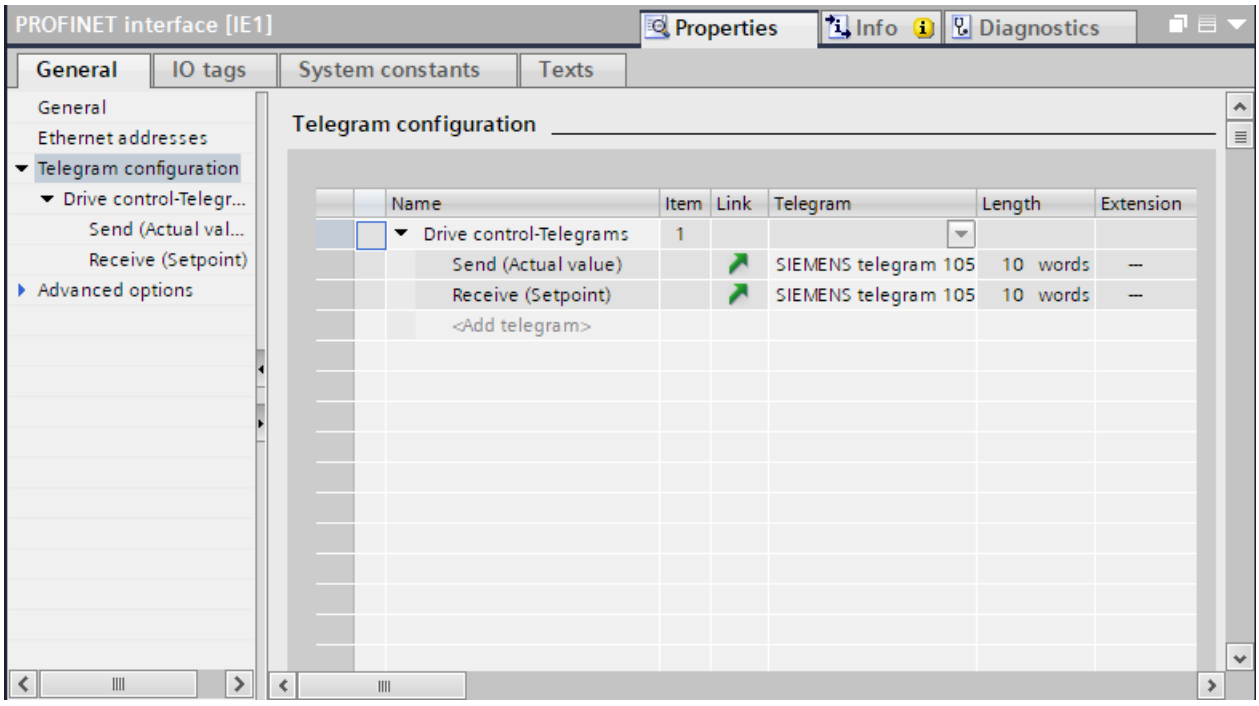
7.2.6.2 Displaying telegram configuration

The "Telegram configuration" screen form is part of the device configuration and is displayed in the Inspector window.

You can open this screen form either in the project navigator or, for Startdrive S drives, also by using direct links in the communication screen forms.

Calling telegram configuration via project navigator

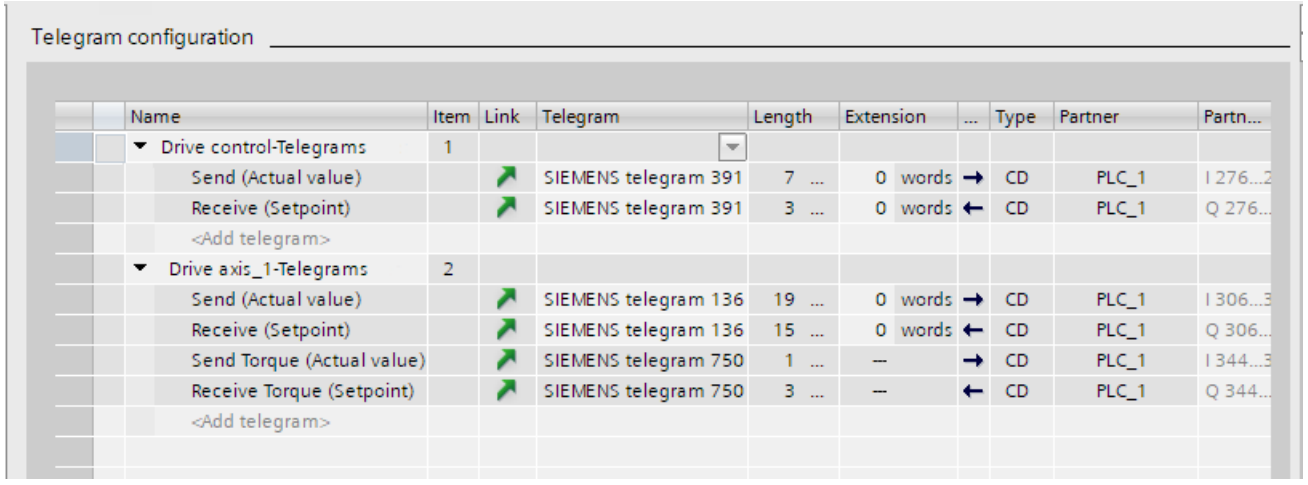
1. In the network view, select the IO device (S210 drive) and then click the PROFINET interface.
2. In the Inspector window, select "Properties > Telegram configuration".
   The telegram configuration settings are displayed.



7.2.6.3 Settings for SINAMICS S120

Telegram configuration for S120 drives

The dialog box for the telegram configuration is structured as follows:

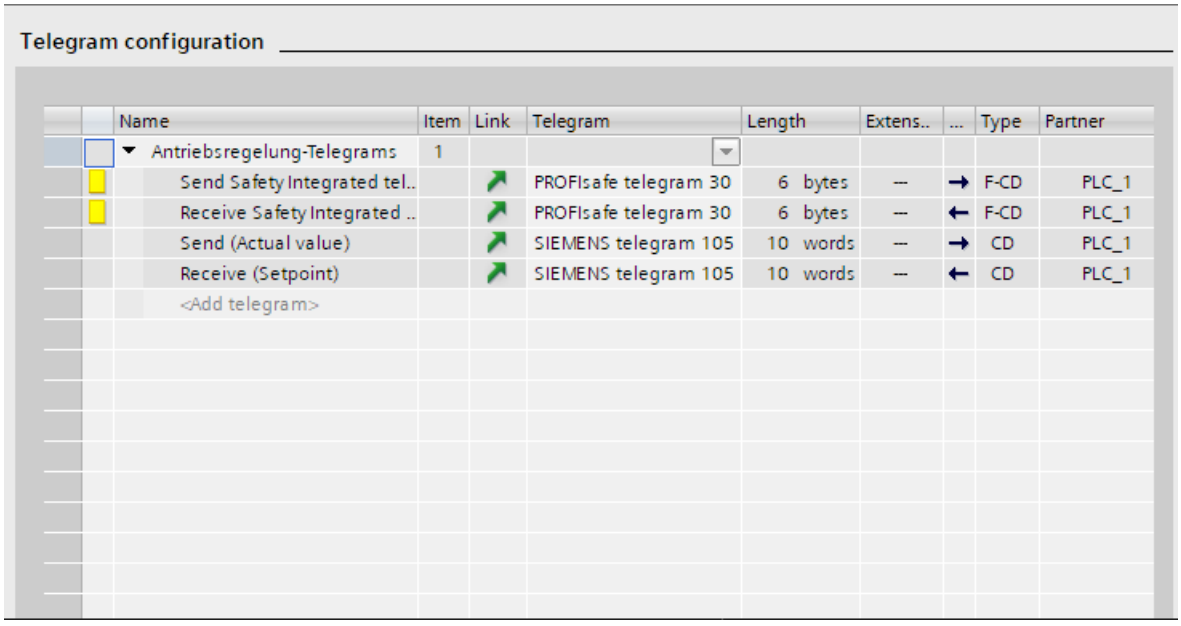


In the telegram configuration area, you can create telegrams and view their properties.

7.2.6.4 Settings for SINAMICS S210

Telegram configuration for S210 drives

The dialog box for the telegram configuration is structured as follows:



In the telegram configuration area, you can create telegrams and view their properties.

7.2.6.5 Parameterizing sending (actual value/safety actual value)

Description

Edit the following parameters for the setpoints of the communication between the drive and the control system. The communication direction is from the drive to the partner (e.g. a controller). The settings relevant to PROFIsafe are marked yellow and only displayed when you add a PROFIsafe telegram.

Note

Check of the PROFIsafe telegrams

By default, the setting of the PROFIsafe telegrams under "Telegram configuration" is not password-protected.

- Apply the TIA Portal project protection to the whole project to protect the telegram settings from being accidentally or deliberately overwritten.
- When working with PROFIsafe telegrams, check the setting of the PROFIsafe telegrams again during the safety acceptance process in order to ensure that the selected PROFIsafe telegram corresponds to the requirements of your application.

Parameter	Drive	Controller
Name	Name of the drive in the project	Name of the assigned controller in the network view. The assignment can only be changed there.
Role	Device	Controller
Telegram	Drop-down list for selecting the telegram (default setting is Telegram 1)	
Telegram (PROFIsafe)	Drop-down list to select the PROFIsafe telegram (default setting is telegram 30).	
IP address (PN drives)	IP address of the drive	IP address of the IO controller (cannot be changed)
F address (only for PROFIsafe)	PROFIsafe address of the destination (F_Dest_Add). The address uniquely identifies the destination.	PROFIsafe address of the source (F_Source_Add). The address uniquely identifies the source.
Slot	Slot of the device	-
Start address	Drop-down list to select the process data word (PZD)	Next free start address for the configured module. You can accept or change the address.
Length	Length of the selected telegram Can only be changed on "free telegrams".	
Extension	Most standard telegrams or Siemens telegrams can be changed. Safety Integrated telegrams and free telegrams cannot be extended. Enter the telegram extension here for the transfer of the actual value. If you have entered an extension at "Telegram configuration", it is also displayed here.	
Consistency	The use of various consistency areas is useful to optimize the performance of an S7-CPU. Consistency areas that are longer than two words must be edited with system functions. You can use the effective Load/Transfer commands for consistency areas up to two words. **Total length:** The consistency applies for all data of this slot. This default entry should usually be sufficient. **Unit**: The consistency applies for one process data word. You must configure at least a "2" word "Total length" for the transfer of a double word.	
Organization block	Select the organization block from the drop-down list. If you have assigned the drive to a controller, you require an organization block for the communication between the drive and the controller. If, for example, you create for an S7-1500, a technology object of the "Positioning axis" type and assign it to a drive axis, you then require an organization block of the "MC-Servo [OB91]" type. The communications must then be isochronous. Further OBs are, for example, Main [OB1] or for safety functions, an FOB_RTG1 [OB123].	
Process image	Select the process image partition that you want to use in the drop-down list in order to transfer the data consistently, e.g. OB1-PI.	
Interrupt OB number	Use the interrupt OB to output diagnostic information.	

Parameter	Drive	Controller
F-watchdog time	Monitoring time in the fail-safe DP standard slave / IO standard device / PA field device. A valid, current safety telegram must arrive from the F-CPU within the monitoring time. This ensures that failures and errors are detected and the appropriate reactions triggered to keep the F system in a safe state or to transfer it to a safe state.	
F-I/O DB number	The number of the block that controls the F-I/O.	
F-I/O DB name	The name of the block that controls the F-I/O.	

7.2.6.6 Parameterizing receiving (setpoint/safety setpoint)

Description

Edit the following parameters for the setpoints of the communication between the drive and the control system. The communication direction is from the partner (e.g. a controller) to the drive. The settings relevant to PROFIsafe are marked yellow and only displayed when you add a PROFIsafe telegram.

Note

Check of the PROFIsafe telegrams

By default, the setting of the PROFIsafe telegrams under "Telegram configuration" is not password-protected.

- Apply the TIA Portal project protection to the whole project to protect the telegram settings from being accidentally or deliberately overwritten.
- When working with PROFIsafe telegrams, check the setting of the PROFIsafe telegrams again during the safety acceptance process in order to ensure that the selected PROFIsafe telegram corresponds to the requirements of your application.

Parameter	Drive	Controller
Name	Name of the drive in the project	Name of the assigned controller in the network view. The assignment can only be changed there.
Role	Device	Controller
Telegram	Drop-down list for selecting the telegram (default setting is Telegram 1)	
Telegram (PROFIsafe)	Drop-down list to select the PROFIsafe telegram (default setting is telegram 30).	
IP address (PN drives)	IP address of the drive	IP address of the IO controller (cannot be changed)
F address (only for PROFIsafe)	PROFIsafe address of the destination (F_Dest_Add)	PROFIsafe address of the source (F_Source_Add)
Slot	Slot of the device	-
Start address	Drop-down list to select the process data word (PZD)	Next free start address for the configured module that you can accept or change.

Parameter	Drive	Controller
Length	Length of the telegram Can only be changed on "free telegrams".	
Extension	Most standard telegrams or Siemens telegrams can be changed. Safety Integrated telegrams and free telegrams cannot be extended. Enter the telegram extension here for the transfer of the setpoint. If you have entered an extension at "Telegram configuration", it is also displayed here.	
Consistency	The use of various consistency areas is useful to optimize the performance of an S7-CPU. Consistency areas that are longer than two words must be edited with system functions. You can use the effective Load/Transfer commands for consistency areas up to two words. **Total length:** The consistency applies for all data of this slot. This default entry should usually be sufficient. **Unit**: The consistency applies for one process data word. You must configure at least a "2" word "Total length" for the transfer of a double word.	
Organization block	Select the organization block from the drop-down list. If you have assigned the drive to a controller, you require an organization block for the communication between the drive and the controller. If, for example, you create for an S7-1500, a technology object of the "Positioning axis" type and assign it to a drive axis, you then require an organization block of the "MC-Servo [OB91]" type. The communications must then be isochronous. Further OBs are, for example, Main [OB1] or for safety functions, an FOB_RTG1 [OB123].	
Process image	Select the process image partition that you want to use in the drop-down list in order to transfer the data consistently, e.g. OB1-PI. For information on process images, please enter the term in the online help search.	
Interrupt OB number	Use the interrupt OB to output diagnostic information.	
F-watchdog time	Monitoring time in the fail-safe DP standard slave / IO standard device / PA field device. A valid, current safety telegram must arrive from the F-CPU within the monitoring time. This ensures that failures and errors are detected and the appropriate reactions triggered to keep the F system in a safe state or to transfer it to a safe state. Activate the "Manual assignment of the F-I/O DB number" option if you want to enter the monitoring time manually.	
F-I/O DB number	The number of the block that controls the F-I/O.	
F-I/O DB name	The name of the block that controls the F-I/O.	

7.2.6.7 Structure of the telegrams, control and status words

Structure of the telegrams

The selection of a telegram determines the process data of the drive unit (Control Unit) that is transferred.
From the drive unit view, the received process data represents the receive words and the process data to be sent represents the send words.

The receive and send words consist of the following elements:

- Receive words: Control words or setpoints
- Send words: Status words or actual values

To maintain the PROFIdrive profile, the following must apply:

- Interconnect PZD receive word 1 as control word 1 (STW1).
- Interconnect PZD send word 1 as status word 1 (ZSW1). (The WORD format must be used for PZD1)

One PZD (process data item) corresponds to one word.

The signals of the control and status words are connected via BICO to the corresponding signals of the drive.

7.2.6.8 Editing telegrams

Overview

You can edit telegrams in the following way:

- Extending standard or Siemens telegrams
- Adding telegrams

Requirement

- You have created a SINUMERIK MCU and a SINAMICS drive (S210 or S120) and connected them via a PROFINET fieldbus.

Extending telegrams

Send and receive telegrams can be extended in the same way. A send telegram is extended in the send direction and a receive telegram is extended in the receive direction. You can set the extension either in the table "Telegram configuration" or in the telegram detail screen form.

To extend a telegram, proceed as follows:

1. In the Inspector window, select "Properties > PROFINET interface > Telegram configuration". Telegrams that you have created are displayed for each existing drive object.
2. In the table "Telegram configuration", select a telegram.
3. In the field "Extension", enter the number of words by which you wish to extend the telegram.
4. Click in another field to accept the input.
   The telegram is extended by the entered number of words.
   You can have additional telegram details displayed in a communication screen form.
5. Click the link to open the appropriate communication screen form.
   In the case of S120 drives, you can connect additional signals in this communication screen form.
6. Interconnect the additional signals there.

Note

Extension not possible

The following telegram types cannot be extended:

- Free telegrams 999
  However, the length of these telegrams can be changed.
- Safety Integrated telegrams:
  - PROFIsafe telegrams 30, 31
  - Siemens- telegrams 901, 902, 903
- Currently on S210 drives,

a selected telegram cannot be extended, which is why the field "Extension" is grayed out.

Adding telegrams

You can add the following telegrams once as long as they are not yet included in the telegram list of the drive object:

- Safety Integrated telegram
- Supplementary telegram
- Torque telegram
- Actual value
- Setpoint

To add a telegram, proceed as follows:

1. In the Inspector window, select "Properties > PROFINET interface > Telegram configuration". Telegrams that you have created are displayed for each existing drive object.
2. Click the "Add telegram" entry (at the required drive object).
   A drop-down list opens. All telegram types that have not been assigned yet can be used.
3. Select the required telegram type.
   The entries for the telegram are created.
4. If required, change the telegram type now, e.g. from telegram 30 to telegram 900. An actual value slot or a setpoint slot are created for the additional data with a "Free telegram".

Result

The telegram has been extended by the entered number of words or a new telegram has been added.

7.3 Commissioning drives via device master files

7.3.1 Overview

If you do not have the "SINAMICS Startdrive" option package or for drives of the SINAMICS family that are not contained in the "SINAMICS Startdrive" option package, you integrate drives in the TIA Portal using the device master files.

You commission a drive in the device master files in the following steps:

- Create or open a TIA Portal project
- Insert an SINUMERIK MCU
- Insert a drive system, e.g. SINAMICS S120 CU320, from the hardware catalog into the project
- Interconnect SINUMERIK MCU and the drive system
- Set the basic parameters of the drive system
- Create and configure the drive axes and telegrams for communication
- Load project data into the target device
- Establish an online connection between Startdrive and the target device
- Perform the commissioning steps

7.3.2 Inserting and networking a SINAMICS drive

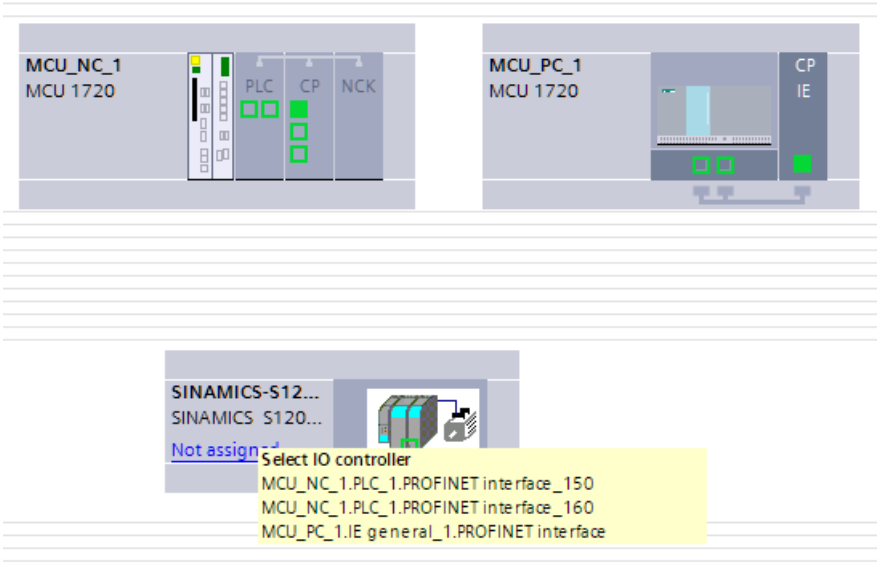
Preconditions

- The TIA Portal has been started.
- A SINUMERIK MCU has been inserted.

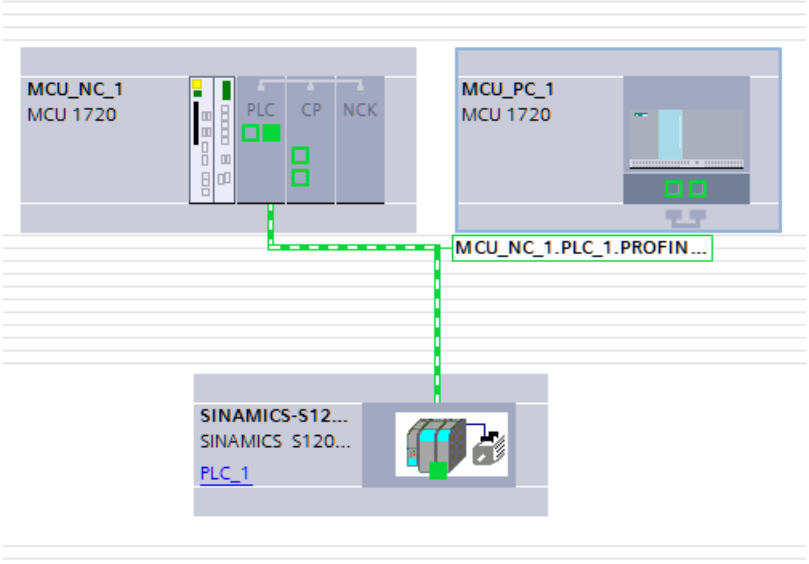
Procedure

1. Switch to the "Network view".
2. In the hardware catalog under "Further field devices > PROFINET IO > Drivers > SIEMENS AG > SINAMICS > Head module", select a drive, e.g "SINAMICS S120/S150 CU320-2 PN Vx.x".
3. Drag the drive onto the "Network view".
   The drive appears in the network view.
   In the project navigator, the drive appears in the project navigator below "Ungrouped devices".

4. To establish a connection to the PN IO interface of the controller, in the drive view, click "Not assigned" and under "IO controller" select "MCU_1.PLC_1.PROFINET_Interface_150".



The PROFINET IO system is created and the drive is assigned to the control.



5. To connect the control and the drive in the topology view, switch to the "Topology view".

Note

You need a telegram for the communication between a control and a drive.

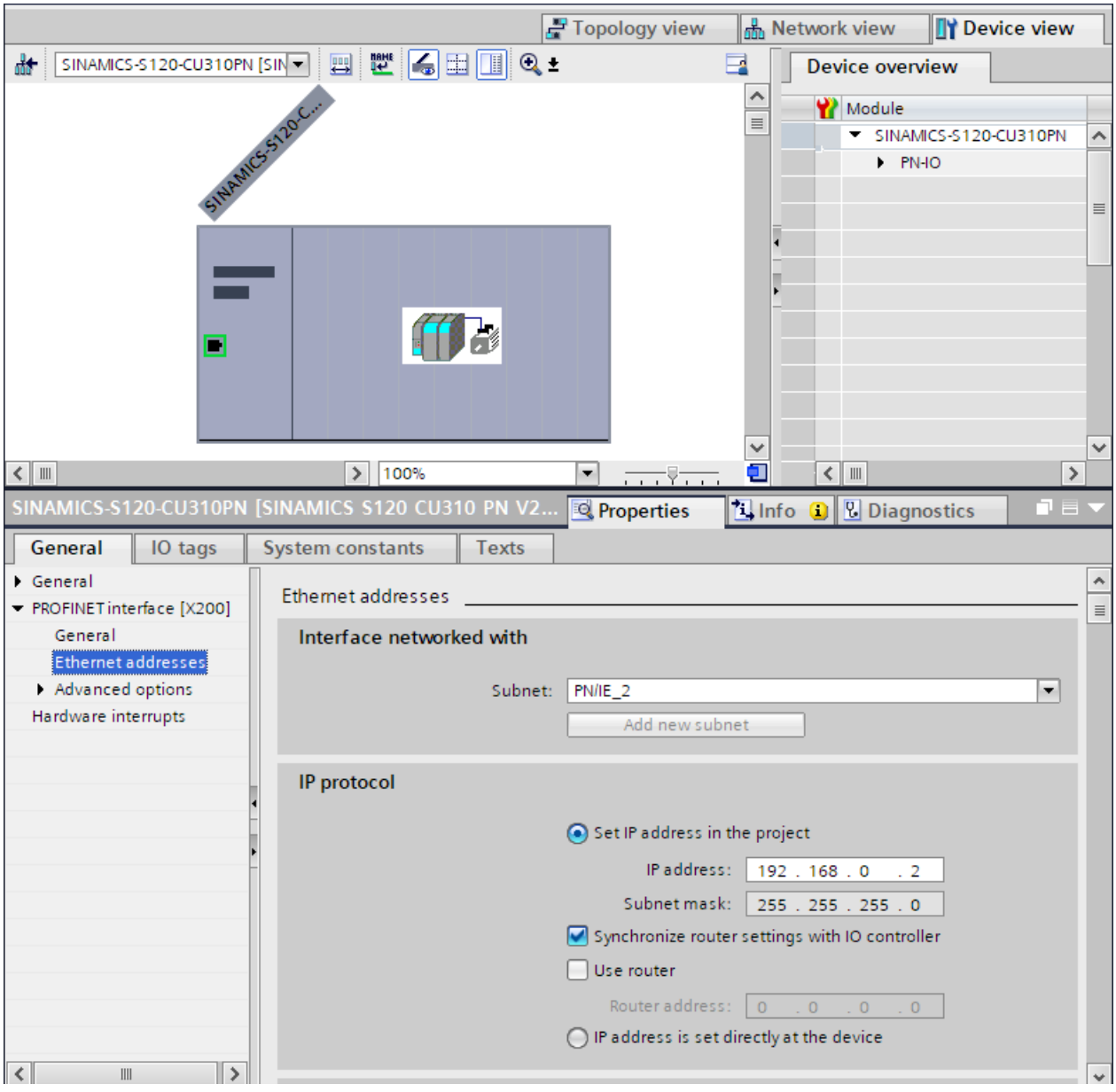
7.3.3 Configuring network settings for the drive

Preconditions

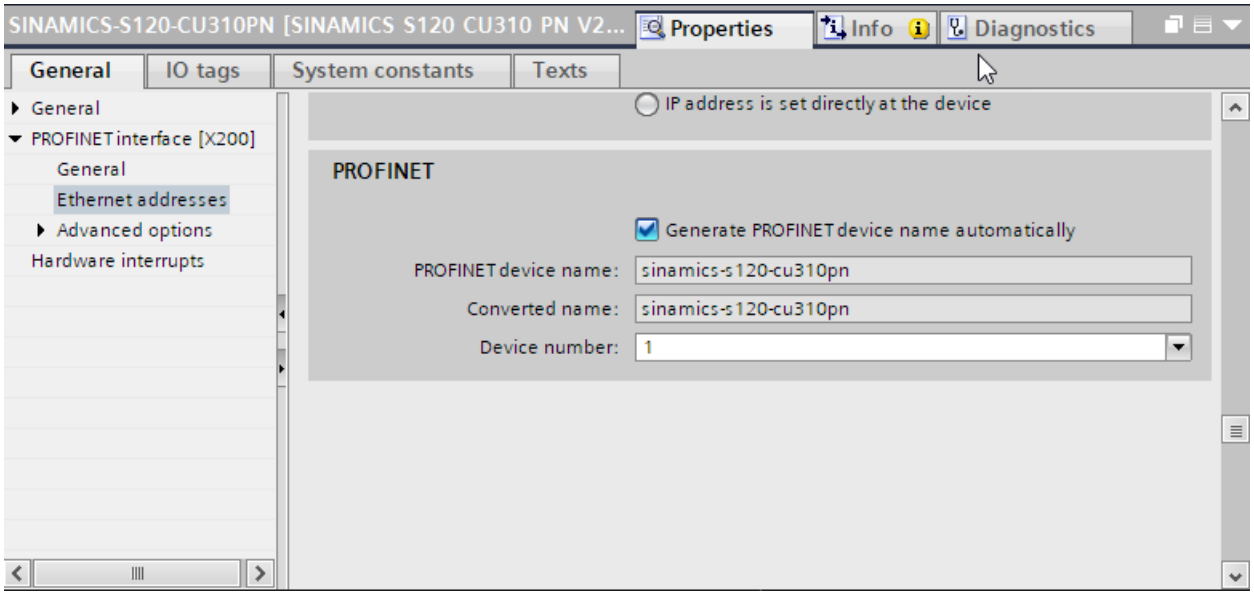
- The TIA Portal has been started.
- A SINUMERIK MCU has been inserted.
- The drive and control are interconnected.

Procedure

1. Under "Project navigation > Ungrouped devices", double-click the drive you created.
   The device configuration for the drive is displayed in the Inspector window.
2. In the Inspector window under "Properties > General > PROFINET interface [X150] > Ethernet addresses", in the "IP Protocol" screen section set the IP address of the drive.



3. In the "PROFINET" screen section, activate "Automatically generated PROFINET device name".



7.3.4 Configuring telegrams for communication

Introduction

You need a telegram for the communication between a control and a drive.

Any axis that you operate on the control must be created via the "DO SERVO" module from the hardware catalog.

For each axis, you also create one telegram.

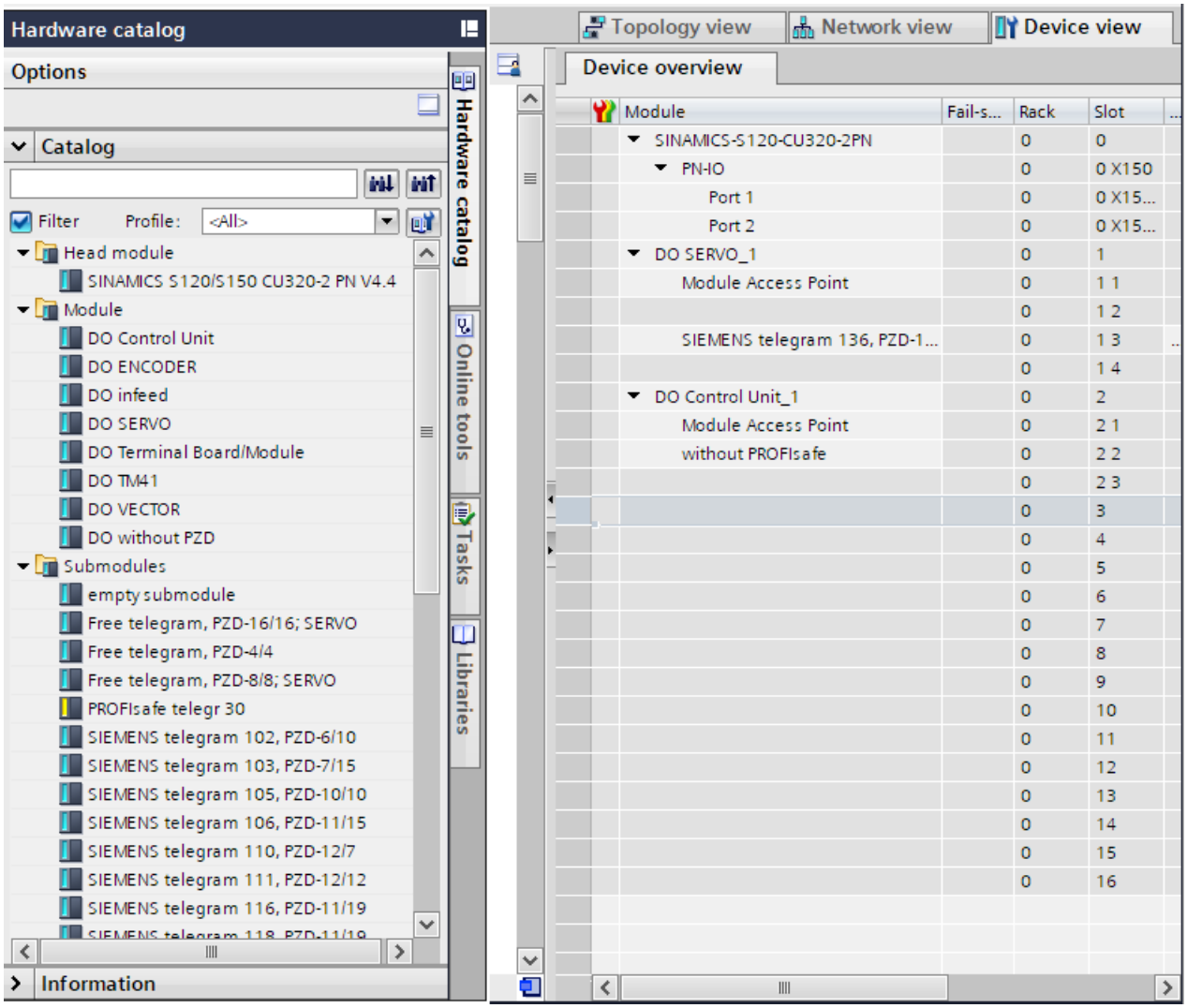
Preconditions

- The TIA Portal has been started.
- A SINUMERIK MCU has been inserted.
- The drive and control are interconnected.

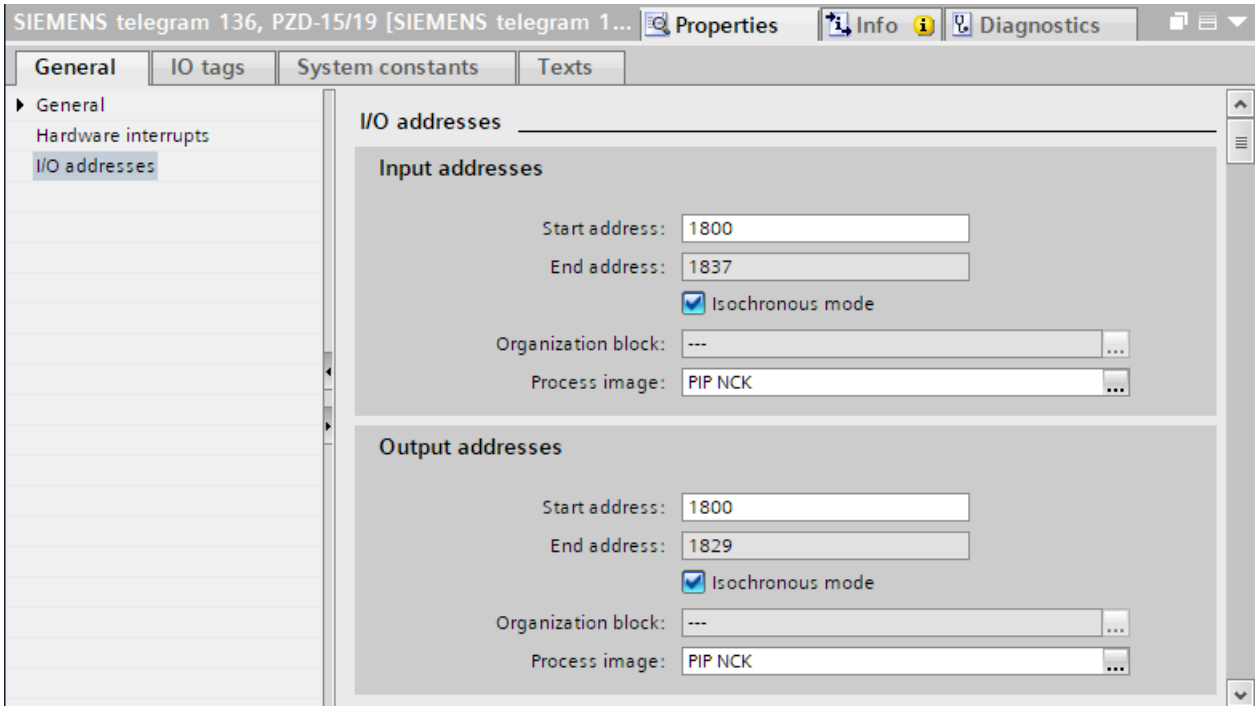
Procedure

To configure telegram communication for the drive, insert the relevant drive objects from the hardware catalog.

1. To display only those modules that are relevant to your configuration in the hardware catalog, select the "Filter" check box.
   The hardware catalog shows the drive objects that are available for this drive.
2. In the hardware catalog, select the following drive objects and drag them onto the device overview:
   - Under "Module", module "DO SERVO"
   - Under "Submodules", telegram "Siemens telegram 136, PZD-15/19"
   - Under "Module", module "DO control unit"
   - Under "Submodules", telegram "Siemens telegram 391, PZD-3/7"



3. In the device overview, select telegram "Siemens telegram 136, PZD-15/19".
   The telegram configuration is displayed in the Inspector window.
4. In the Inspector window under "Properties > General > I/O addresses", make the following settings for input addresses and output addresses:
   - In field "Initial address", enter the value "1800".
   - Select the "Isochronous operation" check box.
   - Under "Process image", select "PIP NCK".



Note

Control with several axes

If you operate several axes on the control, you must insert one telegram for every axis. To do this, first insert an axis delimiter in the "Device overview" of the drive for the second axis. Then drag a further telegram onto the "Device overview".

7.3.5 Completing the configuration

Introduction

To complete the configuration, make the following settings:

- Check and set the send cycle clock on the PLC to allow synchronization of PROFINET IO devices and improve the precision of the cyclic data exchange via PROFINET IO.
- Check and set isochronous operation, e.g. including the Ti/To times
- Check the sync domain, sync master, and sync slave
- Check the PROFINET port interconnection
- Supplement the drive with the other components required, e.g. Line Module, Power Module, Motor, encoder, etc.

Note

The send cycle clock is valid for all PROFINET devices on the IO system. If you set the synchronization role to a value other than "Unsynchronized", you can also set the send cycle clock in the sync domain, i.e. centrally on the PROFINET IO system.

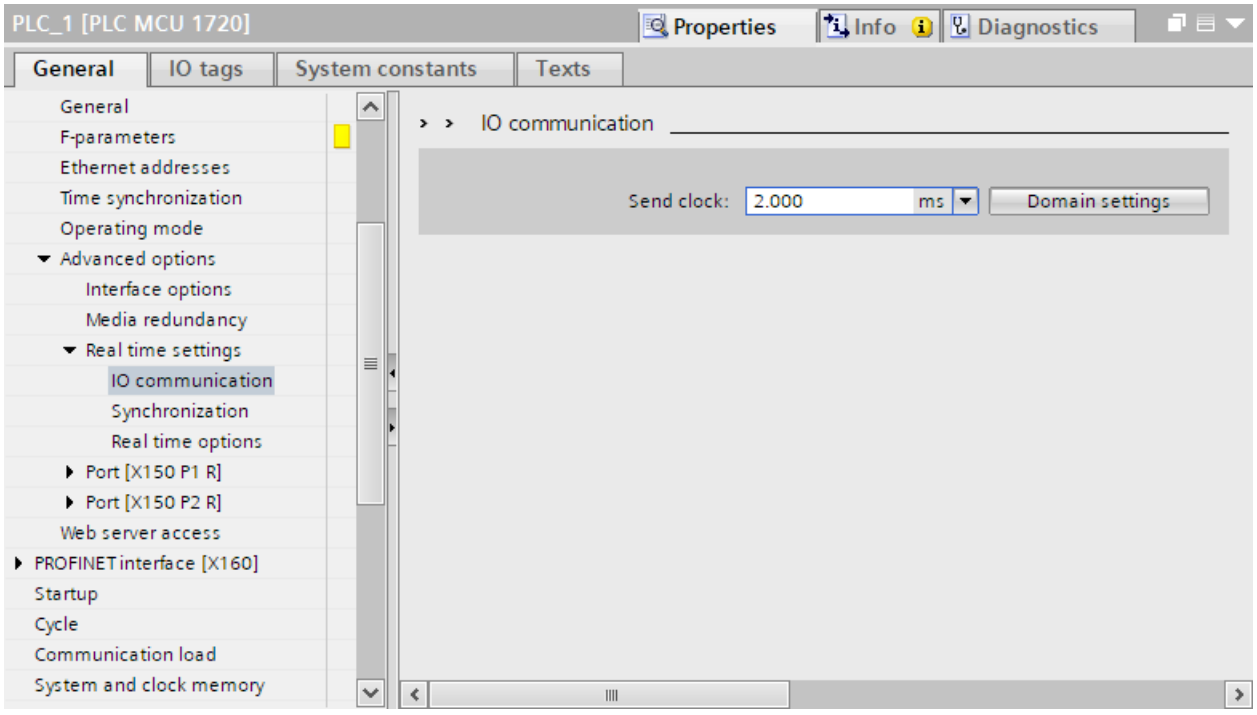
Preconditions

- The TIA Portal has been started.
- A SINUMERIK MCU has been inserted.
- The drive and control are interconnected.
- Axes and telegrams have been created.

Setting the send cycle clock on the PLC

Proceed as follows to set the send cycle clock on the PLC:

1. In the network view, click the PLC in the basic rack of the SINUMERIK MCU.
2. Switch to Inspector window "Properties > General > PROFINET interface [X150] > Extended options > Real-time settings > I/O communication > Send clock".
3. Set the required send cycle clock.



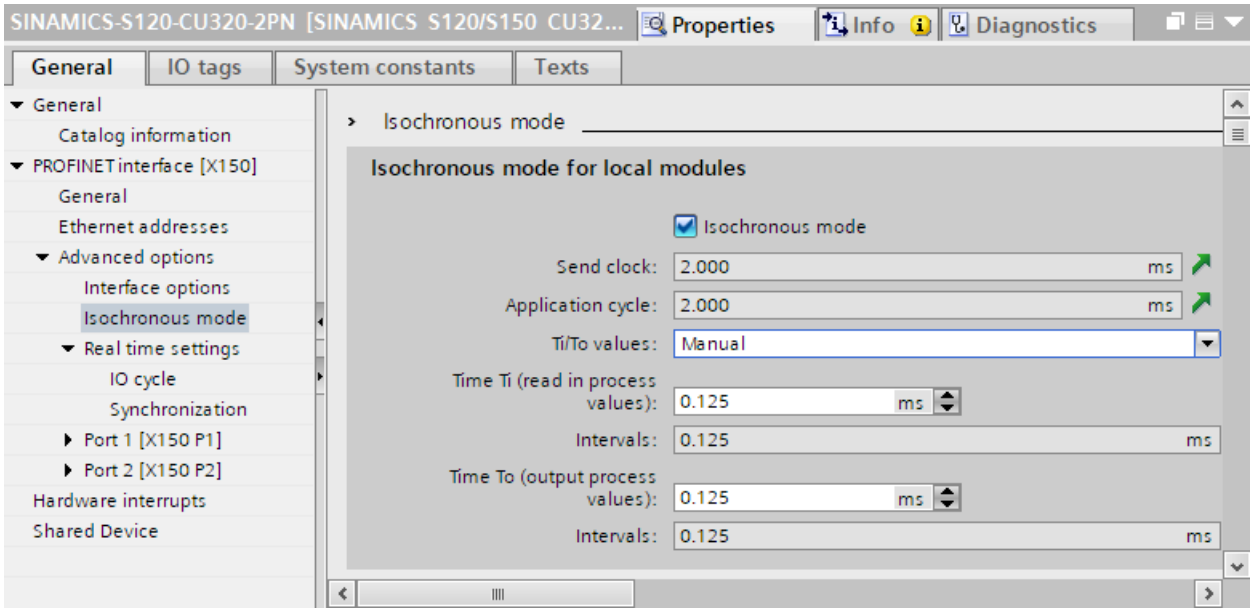
Checking the settings for isochronous operation

The drive and control together form a sync domain. For motion control applications of the PROFINET IO system, you must parameterize the IRT operating mode (for isochronous drives) and the PROFINET settings. Isochronous mode of the application with the bus is only possible with PROFINET IO with IRT. In the case of PROFINET IO with IRT, a sync master generates a synchronization telegram to which all sync slaves synchronize themselves. To use isochronous mode, you must configure it for the IO device.

As default, "Automatic" mode is set for the drive to calculate the Ti/To values. When "Automatic" is activated, STEP 7 calculates a Ti value and a To value that is suitable for all modules that are operated isochronously and assigned to the OB.

To change the calculation mode for the Ti/To values, proceed as follows:

1. Under "Project navigation > Ungrouped devices", double-click the drive you created. The device configuration for the drive is displayed in the Inspector window.
2. In the Inspector window, under "Properties > General > PROFINET interface [X150] > Extended options > Isochronous mode", under "Manual" mode select "Ti/To values".



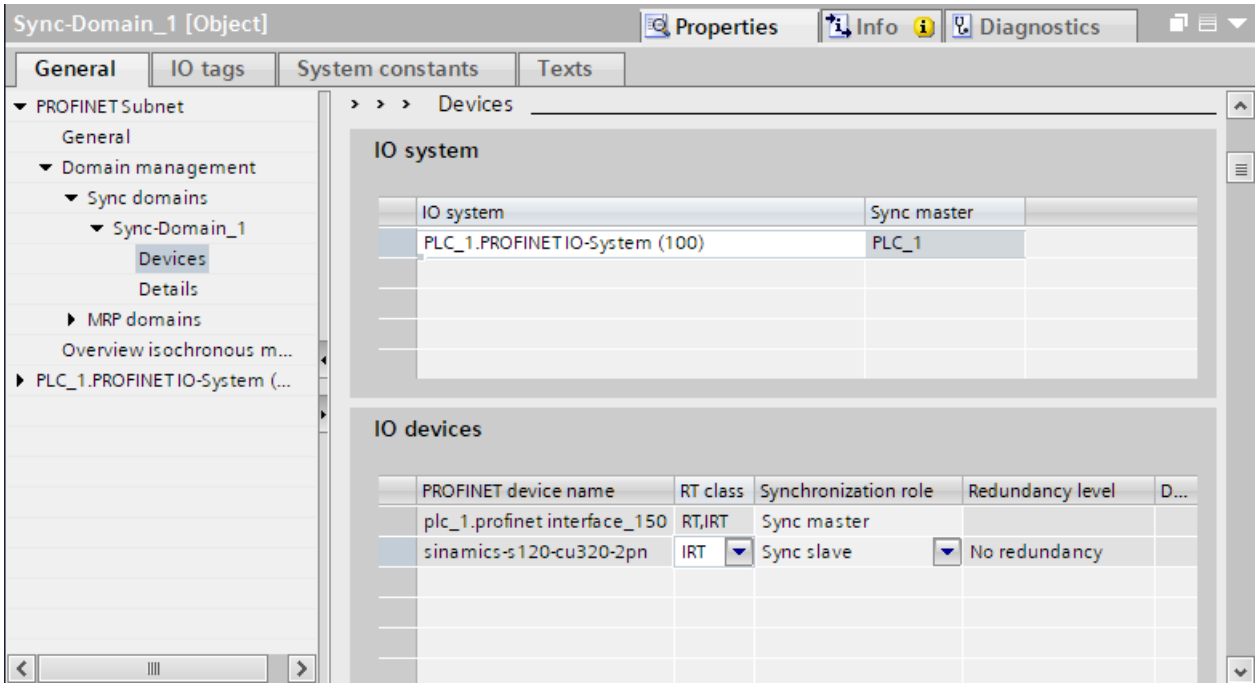
You can edit the Ti/To values in "Manual" mode.

Checking settings for the sync domain

A sync domain is needed to synchronize PROFINET IO devices. To check the assignment of the device to the sync master and sync slave and other sync domain settings, proceed as follows:

1. Switch to the network view.
2. Select the PN/IE connection between the control and the drive.
   The connection settings are displayed in the Inspector window.

3. Under "General", click "PROFINET Subnet > Domain management > Sync domains > Sync-Domain_1".
4. Check the settings, in particular, the assignment of the devices in the "IO devices" section, and complete where necessary.



Check the PROFINET port interconnection

In the topology view, you see an overview of all ports in the project and can interconnect them centrally.

To edit the properties of the port interconnection, proceed as follows:

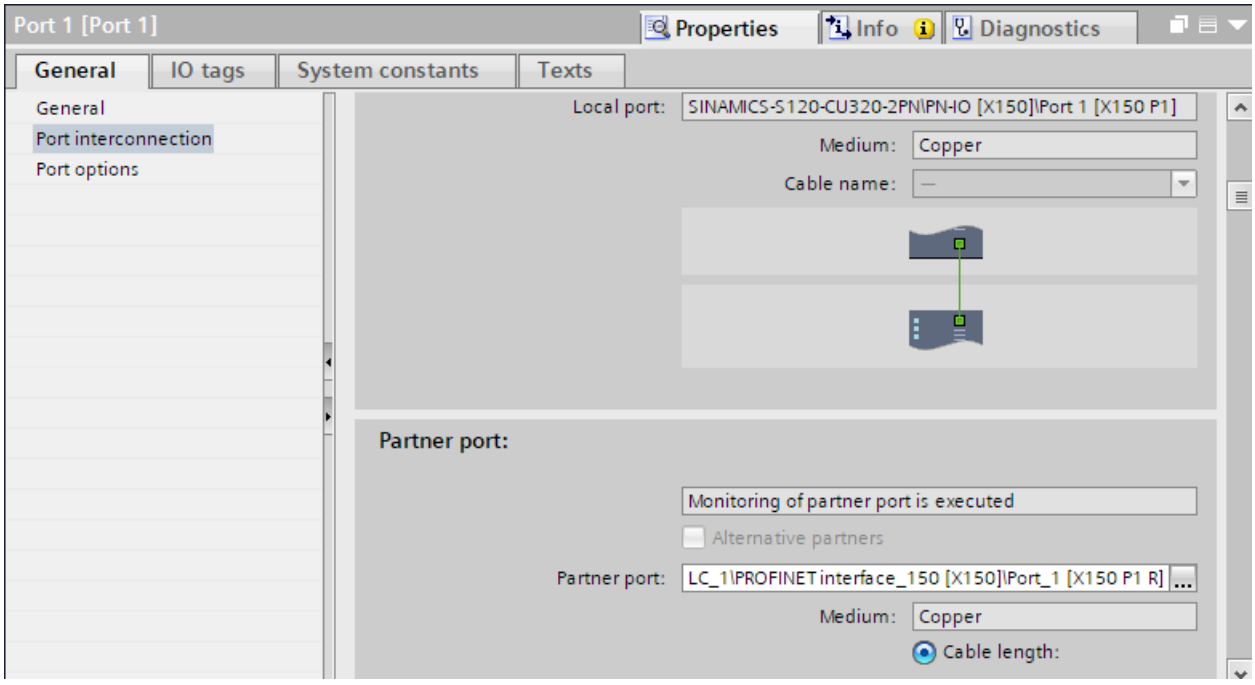
1. Switch to the topology view.

   Note

   If you hover the mouse over the ports, port names are displayed in the tooltip.

2. Select the port with which the drive is connected to the control.
   The port settings are displayed in the Inspector window.

3. Check the settings for the port interconnection.



4. If necessary, edit the other parameters of the port.

7.4 Assigning the basic parameters in SINUMERIK ONE Commissioning

7.4.1 Overview of NC and drive communication

After basic commissioning in "SINAMICS Startdrive" in the TIA Portal, you must make the following settings in SINUMERIK ONE Commissioning to allow communication between the drive and the NC:

- Assign the general machine data (relevant for communication via PROFINET with the drive)
- Assign the axis machine data (relevant for transferring setpoint and actual values)
- Assign the axes
- Assign the components to the drive objects (e.g. assignment of the Motor Modules, motors and encoders and their assignment to the NC machine axes)

When you commission an S120 drive system, SINUMERIK ONE Commissioning supports you with device configuration, assignment of the components to the drive objects and axis assignment.

On an S210 drive system, you must perform manual parameter assignment in SINUMERIK ONE Commissioning.

Note

The configuration in SINUMERIK ONE Commissioning must match that of the configuration in the TIA Portal.

7.4.2 Assignment of the machine data

Some of the machine data settings that you make in the SINUMERIK ONE Commissioning tool differ in the S120 and S210 drive systems.

While the S120 drive system is recognized in SINUMERIK ONE Commissioning under Drive system, and you can automatically read out and display the hardware configuration, for the S210 drive system you must make all of the settings manually.

Assignment of S210/S120 general machine data

The following table lists the general machine data for the S210 and S120 drive systems that you must configure accordingly in SINUMERIK ONE Commissioning:

Number	Designation	Value	Meaning
MD13050	$MN_DRIVE_LOGIC_ADDRESS	• = 4100 (S210) • According to the start address of the inputs/outputs of the drive object / servo telegram on the CU320-2 PN drive.	Telegram address[1)] Cyclic communication The start address of the input and output must be identical with S120.
MD13060	$MN_DRIVE_TELEGRAM_TYPE	• = 105 (S210) • According to telegram configuration (S120)	Telegram type
MD13070	$MN_DRIVE_FUNCTION_MASK	• = FH (S210) • = 2H (S120)	Access to drive parameters
MD13080	$MN_DRIVE_TYPE_DP	• = 1 (synchronous) • = 2 (asynchronous) • = 0 (not defined)	Drive type
MD13120[0]	$MN_CONTROL_UNIT_LOGIC_ADDRESS	= 0	Telegram address
MD30130	$MA_CTRLOUT_TYPE	= 1	Output type setpoint
MD30240	[0] $MA_ENC_TYPE	• = 4 (absolute) • = 1 (incremental)	Acquisition of actual value

[1)] If you set the address in SINUMERIK ONE Commissioning and subsequently change it again in the TIA Portal, you must reload the changed configuration into the drive.

Assignment of the S210/S120 axis machine data

The following table lists axis machine data and parameters for spindle/axis interpolation for the S210 and S120 drive systems that you must configure in SINUMERIK ONE Commissioning depending on the axis type:

Number	Designation	Value	Meaning
MD30300	$MA_IS_ROT_AX	Dependent on task type • = 0 (linear) • = 1 (rotary)	Rotary axis/spindle (axis: rotary/linear)
MD30310	$MA_ROT_IS_MODULO	= 1	Modulo conversion for rotary axis / spindle
MD30320	$MA_DISPLAY_IS_MODULO	= 1	360-degree modulo display for rotary axis or spindle
MD32000	$MA_MAX_AX_VELO	= 8000	Maximum axis velocity
MD31020	$MA_ENC_RESOL	Dependent on the encoder	Encoder pulses / rev.
MD31025	$MA_ENC_PULSE_MULT[n]	Dependent on the encoder type	Encoder multiplication/ Multiturn resolution

Number	Designation	Value	Meaning
MD32250	$MA_RATED_OUTVAL	100 %[1]	Rated output voltage; The rated output voltage must be adapted to the rated speed of the analog drive:
MD32260	$MA_RATED_VELO	According to the real rated motor speed[2]	Rated motor speed
MD30220[0..1]	$MA_ENC_MODULE_NR	According to the index (n) of MD13050: x = n + 1[3]	Actual value assignment: Drive number/measuring circuit number
MD34200[0]	$MA_ENC_REFP_MODE	• 0 (reference point approach not possible) • 1 (referencing of incremental, rotary, or linear measuring systems: zero pulse on the encoder track)	Referencing methods

[1] 100 % setpoint output corresponds to the rated speed of the motor

[2] In the drive, for p2000 the maximum motor speed is entered as a reference speed. In SINUMERIK ONE Commissioning for linear axes with synchronous motor, it is recommended that rated speed p0311 is entered as reference speed p2000.

[3] The logical I/O address of the drive is assigned from MD13050 $MN_DRIVE_LOGIC_ADDRESS[n] using the drive number.

Further information on telegram configuration of the drive system is provided in Chapter "Overview of telegram configuration (Page 139)".

NC commissioning

8

8.1 Machine and setting data

Setting machine data

Adaptation of the control at the machine is performed using the machine and setting data.

- The machine data (MD) is divided into the following areas:
  - General machine data
  - Channel-specific machine data
  - Axis-specific machine data
  - Parameters for the Control Unit
  - Parameter for the infeed
  - Drive parameters
- The setting data (SD) is divided into the following areas:
  - General setting data
  - Channel-specific setting data
  - Axis-specific setting data

The following table provides an overview of the machine data and setting data areas:

Range	Designation
from 9000 to 9999	Display machine data
from 10000 to 18999	General NC machine data
from 19000 to 19999	Reserved
from 20000 to 28999	Channel-specific machine data
from 29000 to 29999	Reserved
from 30000 to 38999	Axis-specific machine data
from 39000 to 39999	Reserved
from 41000 to 41999	General setting data
from 42000 to 42999	Channel-specific setting data
from 43000 to 43999	Axis-specific setting data
from 51000 to 51299	General configuration machine data
from 51300 to 51999	General cycle machine data
from 52000 to 52299	Channel-specific configuration machine data
from 52300 to 52999	Channel-specific cycle machine data
from 53000 to 53299	Axis-specific configuration machine data
from 53300 to 53999	Axis-specific cycle machine data

The SINUMERIK Operate **Online Help** provides a context-related description of the machine data and setting data.

Effectiveness

The effectiveness of a machine data item specifies when the change becomes active:

po	The changed machine data require an "NCK Reset" to become effective.
re	The changed machine data must be activated by pressing the <RESET> key.
cf	The changed machine data must be activated by pressing the "Apply MD" softkey.
so	The changed machine data becomes active immediately.

Changes to the setting data always take effect **immediately**.

Further information

A description of the machine data and setting data is provided in the

SINUMERIK MC Machine Data List Manual

8.2 Procedure when commissioning the NC

NC commissioning

We recommend the following sequence when commissioning the NC:

Sequence		Reference
①	Parameter sets of axis/spindle	Function Manual Axes and Spindles: • Velocities, setpoint/actual value systems, closed-loop control • Spindles
②	Axis configuration	Function Manual Basic Functions: • Axes, coordinate systems, frames Function Manual Axes and Spindles: • Synchronous spindle • Rotary axes Function Manual Monitoring and Offsets: • Compensations
③	Parameterizing axis data: • Parameterizing the incremental-rotary measuring system • Parameterizing the incremental-linear measuring system • Parameterizing the absolute measuring system • Setpoint/actual value channels • Dynamic Stiffness Control (DSC) • Rotary axes • Positioning axes • Position controller • Speed setpoint matching • Axis velocity matching • Axis monitoring functions (static) • Axis monitoring functions (dynamic)	Function Manual Axes and Spindles: • Velocities, setpoint/actual value systems, closed-loop control • Rotary axes • Positioning axes Function Manual Monitoring and Offsets: • Axis monitoring functions
④	Parameterizing the spindle data: • Setpoint/actual value channels • Measuring systems • Gear stages • Velocities and setpoint adaptation • Spindle positioning • Spindle synchronization • Monitoring	Function Manual Axes and Spindles: • Spindles • Velocities, setpoint/actual value systems, closed-loop control
⑤	Referencing axis/spindle: • Incremental measuring system • Distance-coded reference marks • Absolute encoder referencing	Function Manual Axes and Spindles: • Referencing

Setting the technology

User views are lists of machine data and setting data that are compiled for a special application. In order to set all the technology-relevant data for a turning machine or milling machine on the control, the following user views are available to facilitate the commissioning:

- Setup_Milling
- Setup_Turning

The files are stored on the SD card under:

/user/sinumerik/hmi/template/user_views/param

Product announcement (https://support.industry.siemens.com/cs/document/80582059)

8.3 Configuring machine axes

8.3.1 Axis assignment

Introduction

Generally, a distinction is made between four types of axes:

- **Machine axes**
  Machine axes are the motion units existing on a machine, which can also be designated as linear or rotary axes, depending on their usable movement.
- **Channel axes**
  The total of all machine, geometry and special axes assigned to a channel is designated as channel axes. In this context, the geometry and special axes constitute the program-technological part of the machining process, i.e. they are used for programming in the parts program. The machine axes constitute the physical part of the machining process, i.e. they carry out the programmed traversing movements on the machine.
- **Geometry axes**
  The geometry axes constitute the rectangular Cartesian basic coordinate system of a channel. Generally, (Cartesian arrangement of the machine axes) direct imaging of the geometry axes to the machine axes is possible. If the arrangement of the machine axes, however, is not Cartesian at right angles, the imaging is performed using a kinematic transformation.
- **Special axes**
  Special axes are all other channel axes that are not geometry axes. Unlike for geometry axes (Cartesian coordinate system), no geometric context is defined for special axes, neither between additional axes nor with respect to geometry axes.

Note

Geometry and special axes

A maximum of three channel axes can be declared as geometry axes. The geometry axes must be assigned to the channel axes in ascending order without any gaps. All channel axes that are not geometry axes are special axes.

Axis assignment

The assignment of geometry axes to channel axes and channel axes to machine axes, as well as the definition of the names of the different axis types is realized via machine data. The following diagram illustrates this relationship:

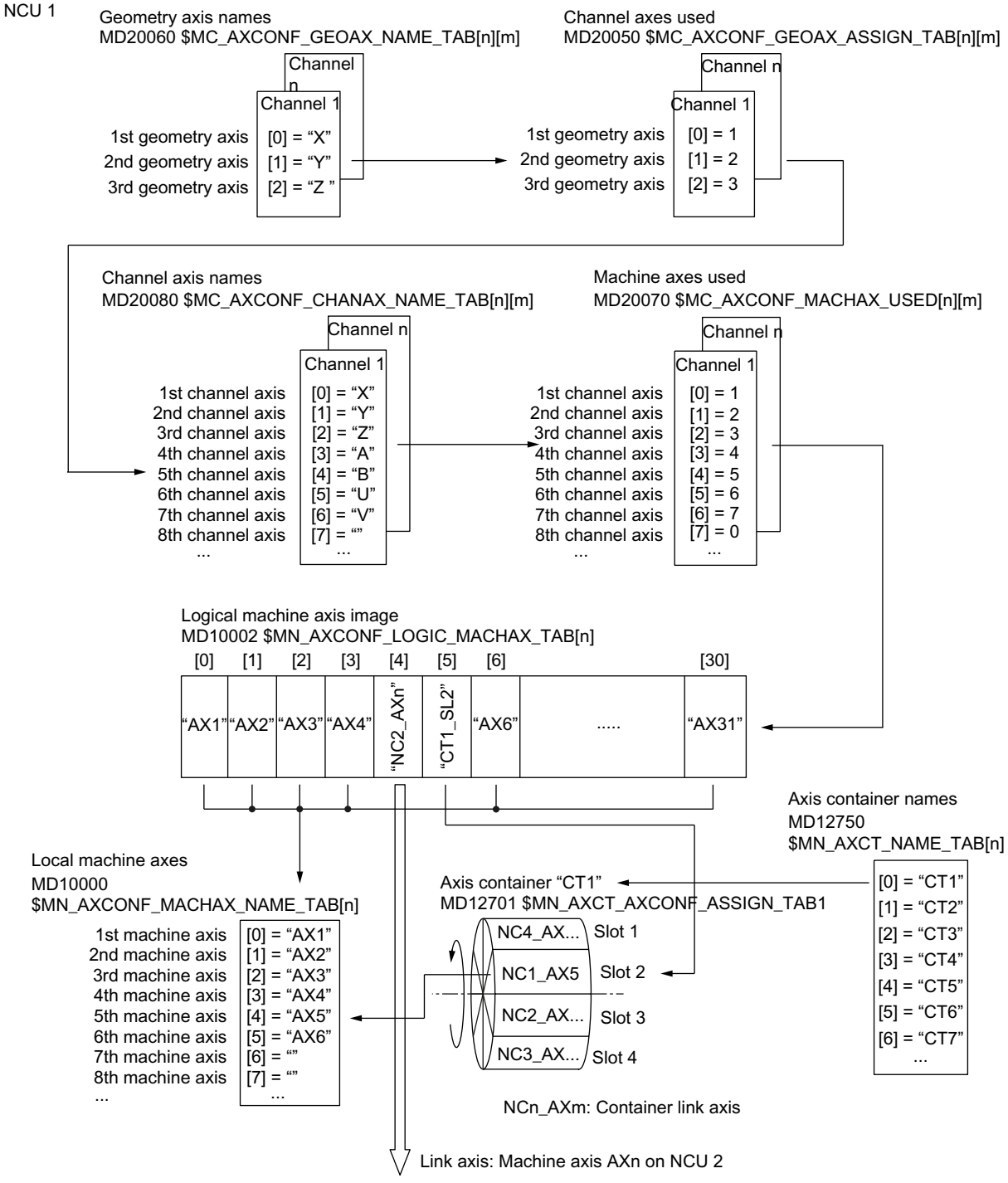


Figure 8-1 Axis assignment

Channel axis gaps

Normally, using MD20070, a channel axis is assigned to one machine axis. Not every channel axis must be assigned to a machine axis. Each channel axis with MD20070 [n] = 0 is not assigned any machine axis and represents a channel axis gap.

Channel axis gaps allow the creation of a uniform configuration of the channel axes over different machine versions of a series. Each channel axis of the series has a defined task or function. If the function and therefore the machine axis is not available on a specific machine, the relevant channel axis is not assigned a machine axis:

MD20070 $MC_AXCONF_MACHAX_USED[<channel axis>] = 0

Advantages:

- Commissioning archive with uniform basic configuration
- Simple post configuration for the specific machine
- Flexible portability of part programs

Enabling channel axis gaps

The use of channel axis gaps is enabled using the machine data:

MD11640 $MN_ENABLE_CHAN_AX_GAP = 1 (channel axis gap allowed).

If the use of channel axis gaps has not been enabled, then the value 0 for channel axis n in the following machine data terminates the allocation of additional machine axes to possible channel axes from channel axis n onwards:

MD20070 $MC_AXCONF_MACHAX_USED[<channel axis n>]

Supplementary conditions:

- Regarding the number of channel axes and the indexing, a channel axis gap counts just the same as axes.
- Ensure that a geometry axis is not assigned to a channel axis, that is not assigned to a machine axis (channel axis gap). **No** alarm is displayed.
- Transformation: When configuring a channel axis in the following machine data, which is not assigned a machine axis (channel axis gap), an alarm is output:
  - MD24110 ff. $MC_TRAFO_AXES_IN1...8
  - MD24120 ff. $MC_TRAFO_GEOAX_ASSIGN_TAB1...8

Example

The 5th channel axis "B" in MD20070 is not assigned to a machine axis.

If channel axis gaps are enabled, six machine axes (1 - 4, 5, 6) are available.

If channel axis gaps are not enabled, then there are four machine axes (1 - 4) available.

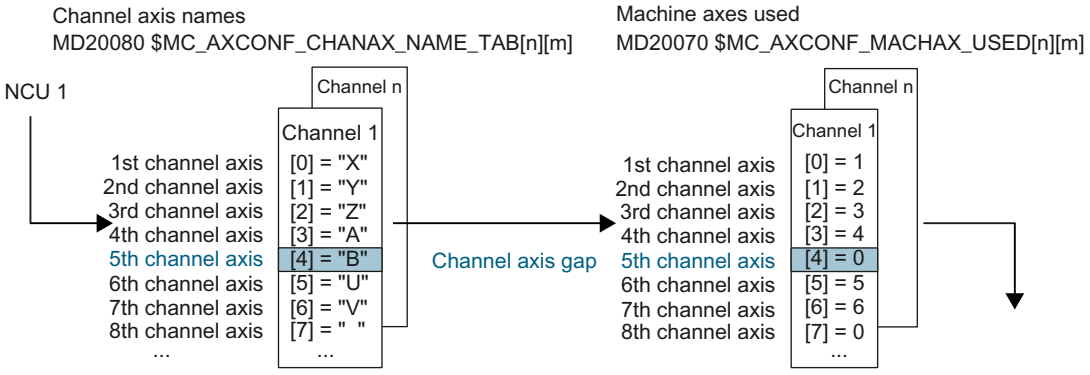


Figure 8-2 Axis configuration with channel axis gap

8.3.2 Axis names

Machine axes

Each machine axis, channel axis and geometry axis is assigned an individual name that clearly identifies the axis. Machine axis names must be unambiguous for the entire NC. The name of the machine axes are defined via the following machine date:

MD10000 $MN_AXCONF_MACHAX_NAME_TAB [n] (machine axis name)

The specified names and the associated index are used in the following cases:

- Accessing axis-specific machine data (loading, saving, displaying)
- Reference point approach from the parts program G74
- Measuring
- Test point traversing from the parts program G75
- Traversing the machine axis from the PLC
- Display of axis-specific alarms
- Display in the actual-value system (machine-related)
- DRF handwheel function

Channel axes

The name of the channel axes are defined via the following machine date:

MD20080 $MC_AXCONF_CHANAX_NAME_TAB[n] (name of the channel axis in the channel)

Channel axis names must be unambiguous for the entire channel.

Geometry axes

The names of the geometry axes must be absolutely unique throughout the channel, and are defined using the following machine data:

MD20060 $MC_AXCONF_GEOAX_NAME_TAB [n] (geometry axis in the channel)

The names for channel and geometry axes are used in the part program for programming general traversing movements and to describe the workpiece contour.

- Path axes
- Synchronized axes
- Positioning axes
- Command axes
- Spindles
- Gantry axes
- Coupled axes
- Guide value coupling axes

8.3.3 Drive assignment

Drive assignment

The assignment of machine axes to the SERVO drive objects is realized using machine data.

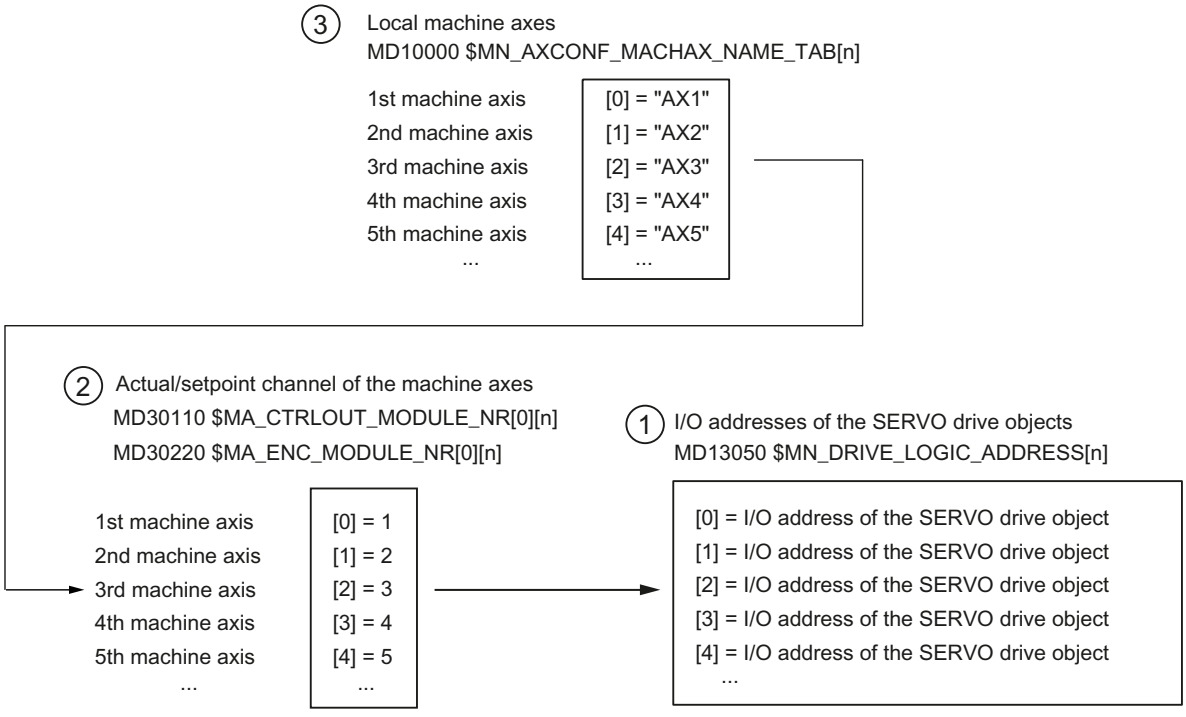


Figure 8-3 Drive assignment

Assignment:

1. Using this machine data, the NC is informed about the I/O addresses of the SERVO drive objects defined in the PLC project:
   MD13050 $MN_DRIVE_LOGIC_ADDRESS[n]
2. Using the following machine data, the setpoint and actual values of the machine axes are assigned to the relevant drive objects:
   – MD30110 $MA_CTRLOUT_MODULE_NR[0]
   – MD30220 $MA_ENC_MODULE_NR[0]

   The logical drive number **m** to be entered into both machine data, refers to the I/O address entered in ① under index n = (**m** - 1).
3. Using machine data MD10000 $MN_AXCONF_MACHAX_NAME_TAB, the machine axes in the NC are assigned a unique name. Index n addresses machine axis (n+1).

8.4 Configuring drive units with SINUMERIK ONE Commissioning

PROFINET connection

The following general machine data are also set by default for the PROFINET connection of the axes to the drive:

- MD13050 $MN_DRIVE_LOGIC_ADDRESS (axis address)
- MD13060 $MN_DRIVE_TELEGRAM_TYPE (telegram type)
- MD13120 $MN_CONTROL_UNIT_LOGIC_ADDRESS (CU address)

The connection of the axes to the drive via PROFINET is displayed in the operating area "Commissioning > Drive system > Drive units > PROFINET".

Example for the connection of relevant axis to the drive:

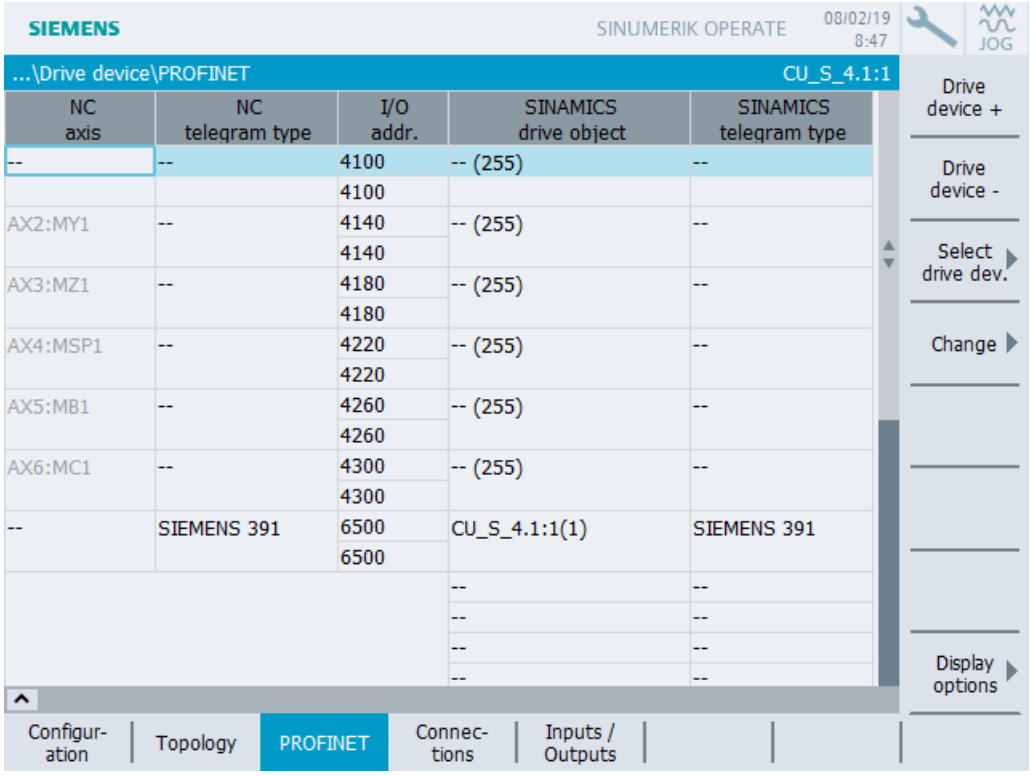


Figure 8-4 Drive units - PROFINET

To change the assignment, press the "Change >" softkey. Then use the arrow softkeys for the new assignment:

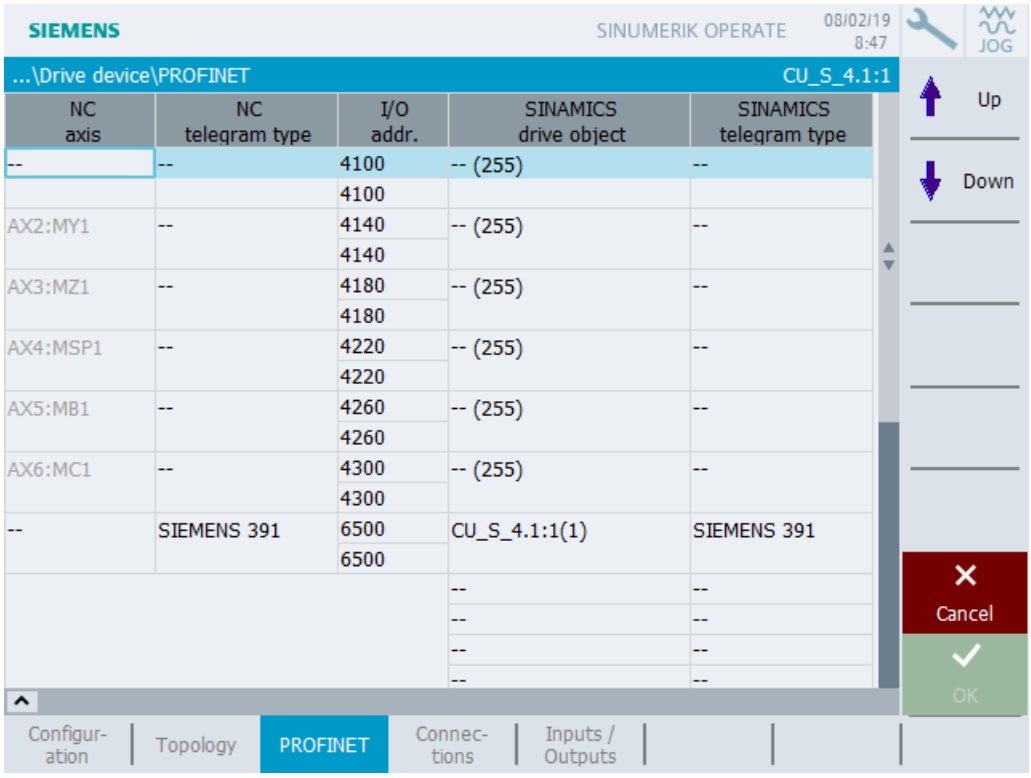


Figure 8-5 Change assignment

Note

Communication with the drive

To ensure communication with the drive, the I/O addresses and telegram types set here must match the settings in the hardware configuration in the SINUMERIK MC STEP 7 Toolbox.

8.5 Configuring the measuring probe

8.5.1 Measuring probe general

Measuring for S120 and S210

SINAMICS S120 and S210 drives are connected to SINUMERIK MC via PROFINET IO. This means that for both drives only distributed measuring is possible:

- Central measuring for SINAMICS S120 CU320-2:
  For the S120, measuring probes 1 and 2 (X122 oder X132) are connected via terminals to the CU. While parameterizing the drive, the measuring probe inputs are assigned to an axis. Use SINUMERIK Commissioning to perform this operation.
- Distributed measuring for SINAMICS S210
  For S210, the measuring probes are connected to the digital inputs.
  Measured values are transferred from the drive to the control system using a PROFIdrive telegram (e.g. telegram 105).

Setting the measurement type

You set the measurement type at each axis using machine data MD13210 MEAS_TYPE and MD30244 ENC_MEAS_TYPE.

8.5.2 Distributed measuring probe with S210

Connecting signals at the drive

For SINAMICS S210, the measuring probe must be connected to each axis (drive device). As a consequence, for three geometry axes and a spindle, the wiring at the devices must be routed from drive to drive.

SINAMICS S210 measuring probe

For SINAMICS S210, the measuring probes are directly connected to the digital inputs. You have already created a SINUMERIK MC and a SINAMICS S210 in the TIA Portal and configured the communication. The configuration is performed using Startdrive (TIA Portal) or directly via the web server at the SINAMICS S210

1. Open the S210 entry in Startdrive.
2. Select "Parameterization" and in the secondary navigation click on "Digital inputs" in the foreground.

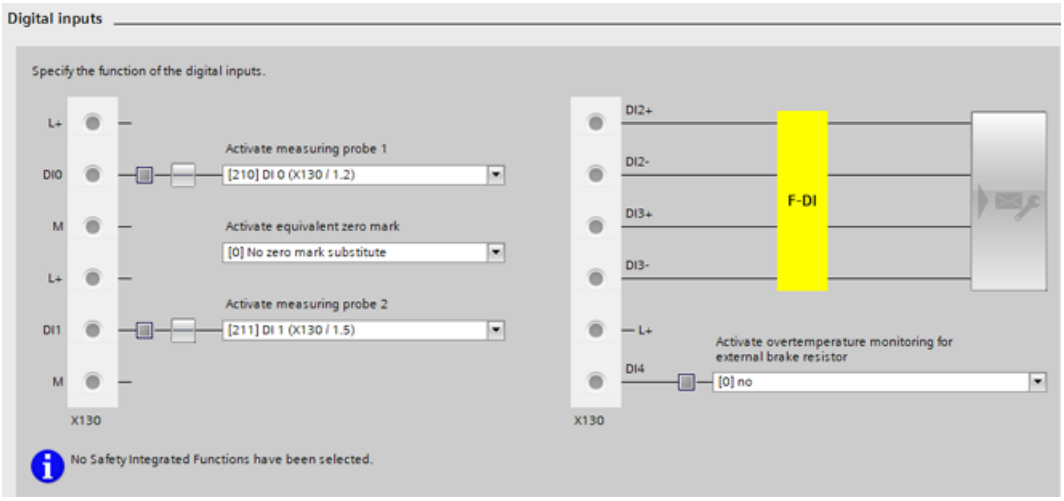


Figure 8-6 S210 digital inputs

Measuring probe 1 and measuring probe 2 have already been parameterized.

Telegram 105

Telegram 105 is preset as default setting for communication between a SINAMICS S210 drive and SINUMERIK MC.

Probe in SINUMERIK ONE Commissioning

In SINUMERIK ONE Commissioning, proceed as follows to be able to use the measuring probe decentrally:

General MD, which is used to set the measuring function for distributed drives.

MD13210 $MN_MEAS_TYPE	Measuring type for distributed drives
= 1 (default 0)	The measuring probe must be decentrally connected at ALL drives. The measuring functionality of the drive is then used. The encoder actual values in the hardware are then saved at the instant of the measurement signal edge.

Axis MD, which is used to set the axis-specific measuring function for drives.

MD30244 $MA_ENC_MEAS_TYPE[n]	Encoder measuring type
= 1	Encoder measuring type distributed (local) measuring

8.5.3 Central measuring probe with S120

Connecting signals at the drive

For SINAMICS S120, measuring probes are connected at terminals X122 or X132 of the Control Unit

Measuring probe connected to SINAMICS S120

For SINAMICS 120, measuring probes are connected at the bidirectional inputs/outputs of X122 or X132. The terminals must be parameterized as measuring probe input using p680. Depending on how many measuring probes are used, PROFIdrive telegrams 391 ... 396 of the CU can be used.

Configuring is performed using Startdrive (TIA Portal) or another commissioning tool.

Probe in SINUMERIK ONE Commissioning

In SINUMERIK ONE Commissioning, proceed as follows to be able to use the measuring probe centrally:

General MD, which is used to set the measuring function for central drives.

MD13210 $MN_MEAS_TYPE	Measuring type for drives
= 0 (default 0)	The measuring probe is centrally connected to the CU of the drive.

Axis MD, which is used to set the axis-specific measuring function for drives.

MD30244 $MA_ENC_MEAS_TYPE[n]	Encoder measuring type
= 0	Encoder measuring type central measuring

Creating and importing archives using SINUMERIK ONE Commissioning

9

9.1 Overview for archiving and data backup

On the one hand, commissioning archives are used to save a specific control status and to restore it (Backup), on the other hand, they allow you to configure a machine series using the same data (Setup). In SINUMERIK MC, these two archive types are supported with the DSF format (Data Storage Folder).

Further, NC data, PLC data, drives and programs can be saved separately or together in archive files, and imported again from there. When selecting, any combinations are possible. The files can be reimported independently of each other and with maximum flexibility.

In contrast to the backup, no specific machine data are considered during a setup. A detailed list of contents of the archive types is included in the table in the section "Data areas".

With the "User" access level, you can read in a backup file only on the control system on which the archive was created. The "Manufacturer" access level is required to read in a backup file on another control. The "Manufacturer" access level is always required to read in a setup file. You can find an overview in the section "Archiving options".

Note

Restriction

Only components NC, PLC, drives and local data can be backed up via commissioning archives in SINUMERIK MC.

Time of the data backup

The following times are recommended for performing a data backup:

- After completion of a prototype machine, to create a commissioning archive for a machine series
- After a commissioning
- After changing machine-specific settings
- After the replacement of a hardware component
- Before a software upgrade
- Before activating memory-configuring machine data (only for inactive NC function Automatic Memory Reconfiguration (AMR))
- After migrating ARC archives as new backup in the *.dsf format

Note

The DSF archive is compressed as a zip file, which contains a file tree with user data and attributes.

Archive options

There are various ways of creating and reloading archives via the SINUMERIK ONE Commissioning Tool user interface.

- **Data archive:** As usual, data can be selected specifically in the data tree and backed up by pressing the "System data" softkey.

  Note

  A data archive is saved in the *.arc format.

- **Commissioning archive**: The following selection is offered with the "Commissioning archive" softkey:
  - Create and import the data backup of all data of the machine (Backup)
    The "User" access level is required (for backup of the same control system).
  - Creating and importing data for a machine series (without specific machine data) (Setup)
    Access level "Manufacturer" is required.
  - Create and import the archive for the machine factory setting (Original)
    Access level "Manufacturer" is required.

  Note

  If you transfer the commissioning archives to another system, the "Manufacturer" access level is required to read in the data.

  Note

  A commissioning archive is saved in the *.dsf format.

  Archive files can be imported in the *.dsf and *.arc formats.

Storage locations

The following directories are available in the operating area "Commissioning (start-up) > System data":

- Archives > User
  or
  Archives > Manufacturer
- All configured logical drives (USB, network drives)

Note

Logs for the last import can be found in the following directory in the *.log format:

HMI data > Logs > Commissioning

Data areas

The following data areas are backed up in a commissioning archive:

Components	Data	Backup	Setup [2]	Setup [2] adapted
NC data [1]	Meta information	●	●	●
	Option data	●	●	●
	Machine data	●	●	●
	Global user data (GUD)	●	●	●
	Definitions and macros	●	●	●
	Frame data	●	●	●
	Kinematic data	●	●	●
	Working and protection area data	●	●	●
	Compensation data • QEC - quadrant error compensation • CEC - operation/angularity compensation • EEC - leadscrew pitch / encoder error compensation **Note:** It only makes sense to archive machine-specific compensation data if the series commisioning file is reloaded into the same control.	●		○
	Axis optimization data (AST)	●		○
	Tool and magazine data	●	●	●
	Setting data	●	●	●
	R parameters	●		○
	Synchronized action data	●	●	●
	System variables	●	●	●
	Standard cycles	●		○
	OEM cycles	●	●	●
	User cycles	●		○
	Workpieces, part, dressing, main and subprograms	●		○
	Compile cycles (manufacturer, user)	●	●	○
	Collision avoidance data	●	●	●
	I/O data	●	●	●
PLC data	PLC project	●	●	●
	Remanence data	●		

Components	Data	Backup	Setup [2]	Setup [2] adapted
Drive data	Drive data archiving	●	●	●
Programs on a local drive/NCextend	Programs contained in the user memory area. **Note**: Because the user data can become very large, the created archive file may require more storage. The content is only backed up if it does not exceed 1 GB.	●	●	●

Data area is available in the archive: ●

Data area can be added to the archive: ○

[1] For NC data, only the deviations from the standard default values are backed up. Machine data MD11210 $MN_UPLOAD_MD_CHANGES_ONLY and MD11212 $MN_UPLOAD_CHANGES_ONLY do not influence the archive content.

[2] The scope of data will be individualized in future software versions.

9.2 Importing the archive into the SINUMERIK MC

A DSF archive can be imported in the usual way into the SINUMERIK MC environment via the user interface of SINUMERIK ONE Commissioning. This allows you to commission NC and PLC components.

NOTICE
Data loss caused by archive difference when importing
Data not contained in the archive can be lost during the import.
Always create a backup file before reading in data

Machine status following read-in

After reading in, the machine has exactly the status that was previously defined with the archive type. The import differs principally with the following behavior:

Backup (for users)

- The existing control data are overwritten by the data from the DSF archive and may be added to the machine status.

Setup (for manufacturers)

- The data from the DSF archive map the exact status of the previously stored control.
- The control system is generally reset when starting the reading process.

Precondition

- Access level "Manufacturer" is required to read in an archive.
- Access level "User" is required to read in a backup (backup of the same control)
- You have a commissioning archive in the format *.dsf or *.arc.

Procedure

1. In SINUMERIK ONE Commissioning, switch over to the "Commissioning" operating area via "MENU SELECT > Commissioning > Commissioning archives".
2. Select the "Select archive" option for importing an archive and confirm with "OK".
   The "Import archive: Select Archive" window opens.
   - OR -
   To import the existing factory setting, select the "Restore factory setting" option and confirm with "OK".
   SINUMERIK ONE Commissioning automatically accesses the "original.dsf" file.

3. Select the archive and confirm with "OK".
   You obtain an overview with path details, version information, name of the archive, etc., as well as a list of the archived components.
   Clear the check box to exclude a component from the import process.
4. To import the archive, confirm with "OK".
   The "Import archive" window shows the import process with a progress display.

9.3 Creating a DSF archive on SINUMERIK MC

Archives can be created in the normal way via the SINUMERIK ONE Commissioning user interface. The data backup is made as commissioning archive in the *.dsf format. A commissioning archive can be generated, for example, after the control has been commissioned. To do this, control components can be saved individually or jointly. It is also possible to transfer the data backup to other controls so they can be updated to the same status.

The following archive types can be selected for the data backup:

All data of this machine (backup)

- Complete backup for restoration
- Complete backup for software upgrades

Data for a machine series (Setup)

- Data inventory for equipping a machine series
  The archive does not contain specific machine data, such as
  tools, part programs, address settings, compensations, PLC remanent data, workpiece counters, etc.

Factory setting of this machine (original)

- Data backup at a defined storage location

Note

We recommend that a backup archive is created regularly for specified work states of the SINUMERIK MC environment so that a required state can be reproduced whenever necessary.

Note

Restriction

An original archive is represented as backup.

Precondition

- Access level "User" is required to create a backup (backup of the same control).
- Access level "Manufacturer" is required to create a setup or original.

"Create archive" view

Parameter	Remark for configuration
Header	The header shows the selected archive type.
NCU components	Selected components to be written to the archive: • NCK • PLC • Drives • NCextend A progress display appears for each selected component during the archive creation. Once all components have completed their action, the status of each component is displayed. The archive is saved when all components have stored their data correctly. If any errors occur, even only for a single individual component, the archive is not saved. The error log is displayed.
Storage path	The archive path is preassigned, but can be changed with the "Change storage path" softkey.
Archive name	The system suggests a generic archive name. The generic archive name is formed from: • Archive type (e.g. Backup) • Abbreviation for selected components: NCK: N PLC: P Drive: D NCextend: L • Abbreviation for customization: CUST • Date (ISO) • Possibly an extension (1, 2, 3, etc.) **Example** Backup_NL_2019-06-03 Backup_NPD_2019-06-03_1 **Note** The generic archive name does not make any distinctions in the HMI runtime environment (PC, IPC, ...). The "original.dsf" archive name for restoring the factory setting cannot be changed.
Created by	Input field for the creator as well as the creation date of the archive (optional).
Comment	Input field for possible comments regarding the archive (optional).

Procedure

1. In SINUMERIK ONE Commissioning, switch over to the "Commissioning" operating area via "MENU SELECT > Commissioning > Commissioning archives".
2. Select one of the options for creating an archive and confirm with "OK".
   The "Create archive" window opens.
   This provides an overview with path details, name of the archive, etc., as well as an overview of the components to be archived.
3. Clear the check box to exclude a component from the creation process.
   The displayed archive name is automatically changed appropriately.
4. If required, change the storage location with the "Change storage path" softkey.
5. To create the archive, confirm with "OK".
   The "Create archive" window shows the creation process for each component with a progress display.

9.4 Creating a user-specific DSF archive on SINUMERIK MC

In addition to the NC control components, you can also adapt and create their data area specifically for a user-specific setup archive.

Procedure

1. In SINUMERIK ONE Commissioning, switch over to the "Commissioning" operating area via "MENU SELECT > Setup > Setup archive".
2. Select the option Setup to create an archive and confirm with "OK".
   The "Create archive" window opens.
3. Click the "Individual" softkey.
   The "Change" softkey is displayed.
4. Click the "Change" softkey.
   The "Change customization list" dialog with the NC data area is displayed.
5. Check or uncheck the checkboxes to include or exclude data from the archive creation process.

   Note

   System-relevant data are marked with grayed out checkboxes and cannot be adapted.

6. To reset the user adjustments, click the "Reset" softkey.
   All changes in the "Change customization list" dialog are reset to the default.
7. To confirm the customization, click "OK".
   At the edited component it is indicated that it has been adapted.
   The displayed archive name is supplemented with the addition CUST.
8. To disable the customizations, click the "Customized" softkey again.
   The "Change" softkey is hidden. The archive standard is restored.

   Note

   The customizations are reactivated when you click on "Customized" again. Settings that have already been adapted are not reset.

9. To create the customized setup archive, confirm with "OK".

Installation / upgrading 10

10.1 With the help of an MCU service system

10.1.1 Introduction, upgrading

Upgrade options

You have the option of initiating an upgrade of the CNC software with a USB flash drive:

Note

An upgrade is possible as of CNC software 1.22. An upgrade from other software versions is not permitted. In this case, a new installation is required.

Before the upgrade, you can make a backup of the complete SD Card. You can restore this backup to the SD Card using the Restore function.

Data backup before upgrades

Carry out a data backup before each upgrade:

- Commissioning archive of NC/PLC data
- Load PLC project to PC/PG (TIA Portal)
- License key

When the software is upgraded, all user data are kept on the SD Card in the directories /user, /addon, /oem. The license key is also kept.

Prior to overwriting a licensed SD Card, it is mandatory that the license key is backed up. The key is available in file 'keys.txt" and is stored under the path keys/sinumerik.

Note

Each license is assigned to a specific SD Card (card ID), and is only valid on the assigned card.

The license key can be read back via Web License Manager (Page 65) using the card number.

Tools for installation/upgrade

For an installation/upgrade, you require a bootable USB flash drive with approx. 16 GB capacity as your MCU service system. See Chapter "Creating a service system (Page 191)" for how to create a service system.

10.1.2 Upgrading the CNC software using VNC Viewer on PC/PG

Flow diagram

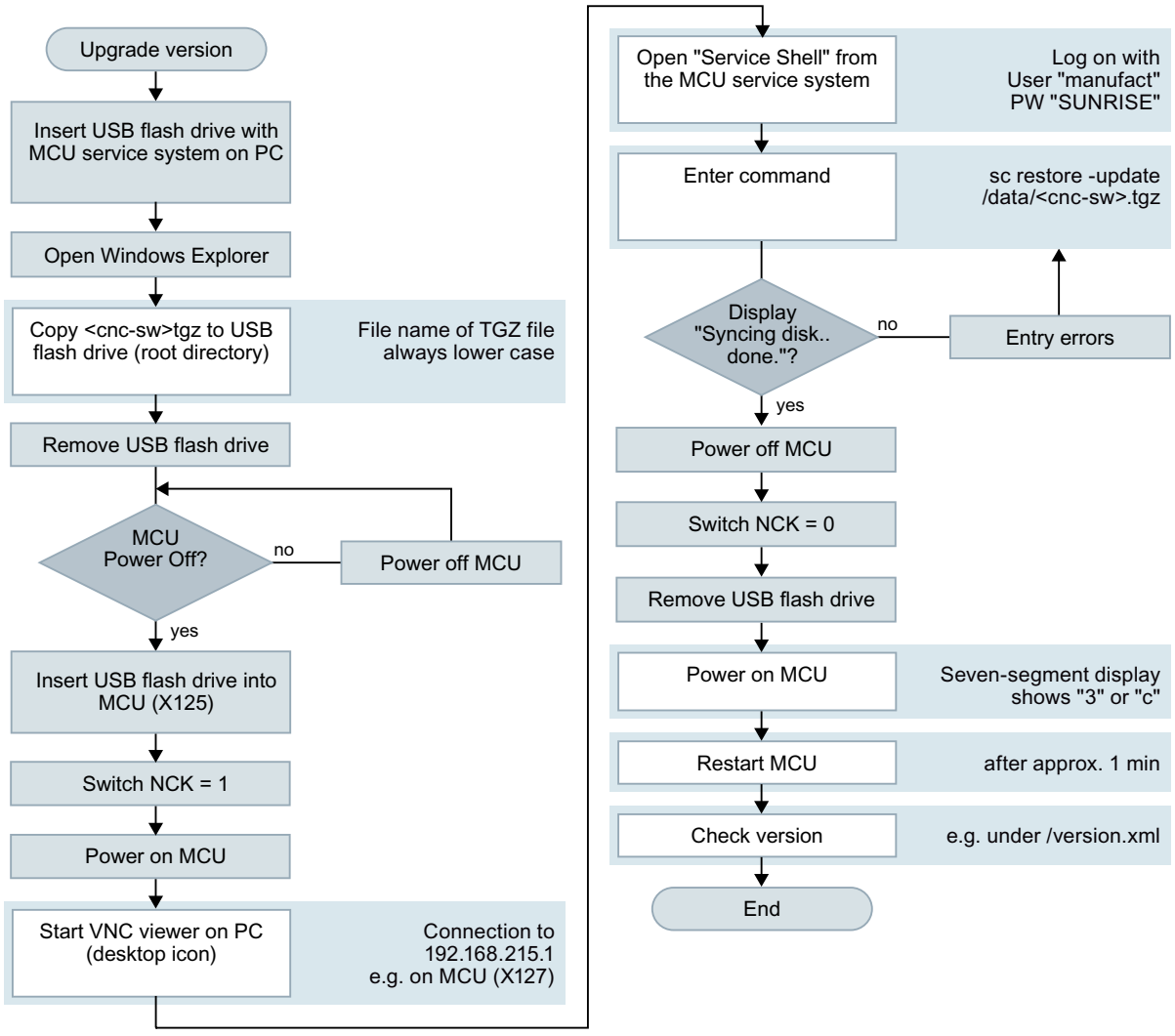


Figure 10-1 Upgrading the CNC software using VNC Viewer on PC/PG

10.2 Creating a service system

10.2.1 This is how you create a service system for the MCU

Purpose

In case service is needed, create a portable "Emergency Boot System" (EBS) on a USB memory. Now you can boot the MCU from the service system and perform various service tasks, such as, for example, data backup or updates, in a service shell.

Two partitions are created on the service system:

- A Linux partition that is not displayed under Windows.
- An FAT partition, to backup files or save software updates.
  The FAT partition can be read and written to under Linux as well as from a Windows system.
  The FAT partition can be addressed under the path/data in a command shell under Linux.

Scope of delivery

To create a service system on a USB flash drive, the following files are included on DVD:

- The program Access MyMachine /P2P
- An image file for the USB flash drive

Recommendation:

It is better to use SIMATIC PC USB flash drive.

Note

To create the service system, you need administrator rights.

All data already on the USB storage medium will be deleted.

Transfer is optimized for USB 2.0; this is why transfer to a USB flash drive using USB 1.1 takes longer than with USB 2.0.

Procedure

To create a service system on a USB storage medium:

1. Copy the service system onto a local hard disk of your PG/PC.
2. Connect the USB storage medium to the USB interface of the PG/PC.
3. In the Windows Explorer, find out which drive letter has been assigned to the USB flash drive, e.g. H:
4. Format the USB flash drive.
5. Open the program Access MyMachine /P2P.

6. In the menu bar of the program, click "Options" → "Write image to CF card...".
   Dialog box "Write image to CF card..." opens.

   Note

   As of Access MyMachine /P2P V4.9, you can find the "Write image to CF card" dialog in the menu bar under
   "Tools" → "Card image" → "Write image to card...".

7. In the dialog box, select an image file (.img) and drive letter (e.g. H:\) for the memory medium.
8. Click "Write".
   The image is written to the USB flash drive.

10.2.2 This is how you operate the service system

Connecting the service system, the first startup

Procedure:

1. Connect the USB flash drive to USB interface X125 or X135 of the MCU.
2. Switch off the system.
3. Turn the NCK commissioning switch on the interface front to position > 1.
4. Switch the system on again.
5. When the MCU boots for the first time, the service system is unzipped from the USB flash drive: Only then can the USB storage medium be used as service system and the complete storage capacity is available.

NOTICE
Restoring the SD Card To restore the SD Card in case of loss or damage to the partitions, use the image of the SD Card (available on PridaNet) and a data backup.

Operating the service system

Keys and softkeys to navigate in the service system:

Softkey	Key on the OP	External keyboard	Description
↓	HSK1	<F1>	Moves the cursor down a row
↑	HSK2	<F2>	Moves the cursor up a row
Page↓	HSK3	<F3>	Moves the cursor down a page

Softkey	Key on the OP	External keyboard	Description
Page↑	HSK4	<F4>	Moves the cursor up a page
Char↓	HSK5	<F5>	Inserts text or digits
Char↑	HSK6	<F6>	Inserts text or digits
Cancel	VSK7	<Shift> + <F7>	Cancel / Return
Ok	VSK8	<Shift> + <F8>	OK / Confirm
---		Pos1	Moves the cursor to the top row
---		End	Moves the cursor to the bottom row

Note

Operation with Touch Panels

The service system supports touch operation. The input fields are touch operated and the integrated keyboard automatically appears.

For example: SINUMERIK OP 019 black, SIMATIC HMI Industrial Thin Client

Installing and setting up PCU-Basesoftware /IPC 11

11.1 Delivery state

11.1.1 PCU-Basesoftware /IPC with Microsoft Windows 10

11.1.1.1 Overview

The software **PCU-Basesoftware /IPC** forms the basis for operating SINUMERIK software on your internal MCU-IPC (PC system) with Microsoft Windows 10:

SINUMERIK MC control system

The software PCU-Basesoftware /IPC is compatible for the SINUMERIK MCU 1720 CNC with the following article number:

- 6FC5222-1AA00-0AA0

For these MCU-IPC configurations, you can specifically order PCU-Basesoftware /IPC under the following article number:

- 6FC5800-0CP86-1YB0 (print license CoI) or
- 6FC5800-0CP86-1YH0 (electronic license eCoI)

More information

You can find an example workflow for commissioning and configuration under Overview (Page 200).

Note

PCU-Basesoftware /IPC V15.0 SP1 requires a new installation. A software update to this version is not possible. If necessary, check the MCU IPC system and manually back up your own PCU Base settings before performing the new installation.

Note

Do not switch off the hardware for PC systems with Microsoft Windows!

Data may be lost for Microsoft Windows-based systems if the system is not shut down properly before it is disconnected from the line supply. For technical reasons, data is still being written to the SSD/SD shortly after shutdown.

To avoid loss of data, use a SITOP UPS module.

See Configuring the SITOP UPS module for use with the PCU-Basesoftware /IPC (Page 210).

11.1.1.2 Supplied software

Overview

The software PCU-Basesoftware /IPC includes the following software and tools:

Software	Function
Microsoft Windows 10	Service Desktop
Microsoft Windows PE	Service Center
Paragon Hard Disk Manager™ 17 Suite	Creating and restoring disk images
SIEMENS PCU Installer	Installing software and updates
VNC Viewer	Remote access to other devices from the PC
PuTTY	Remote access to other devices from the PC
PuTTY Key Generator	Generating an SSH key pair
Npcap	Network packet driver - required for the support of SINUMERIK Thin Clients
Various configuration templates and scripts in the directory: `C:\ProgramData\Siemens\MotionControl\SIEMENS`	Templates for simplifying configuration

Note

Acknowledgements

- This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)
- This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

Note

Disk images of the **Symantec Ghost** software in *.gho format are not supported by PCU-Basesoftware /IPC Version 15 or higher.

11.1.2 Hardware configuration of the internal MCU-IPC

11.1.2.1 Network settings

The internal MCU-IPC has two Ethernet interfaces, which are set by the PCU Base for connection to the SINUMERIK system.

Table 11-1 SIMATIC

Hardware designations	Designation in PCU Base[1]	Configuration
X1	Local Area Connection 2	Preset as a standard DHCP client for connection to a **company network**. The IP address is dynamically fetched from the DHCP server at X1.
X2	Local Area Connection	Preset as SINUMERIK DHCP server (**system network**, preset IP address 192.168.0.241) in conjunction with X150 (NC/PLC, preset IP address 192.168.0.1). X2 is automatically configured as the master during installation of the PCU Base Software /IPC as of V15.0 SP1. By connecting the two networks of X2 and X150, SIMATIC ITC V3 and SINUMERIK HT 10 can be used as SINUMERIK Thin Clients. It is also possible to use SINUMERIK HT 2 on the MCU (Page 307).
X3	---	Disabled by default and not available for use
X4	---	Inaccessible from the outside Internal network connection to NC/PLC with designation "Intel(R) ... Gigabit Backplane Connection". Through the PCU Base Software /IPC as of V15.0 SP1, this interface receives the preset IP address 192.168.214.241. The NC/PLC has IP address 192.168.214.1 at this interface. This allows you to set up a connection to the NC/PLC over this interface via PuTTY/WinSCP or VNC Viewer (using the SINUMERIK Service System (Page 189)) for service purposes. This interface can also be used as a communication interface for the SINUMERIK ONE Commissioning installed on the MCU.

[1] The network designation may deviate depending on the system.

More information

- Setting the IP address and domain (Page 204)
- Adapting the firewall settings (Page 222)
- Remote access for diagnostics (Page 302)
- Network settings in the Service Center (Page 272)

11.1.2.2 Partitioning of the SSD

The partitioning of the SSD of your internal IPC is not changed when installing PCU-Basesoftware /IPC. Partition C: must have a minimum of 30 GB in order to be able to install PCU Base.

Name of the partition	**System (C:)**	**Data (D:)**
File system	NTFS	NTFS
Memory used by the system	~ 20 GB	~ 0 GB
Already occupied by	• Microsoft Windows 10 • PCU Base, including various applications and configuration templates (see Chapter Supplied software (Page 196))	-
Purpose	Installing user programs	• Customer-specific data • Backup images • Setup packages

11.1.3 Directory structure and file conventions

Templates for configuration files

To assist you with the system parameterization, templates for various configuration files are provided on the internal PC system. The templates are organized into various directories, which you will find below the following directory:

- `C:\ProgramData\Siemens\MotionControl\siemens`

These templates are already fully functional when supplied and will be used automatically if you do not create your own configuration files based on these templates.

Note

Do not modify files in the template directory `siemens`!

The `siemens` directory contains only files with the factory settings that can be copied and used as templates.

Never overwrite these files. Instead copy them into another directory (see Section *Your settings*).

Directory hidden in delivery condition

For security reasons, the `C:\ProgramData` directory is hidden in the delivery condition.

To view the directory, proceed in one of the following ways:

- To switch quickly to a hidden directory, type the address in the Windows Explorer.
- To show all hidden directories by default, change the setting in the Control Panel under "Appearance and Personalization > File Explorer Options > View > Advanced Settings".
- To show only one directory by default, first make the setting to show all hidden directories, then activate the attribute "Hidden" in the properties of the directory and finally again make the setting to not show all hidden directories.

Your settings

Several directories are available into which you can copy and adapt configuration files in order to make your own settings. In decreasing order of priority, these are:

- `C:\ProgramData\Siemens\MotionControl\`**user**
- `C:\ProgramData\Siemens\MotionControl\`**oem**
- `C:\ProgramData\Siemens\MotionControl\`**addon**

The settings in a configuration file in a directory with higher priority always replace those from one of lower priority. Template directory `siemens` has the lowest priority.

To define your own settings, therefore, copy a setting from the relevant template file into a directory with higher priority, e.g. below directory `user`.

11.2 Commissioning the internal MCU-IPC for the first time

11.2.1 Overview

After you have commissioned your MCU-IPC configuration (Page 195) for the first time using PCU-Basesoftware /IPC, you can configure the internal IPC just the same as a SINUMERIK PCU.

You can find an example workflow of the first commissioning and configuration in this tabular overview.

Note

For PC systems with Microsoft Windows 10, do not switch off the hardware!

Data may be lost for Microsoft Windows-based systems if the system is not shut down properly before it is disconnected from the line supply. For technical reasons, data is still being written to the SSD shortly after shutdown.

To avoid loss of data, use a SITOP UPS module.

See Configuring the SITOP UPS module for use with the PCU-Basesoftware /IPC (Page 210).

Example workflow

No.	Step	Description
1	Set up and commission the MCU (according to the operating instructions)	Information on setting up and installing your MCU can be found in the corresponding hardware documentation.
2	Install PCU-Basesoftware /IPC	Ideally, SINUMERIK PCU-Basesoftware /IPC is installed and set up on the internal PC system of the MCU. If required, adapt the installation settings (Page 200) and install PCU-Basesoftware /IPC (Page 201).
3	Connect the PG/PC	To be able to access a directory of a PG/PC in the network, for example, connect the PG/PC in the network (Page 291).
4	Configure network settings on PG/PC	Once you have networked the PC system, a PG/PC and any other devices with one another, configure the network settings of your PG/PC (Page 291).
5	Set up more user accounts	Before you install software, at least one user account with limited rights must be set up (Page 203).
6	Install software and updates	Install the automation software and Microsoft Windows updates required (Page 252).
7	Configure the system	Configure the installed software (Page 252), Windows 10 and other system characteristics (Page 203) and, if necessary, the SITOP UPS module (Page 210).
8	Create a disk image (backup)	Create a disk image of the SSD as a backup (Page 270) to be able to return to this version in a maintenance situation.

11.2.2 Adapting the installation settings

The setup of PCU-Basesoftware /IPC also contains the setup.ini configuration file which can be parameterized before calling the setup. Note that some settings are only suitable for test purposes.

Before you adapt the settings in this file, you should copy the original file.

Section	Setting	Description
[IPC]	FirewallSettings=	• 1 (default setting) The Microsoft Windows Firewall settings are adapted appropriately for the company network by the PCU-Basesoftware /IPC, as described in this documentation. • 0 The current firewall settings are not changed by the setup.
	InstallWin10Updates=	• 1 (default setting) When setting up PCU-Basesoftware /IPC, important Microsoft Windows updates are installed that are required when using PCU Base. If these updates cannot be installed, the setup of the PCU Base is canceled. • 0 The setup does not check whether the Microsoft Windows updates required for PCU-Basesoftware /IPC have been installed or can be installed. This setting may be required when new updates have already been installed on the PC system, for example.
	TestSystemEnglish=	• 1 (default setting) The setup checks whether an English Microsoft Windows version has been installed. • 0 The setup does not check the Microsoft Windows language version. In this case, there is an additional prerequisite that the names of the network adapter do not, for example, contain a hyphen. Note that this setting is only suitable for test purposes. PCU-Basesoftware /IPC is only compatible with English Microsoft Windows versions.
[SetupControl]	FinalReboot=	• 1 (default setting) The PC system is restarted after installation. • 0 The setup does not restart the system or call a dialog after the installation as to whether a restart is to be performed (supervised installation).

11.2.3 Installing PCU-Basesoftware /IPC

You can install PCU-Basesoftware /IPC on the internal IPC of the MCU (Page 195) (PC system) (using an installation medium that can be individually ordered and licensed).

In the Industry Mall you can find the PCU-Basesoftware /IPC under the following article number:

- 6FC5800-0CP86-1YB0 (print license CoI) or
- 6FC5800-0CP86-1YH0 (electronic license eCoI)

Requirement

- You can connect an operator panel front or screen and keyboard directly to the PC system.
- The commissioning of the PC system is completed and an administrator account is set up.

- There is an English Microsoft Windows installation on the PC system.
- The partition C: of the PC system has a minimum size of 30 GB.
- The installation medium is available on the PC system.

Procedure

To install PCU-Basesoftware /IPC on your PC system, proceed as follows:

1. Open Microsoft Windows Explorer and switch to the installation medium of PCU Base.
2. Double-click the file "setup.exe".
3. Restart the PC system after you have installed PCU Base.

Result

PCU-Basesoftware /IPC has been installed. During the installation, the previously existing settings on the PC system, e.g. user accounts, keyboard layout, date and time settings, were imported. Set up additional user accounts (Page 203) if necessary and set the keyboard layout to English (Page 206).

The PCU Installer is initially inactive after the installation. It must be activated (Page 258) before software can be automatically installed.

11.3 Configuration of the system

11.3.1 Overview

Once you have completed the first commissioning, you can adapt the configuration of the system:

- For security reasons, set up user accounts (Page 203) with limited rights.
- You can view or change (Page 204) the name of the PC system.
- The network settings (Page 204) in the state when delivered have been adapted for use with the SINUMERIK system, and usually do not have to be changed.
- You can deactivate the USB interfaces (Page 204) to prevent malicious software from entering the system network via this route.
- You can set up an external screen (Page 206) or set the screen resolution (Page 207) and color depth (Page 209).
- If you use a SITOP UPS module for the uninterruptible power supply or plan to use one, configure it for use with PCU-Basesoftware /IPC (Page 210).
- Use the BitLocker drive encryption (Page 246). This protects your data storage medium against data theft.

Other configuration options (e.g. desktop background) are available directly from the Service Desktop and can be implemented using Microsoft Windows 10 methods.

More information

- To call Windows help, click "Get Help" in the Start menu.
- Help for Microsoft Windows 10 is available on the Internet on the Microsoft website: Microsoft Windows support (https://support.microsoft.com/en-us/hub/4338813/windows-help?os=windows-10)

11.3.2 Managing user accounts

Overview

When commissioning for the first time, you must create a local Microsoft Windows administrator account and define a password.

You can set up and manage additional Microsoft Windows user accounts in the Control Panel. To do that, log on with administrator rights.

Note

Administrator account cannot be recovered

If you have forgotten the password of the administrator account there is no way of recovering it!

11.3.3 Changing the name of the PC system

A unique computer name is set after installing PCU-Basesoftware /IPC. You can view and change it in the Control Panel of the Service Desktop.

You can find the computer name in the Microsoft Windows Control Panel under Category "System" in Section "Computer name, domain and workgroup settings".

11.3.4 Setting the IP address and domain

The network settings in the state when delivered have been adapted for use with the SINUMERIK system, and usually do not have to be changed.

If you want to distinguish your network configuration from the factory settings, you can adapt them in the Microsoft Windows Control Panel.

You can find the settings in the following menu (icon view):

- "Control Panel > Network and Sharing Center > View network connections"

More information

You can adapt the network settings for backing up and restoring disk images in the configuration of the Service Center (Page 219).

11.3.5 Configuring USB interfaces

To prevent malware from entering the control or the system network via the USB interfaces, you can deactivate the USB interfaces.

You can configure the USB interfaces on the Service Desktop via a command in the "Run" dialog box in the prompt.

Procedure

To activate or deactivate the USB interfaces, enter the relevant command on the Service Desktop in the "Run" dialog box or at the prompt:

Table 11-2 Disabling USB interfaces with the "sc_usb disable" command

Syntax:	sc_usb disable [-minutes] [all] [HOSTS...]
Description:	• Without a time indication [-minutes], a permanent disable is set. With time indication, the disable takes the time set in minutes. • The disable may refer to all network nodes of the system network, or a list of host names or IP addresses may be specified to which the disable should apply.

Table 11-3 Activating USB interfaces with the "sc_usb enable" command

Syntax:	sc_usb enable
Description:	With "sc_usb enable" USB storage units on permanently disabled USB interfaces or on certain host names or IP addresses are enabled again.

11.3.6 Configuring network access on the USB data storage medium

If you connect a removable data storage medium (e.g. a USB flash drive) to a USB interface of the PC system, a network drive is set up automatically. In this way, a removable data storage medium can be accessed from an NC in the network. The file and the printer sharing is activated automatically by Microsoft Windows.

If you do not require network access to USB removable data storage medium, you should deactivate the automatic network share.

You can find this setting in the `basesys.ini` at `EnableUSBShares`.

Precondition

- Hidden directories are visible
- A copy of the basesys.ini configuration file is stored in the `user` directory:
  `C:\ProgramData\Siemens\MotionControl\`**`user`**`\System\etc\basesys.ini`
- The `basesys.ini` configuration file in the `user` directory is not write-protected

Further information at Directory structure and file conventions (Page 198)

Procedure

To configure the automatic network share of USB data storage media of the PC system, proceed as follows:

1. Open the basesys.ini configuration file in the `C:\ProgramData\Siemens\MotionControl\`**user**`\System\etc\` directory.
2. Remove the semicolon in front of the EnableUSBShares line and set the required value.
   - `EnableUSBShares=0`
     The automatic network share of USB data storage media (and the associated file and printer sharing) is deactivated.
   - `EnableUSBShares=1` (default value)
     The automatic network share of USB data storage media is activated.
3. Save and close the file.

11.3.7 Configuring the keyboard layout

It is assumed that the English keyboard layout is used in SINUMERIK ONE Commissioning and for the SINUMERIK operator panel fronts.

If a different keyboard layout is set in Microsoft Windows, this should therefore be changed while commissioning the PC system or before using SINUMERIK ONE Commissioning.

The setting of the keyboard layout as well as the display of the active keyboard layout is shown in the Microsoft Windows task bar.

11.3.8 Setting up an external screen

You can connect an external screen (SIMATIC IFPxx00 V2 Multitouch) to the MCU IPC system. The procedure follows the usual procedure under Microsoft Windows 10.

Procedure

To use an external screen for the Service Desktop or service system, proceed as follows:

1. The PC system is switched off.
2. The external screen is connected to the DisplayPort of the MCU.
3. The PC system is switched on again. The screen (preferably, SIMATIC IFPxx00 V2 Multitouch) is automatically detected.

Result

The external screen has been connected and can be used.

11.3.9 Setting the screen resolution

You can set the screen resolution directly in Microsoft Windows 10 or use the PCU Base-specific file tcu.ini.
The settings in tcu.ini overwrite the Microsoft Windows system settings. Compared with Microsoft Windows, they offer additional functions for switching over the resolution of the PC system depending on, for example, the screen connected during run-up.

Further information regarding configuration file tcu.ini is available in the following Chapter (Page 207).

11.3.10 Set the resolution in the tcu.ini

Overview

The system behavior during run-up for the screen resolution is set in the `tcu.ini` file in Section [VNCServer].

You will find a template of the `tcu.ini` under `C:\ProgramData\Siemens\Motion Control\siemens\System\etc\`
Do not overwrite this template, but rather create your own `tcu.ini` inside one of the user directories.

Further information: Directory structure and file conventions (Page 198)

Setting the resolution during run-up of the PC system

The following options are available for selection in the tcu.ini file in the [VNCServer] section (below the `# RESOLUTION` comment):

```
0 = SYSTEM
1 = AUTO_OP_1 (default)
2 = AUTO_OP_2
3 = AUTO_MON_1
4 = AUTO_MON_2
5 = 640x480
6 = 800x600
7 = 1024x768
8 = 1280x1024
9 = 800x480
10 = 1280x800
11 = 1366x768
12 = 1920x1080
13=3840x2160
```

The meaning of the settings are as follows:

Table 11-4 Settings in the configuration file `tcu.ini`

Setting	Meaning
SYSTEM	The resolution is not specially set during run-up. i.e. the resolution last used in the system is active, e.g. the resolution which had been set manually in the Control Panel.
AUTO_OP_1	Default setting: When running up, the resolution is automatically set in accordance with the following scenarios:
Example 1:	There is a panel (irrespective of whether a monitor possibly exists): The resolution is set to the max. resolution of the panel (max. 1920x1080).
Example 2:	There is no panel, but there is a monitor: The resolution is not specially set; i.e. the resolution last used in the system is active, e.g. the resolution which had been set manually in the Control Panel. (Difference with respect to AUTO_OP_2 !)
AUTO_OP_2	Like AUTO_OP_1, except: Example 2: There is no panel, but there is a monitor: The resolution is set to the max. resolution of the monitor, reduced to the next lowest SINUMERIK resolution. SINUMERIK resolutions are 640x480, 800x600, 1024x768, 1280x1024, 800x480, 1280x800, 1366x768 and 1920x1080. **Example:** In the case of a monitor with a max. resolution of 2048x1152, the SINUMERIK resolution setting is 1920x1080.
AUTO_MON_1	While running up, the resolution is automatically set ("monitor" has priority) in accordance with the following scenarios:
Example 1:	There is a monitor (irrespective of whether a panel possibly exists): The resolution is set to the max. resolution of the monitor, reduced to the next lowest SINUMERIK resolution. SINUMERIK resolutions are 640x480, 800x600, 1024x768, 1280x1024, 800x480, 1280x800, 1366x768 and 1920x1080. **Example:** In the case of a monitor with a max. resolution of 2048x1152, the SINUMERIK resolution setting is 1920x1080. If there is a panel, the display there is panned if the max. resolution of the panel is lower than the max. resolution of the monitor.
Example 2:	There is no monitor, but there is a panel: The resolution is not specially set; i.e. the resolution last used in the system is active, e.g. the resolution which had been set manually in the Control Panel. (Difference with respect to AUTO_MON_2 !)
Example 3:	There is neither a monitor nor a panel (headless operation): The resolution is not specially set - i.e. the resolution used during the previous session in the system is active, e.g. the resolution set manually in the Control Panel.
AUTO_MON_2	Like AUTO_MON_1, except: Example 2: There is no monitor, but there is a panel: The resolution is set to the max. resolution of the panel (max. 1920x1080).
640x480	During run-up, the SINUMERIK resolution is set to 640x480.
800x600	During run-up, the SINUMERIK resolution is set to 800x600.

Setting	Meaning
1024x768	During run-up, the SINUMERIK resolution is set to 1024x768.
1280x1024	During run-up, the SINUMERIK resolution is set to 1280x1024.
800x480	During run-up, the SINUMERIK resolution is set to 800x480.
1280x800	During run-up, the SINUMERIK resolution is set to 1280x800.
1366x768	During run-up, the SINUMERIK resolution is set to 1366x768.
1920x1080	During run-up, the SINUMERIK resolution is set to 1920x1080.
3840x2160	During run-up, the SINUMERIK resolution is set to 3840x2160.

11.3.11 Setting the color depth in the tcu.ini file

The color depth of the PC system is set to 16 bits as default via the `tcu.ini` configuration file, and is reset to this value each time the system runs up.

To use a different color depth, you must adapt the setting in the `tcu.ini` file in the [VNCServer] section.

Precondition

- Hidden directories are visible
- A copy of the tcu.ini configuration file is stored in the `user` directory:
  `C:\ProgramData\Siemens\MotionControl\`**`user`**`\System\etc\tcu.ini`
- The `tcu.ini` configuration file in the `user` directory is not write-protected

Procedure

To adapt the color depth of the PC system, proceed as follows:

1. Open the tcu.ini configuration file in the `C:\ProgramData\Siemens\MotionControl\`**`user`**`\System\etc\` directory.
2. Enter the required value in the [VNCServer] section (below the `#COLOR DEPTH` comment):
   - `ColorDepth=0`
     The color depth is not changed during run-up, but rather the color depth used last is retained. This means that you can adapt the color depth in the Microsoft Windows settings.
   - `ColorDepth=1` (default value)
     The color depth is set to 16 bit while running up.
   - `ColorDepth=2`
     The color depth is set to 32 bit while running up.
3. Save and close the file.

11.3.12 Configuring the SITOP UPS module for use with the PCU-Basesoftware /IPC

11.3.12.1 Overview of SITOP UPS

SITOP UPS modules can temporarily maintain operation of the MCU with the internal PC system if a power failure occurs, and/or run down the system correctly.

For example, a SITOP UPS module also protects against data loss when the MCU-PC system hardware is shut down, because with Microsoft Windows-based systems, data is still briefly written to the SSD after the system has been run down for technical reasons.

- You will find general information about SITOP UPS modules used in combination with PCU-Basesoftware /IPC in Chapter SITOP modules for IPC (Page 211).
- If you want to use a SITOP UPS module in combination with PCU-Basesoftware /IPC, you must first adapt the settings of the SITOP software (Page 211).
- Optionally, you can adapt the wait time after which the operating software will be forced to shut down (Page 214).
- You must configure the hardware (Page 217) of the SITOP UPS module before using it with PCU-Basesoftware /IPC.

NOTICE
Ensure the readiness for operation of the SITOP power supply In order to prevent data loss, the SITOP power supply must be ready for operation. Note the following: • The SITOP power supply may not be ready for operation immediately after being switched on (a capacitor-buffered UPS500 requires 1-2 minutes make time, for example). • The operating system and the SITOP software must have run up so that the SITOP software can shut down the system correctly when a power failure occurs. • The readiness for operation and the functional capability of the SITOP power supply must be ensured (e.g. battery of capacitor charged). • Please also note all the information on the readiness for operation in the documentation of your SITOP device.

More information

Information on using SITOP UPS modules in combination with PCU-Basesoftware /IPC can also be found on the Internet:

- Example of using an uninterruptible power supply (http://support.automation.siemens.com/WW/view/en/90142681)
- Typical values for an operator station with Microsoft Windows (http://support.automation.siemens.com/WW/view/en/76773241)
- Catalog KT 10.1 SITOP Power Supply
- SIEMENS Industry Mall > 24 V DC Uninterruptible Power Supplies (https://eb.automation.siemens.com/mall/en/US/Catalog/Products/7010117)

11.3.12.2 SITOP modules for IPC

Suitable SITOP UPS modules

SITOP UPS modules can temporarily maintain operation of the MCU with the internal PC system if a power failure occurs, and/or run down the system correctly.

In conjunction with PCU-Basesoftware /IPC, all specific applications are taken into account (e.g. operating software) with the `USVShutdown.bat` component.

In the delivery condition of the MCU, when the power fails, it takes approximately 20 seconds to safely run down the internal IPC. For a typical power consumption of approx. 60 W, a capacitor-buffered UPS with an energy storage device of 2.5 kW is recommended. If longer buffer times are required, then several expansion modules can be connected in a cascade connection.

Example of a SITOP UPS module that can be used (USB):

SITOP 500S (15 A / 2.5 kWs capacitor)

Article No.: 6EP1933-2EC41

Example of a SITOP UPS with Ethernet/PROFINET interface that can be used:

SITOP UPS1600 starter kit

- DC-UPS SITOP UPS1600 24V DC/10A
- SITOP UPS1100 3.2 AH battery module

Article No.: 6EP4134-3AB00-2AP0

Note

Information about the test environment for machine OEMs

The functionality has been tested in the standard configuration with PCU-Basesoftware /IPC.

When installing add-on or OEM software components, you must check the shutdown procedure of the entire system and adapt the factory setting (180 seconds).

Further information at Parameterizing the wait time to exit the operating software (Page 214)

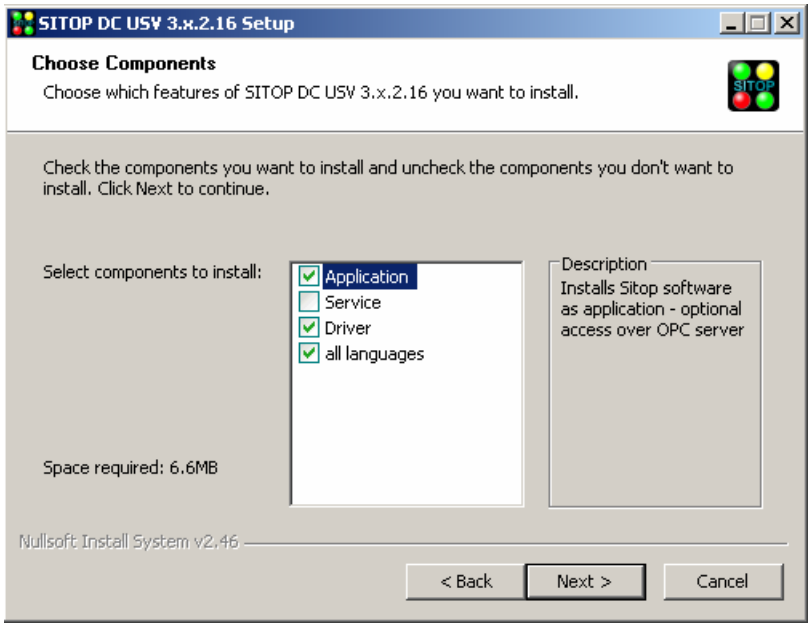
11.3.12.3 Configuring SITOP software for PCU Base

Configuring SITOP software V3.x (USB)

If you want to use a SITOP UPS module in combination with PCU-Basesoftware /IPC, you must first adapt the settings of the SITOP software.

Requirement

- The SITOP UPS hardware is connected via the USB interface.
- The SITOP software of version 3.x.2.16 or later is installed in directory `C:\Program Files (x86)\SITOP\`
- If you want to use SITOP software of version 3.2.1.16 or older, this must be installed as a normal application, not as a service.



Note

Microsoft Windows service of the SITOP software version 3.2.1.16 or older is not compatible with PCU-Basesoftware /IPC

If you use SITOP software, version 3.2.1.16 or older as a Microsoft Windows service with PCU Base for IPC, the correct shutdown procedure cannot be performed!

If you have installed the SITOP software of version 3.2.1.16 as a Microsoft Windows service, you must uninstall this and install it again as an application in order to be able to use it in conjunction with PCU Base.

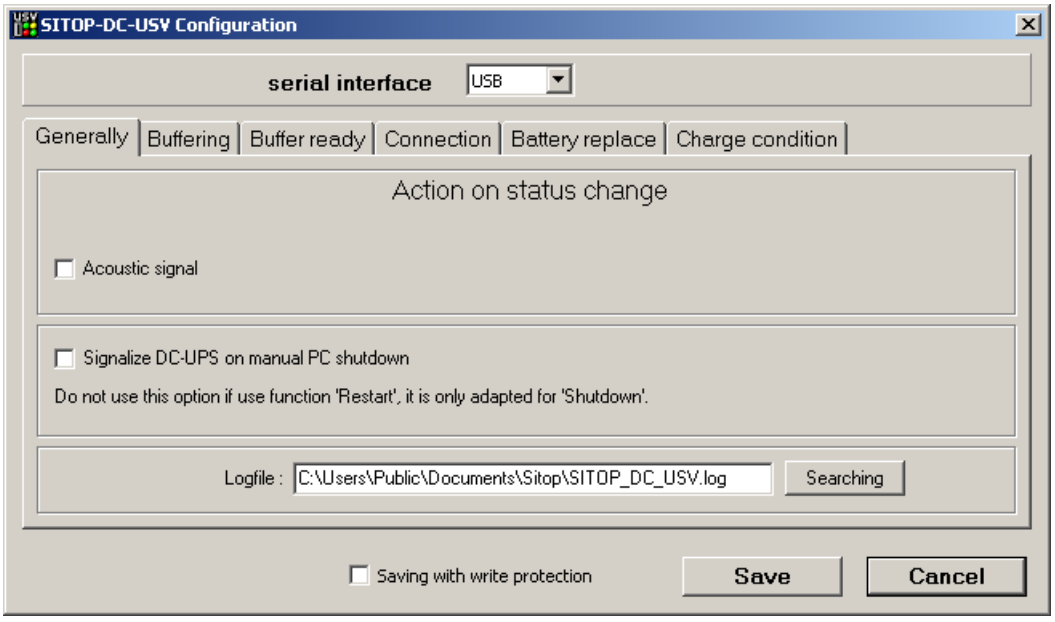
From version 3.2.1.17, the SITOP software can be used as service with PCU-Basesoftware /IPC and is recommended.

- The SITOP software was configured during the installation so that it starts automatically when Microsoft Windows is run up (factory setting).
- The Service Desktop is active.

Procedure

Proceed as follows to configure the SITOP software for use with PCU-Basesoftware /IPC:

1. Call the settings of the SITOP software, for example, by right-clicking the SITOP UPS icon in the Microsoft Windows information area and then selecting "Configuration".
   The "SITOP DC UPS Configuration" dialog box opens.



2. In the "General" tab, select "UPS" in the drop-down list at "Serial interface".

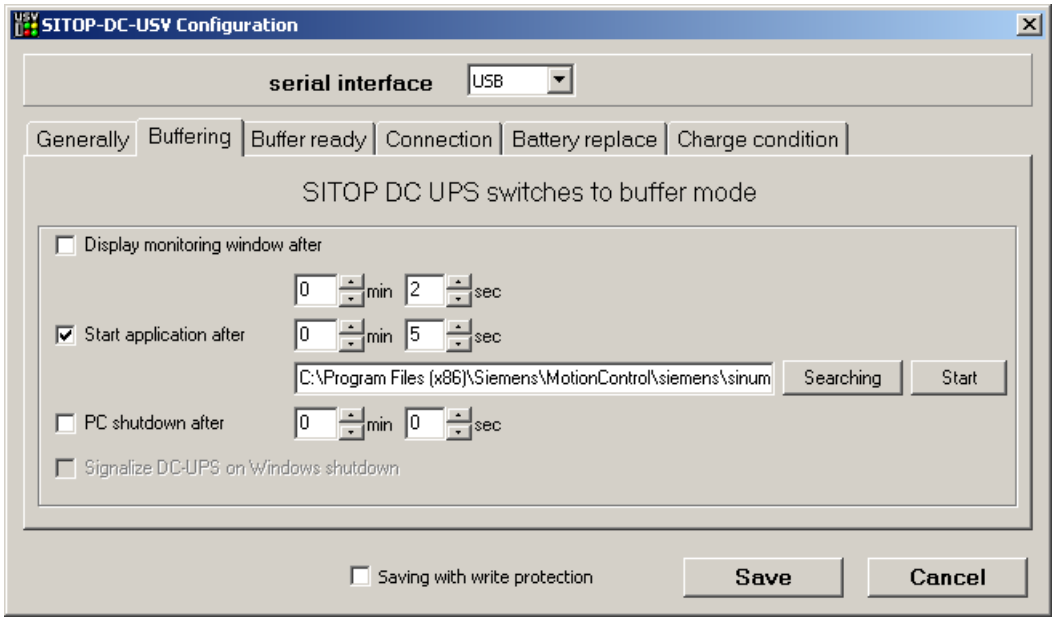
3. Switch to the "Floating operation" tab and make the following settings:
   – Deactivate the "Display monitoring window after" checkbox

   Note
   Deactivating the monitoring window
   Display of the monitoring window can cause malfunctioning of the operating software.

   – Click directly in the text field at "Start application after" and specify the path of the `USVShutdown.bat`:
   `C:\Program Files (x86)\Siemens\MotionControl\siemens\sinumerik\hmi\base\USVShutdown.bat`

   Note
   Do not use the "Browse" button
   The dialog can crash if you use the "Browse" button to specify the path of the `USVShutdown.bat`.
   Instead, enter the path directly in the text field.

   – After you have specified the path of the `USVShutdown.bat`, activate the "Start application after" checkbox. Optionally, you can specify the wait time after which the `USVShutdown.bat` is to be executed (e.g. 5 seconds).



4. Confirm the settings with "Save".

Parameterizing the wait time to exit the operating software

Before the SITOP Monitor runs down Microsoft Windows, `USVShutdown.bat` shuts down operation of the operating software.

If the operating software cannot be shut down within 180 seconds (factory setting) due to an error, then the application is forced to shut down and Microsoft Windows is run down.

If the operating software of your OEM installation is not shut down within 180 seconds, then you can manually parameterize this wait time.

Note

Information about the test environment for machine OEMs

The function "SITOP UPS" has been tested in the standard configuration with PCU-Basesoftware / IPC. When installing add-on or OEM software components, you must check the shutdown procedure of the entire system and adapt the factory setting.

Requirement

- The SITOP UPS module is configured for use with PCU-Basesoftware /IPC.
  For further information see under Configuring SITOP software V3.x (USB) (Page 211).
- The Service Desktop is active.

Procedure

Proceed as follows to change the delay time:

1. Call the settings of the SITOP software, for example, by right-clicking the SITOP UPS icon in the information area and then selecting "Configuration".
2. In the "SITOP DC UPS Configuration" dialog box, enter the wait time in seconds as a command line parameter in the "Buffering" tab:
   - Syntax: `<path>\USVShutdown.bat -<time in seconds>`
   - Example: `C:\Program Files (x86)\Siemens\MotionControl\siemens\sinumerik\hmi\base\USVShutdown.bat -180`

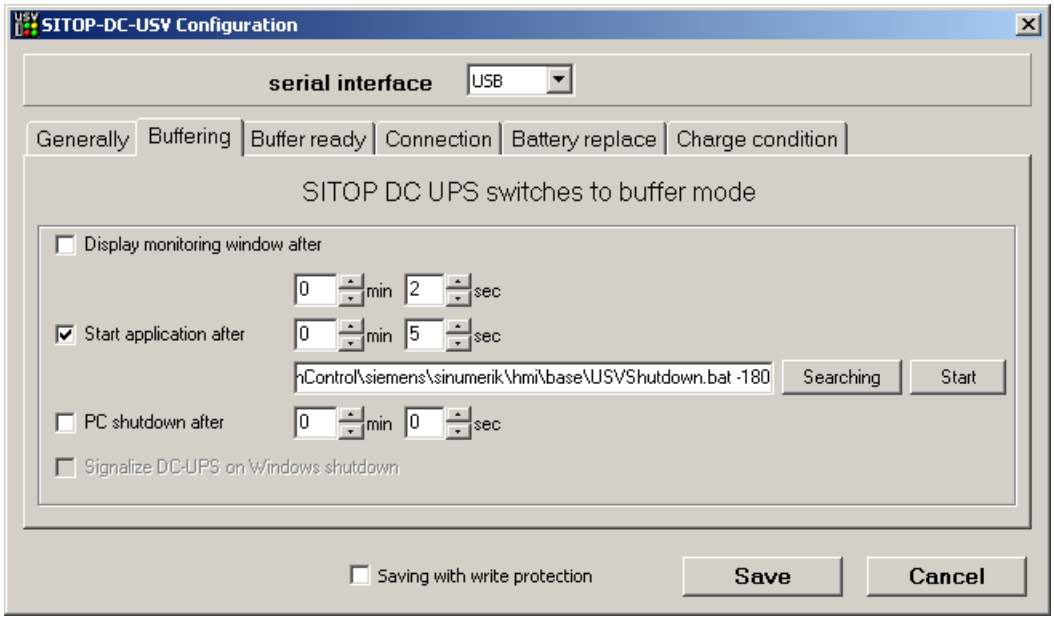


Figure 11-1 SITOP Monitor Floating operation

3. Confirm the setting with "Save".

Configuring SITOP UPS Manager (Ethernet)

Requirement

- The SITOP UPS hardware is connected via the Ethernet interface.
- The SITOP-UPS Manager has been installed and configured for Ethernet.

Note

Validity of the information on the SITOP components in this manual

This information only involves the configuration of the settings relevant for PCU Base. In addition, all the information and notes in the corresponding manuals of your SITOP UPS hardware and SITOP UPS Manager apply.

Procedure

1. Call the SITOP UPS Manager.
2. Change to "Software configuration > Buffer mode".
3. Make the following settings:
   - Activate the checkbox "Start application on power failure" - and there, enter the path of USVShutdown.bat:
     C:\Program Files (x86)\Siemens\MotionControl\siemens\sinumerik\hmi\base\USVShutdown.bat
   - When required, configure the wait time until the operating software is terminated using USVShutdown.bat (factory setting = 180 seconds).

     Note

     Information about the test environment for machine OEMs

     The function "SITOP UPS" has been tested in the standard configuration with PCU-Basesoftware /IPC. When installing add-on or OEM software components, you must check the shutdown procedure of the entire system and adapt the factory setting.

     To do this, enter the wait time in seconds as command line parameter:
     Syntax: <path>\USVShutdown.bat -<time in seconds>
     Example: C:\Program Files (x86)\Siemens\MotionControl\siemens\sinumerik\hmi\base\USVShutdown.bat -180
4. Confirm the settings with "Configuration changed, restart application now".

11.3.12.4 Hardware configuration of the SITOP UPS module

Buffering parameterization

The UPS module can be used to select whether buffering should be completed after a predetermined period of time or not until the accumulator's lowest discharge threshold (= maximum buffer time) has been reached. Both buffering parameterizations result from this.

"Maximum buffer time" mode

This mode enables the system to be shut down in a time-optimized manner. The UPS module is synchronized with the shutdown of the operating system. Buffering is maintained until the operating system has been shut down. The operating system must shut down within a maximum of 5 minutes (including all applications). Otherwise, the UPS module buffers for the maximum buffer time (dependent on the accumulator state).

Required settings on the UPS module (USB interface)

	On - Off			
1		○	+2V	Cut-in threshold +22V fixed
2		○	+1V	
3	○		+0.5V	

	On - Off			
4		○	+1V	End-of-charge voltage + 26.3V fixed
5		○	+1V	
6	○		+0.5V	
7	○		+0.2V	
8		○	+0.2V	
9		○	+0.1V	
10		○	0.35A / 0.7A	Charging current

	On - Off			
1		●		Set time/max. time
2		○	+320 s	Buffer time +5 s fixed
3		○	+160s	
4		○	+80s	
5		○	+40s	
6		○	+20s	
7		○	+10s	
8	●			Disconnection
9		○		Battery operating state on/off

Legend:

○ Delivery condition setting

● Setting for operation at the MCU with internal PC system

"Fixed buffer time" mode

In this mode, the UPS module always buffers for the pre-selected, fixed period of time. It is not possible to synchronize the UPS module with the operating system shutdown.

Required settings on the UPS module

	On - Off			
1		○	+2V	Cut-in threshold +22V fixed
2		○	+1V	
3	○		+0.5V	

	On - Off			
4		○	+1V	∘ ∘ End-of-charge voltage + 26.3V fixed
5		○	+1V	
6	○		+0.5V	
7	○		+0.2V	
8		○	+0.2V	
9		○	+0.1V	
10		○	0.35A / 0.7A	Charging current

	On - Off			
1	●			Set time/max. time
2		○	+320 s	∘ ∘ Buffer time +5 s fixed
3	●		+160s	
4		○	+80s	
5		○	+40s	
6		○	+20s	
7		○	+10s	
8	●			Disconnection
9		○		Battery operating state on/off

Legend:

○ Delivery condition setting

● Setting for operation at the MCU with internal PC system

11.3.13 Configuration of the Service Center

11.3.13.1 Overview

You can permanently adapt the settings for the backup and restoration of disk images (Service Center (Page 270) component) in the "Service Center Backup/Restore" dialog box:

- Configuration of the network adapter (Page 220)
- Configuration of the host (Page 221)

Adaptations that you make here are stored in the `servicesystem.ini` configuration file.

You can also adapt the settings directly in the configuration file `servicesystem.ini`.

You can also view the log files of the Service Center or restart the internal PC system in the Service Center in dialog "Service Center Backup/Restore".

To open the dialog box, click the ServiceCenter Backup-Restore icon on the Desktop.

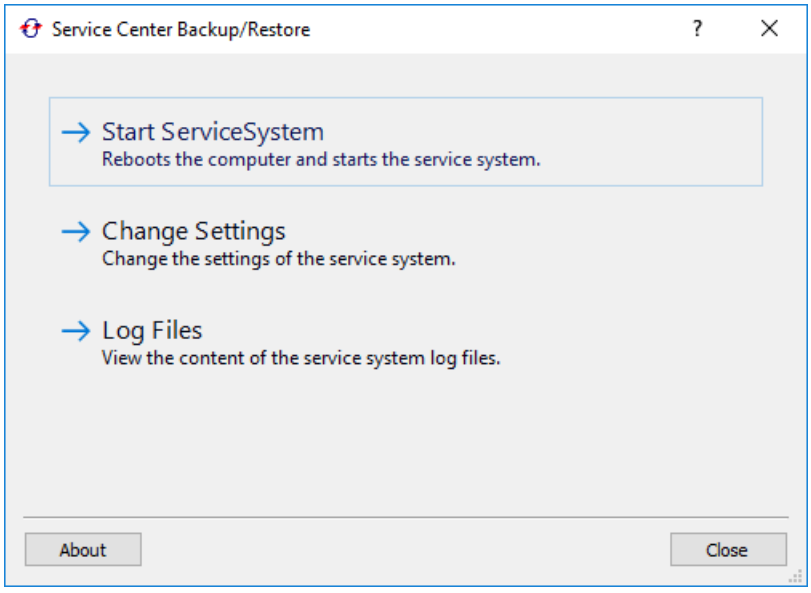


Figure 11-2 Service Center Backup/Restore

Note

Deactivate the BitLocker encryption to carry out settings in the "Service Center Backup/Restore" dialog via headless operation.

11.3.13.2 Configuration of the network adapter

You can make the network settings in the "Adapter Settings" tab and permanently save this configuration, in contrast to the settings in the "Network Settings" dialog box of the Service Center (Page 272).

Settings that you make in this dialog box are stored in the `servicesystem.ini` configuration file.

Overview

You can make the following IP settings in the "Adapter Settings" dialog box:

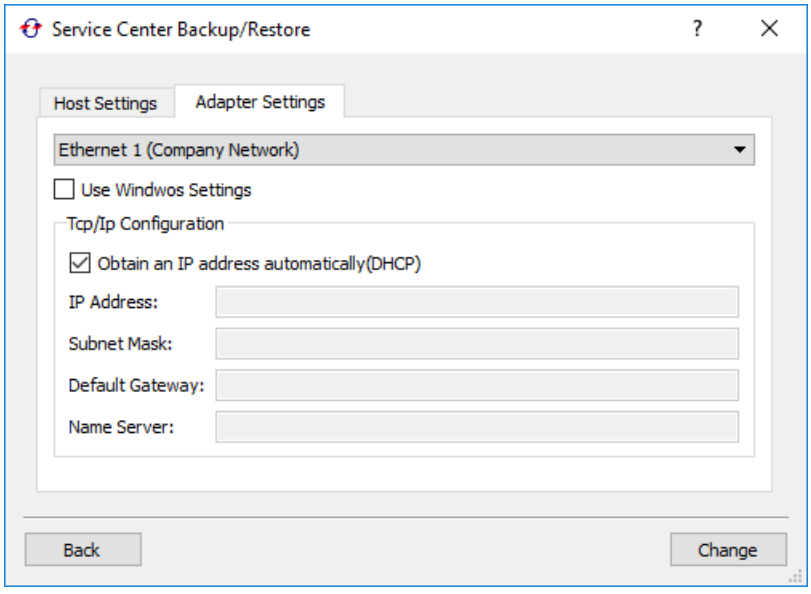


Figure 11-3 Adapter settings - Ethernet 1 (company network)

Table 11-5 Settings in the "Adapter Settings" dialog box

Setting	Purpose
Adapter	Select the Ethernet interface that you want to configure. All settings in this dialog box refer to the selected Ethernet interface.
Use Windows Settings	Select whether the values set in the Microsoft Windows Control Panel should be used.
Obtain an IP address automatically (DHCP)	Select whether the addresses are to be fetched dynamically from the DHCP server. If the checkbox is deactivated, you must make the settings manually.
IP Address	Set the IP address of the NCU. You can specify an IP address from the following range: 192.168.214.250 - 254
Subnet Mask	Specify a subnet mask, e.g. 255.255.255.0
Default Gateway	Set the IP address of the standard gateway. A standard gateway creates a standard route in the IP routing table for all destinations that are not in the subnet.
Name Server	Set the IP address of the name server. A name server answers questions asked about a domain name zone using a DNS database.

11.3.13.3 Configuration of the host

You can make the network settings in the "Host Settings" tab and permanently save this configuration, in contrast to the settings in the "Network Settings" dialog box of the Service Center.

Settings that you make in this dialog box are stored in the `servicesystem.ini` configuration file.

Overview

You can make the following settings in the "Host Settings" dialog box:

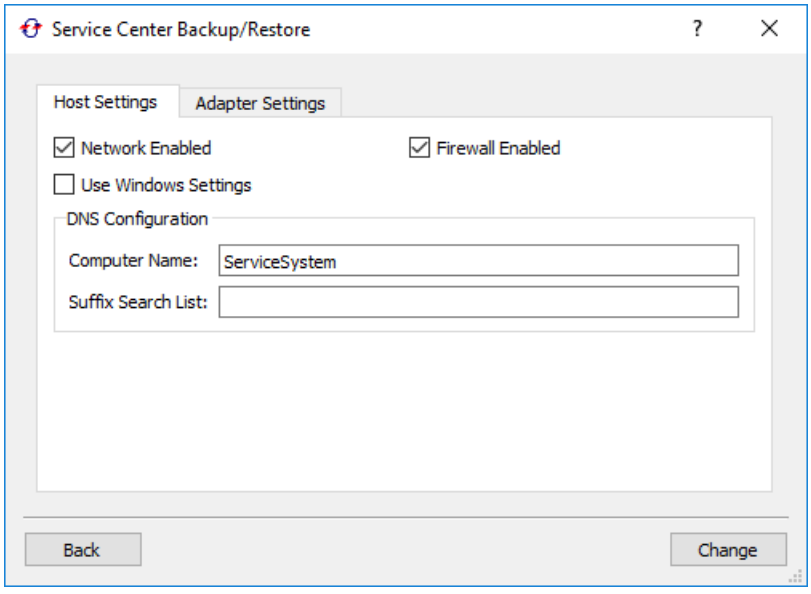


Figure 11-4 Host settings

Table 11-6 IP settings in the "Host Settings" dialog box

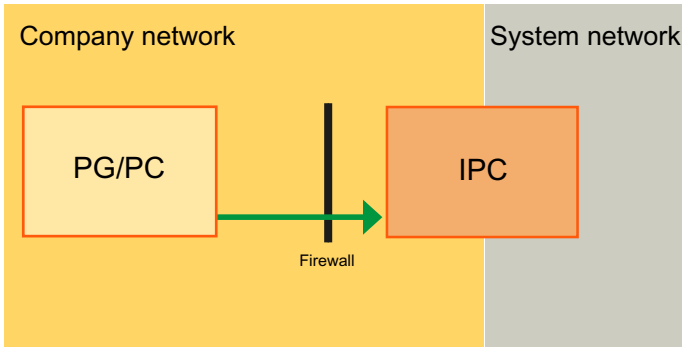
Setting	Purpose
Network enabled	Activate or deactivate network interfaces of the internal PC system.
Firewall enabled	Activate or deactivate the firewall of the internal PC system.
Use Windows Settings	Select whether the values set in the Microsoft Windows Control Panel should be used.
DNS Configuration > Computer Name	Specify the DNS computer name.
DNS Configuration > Suffix Search List	Parameterize a search list for DNS suffix, e.g. "network.com". The factory setting of the Ethernet interface "Local Area Connection" is ".local".

11.3.14 Adapting the firewall settings

11.3.14.1 Overview

From a PG/PC in the system or company network, you can directly access resources on the internal MCU-IPC (PC system). The same also applies when accessing a PG/PC in the system or company network from the PC system.

For example, if you want to access the internal PC system via the company network, you must adapt the firewall settings.



You can adapt the following settings:

- Activating remote access to the internal PC system (Page 228)
- Enabling SNMP communication (Page 226)
- Activation/deactivation of the file and printer release (Page 231)
- Activation of the ping execution (ICMP) (Page 240)

As a rule, you can make these settings in the Control Panel or via the prompt or a script/batch file (relevant for series commissioning) (Page 225).

You can save and restore (Page 242) the firewall settings, (even on different IPCs, e.g. due to series commissioning)

Also note the general information in this chapter:

- Factory setting of the Microsoft Windows Firewall on the MCU-IPC (Page 223)
- General information on the operating principle of the Microsoft Windows Firewall (Page 224)
- General information on the settings recommended for Microsoft Windows (Page 225)

11.3.14.2 Factory setting of the Microsoft Windows Firewall on the MCU-IPC

The Microsoft Windows Firewall settings on your internal PC system are appropriately configured by PCU-Basesoftware /IPC for the use of SINUMERIK software and systems. For security reasons, the Microsoft Windows Firewall is activated in the company network and expanded by additional rules. The descriptions in this chapter largely relate to the adaptation of the firewall settings for the company network.

Table 11-7 Factory settings for network adapter and Windows Firewall

	System network	Company network
Interface	X2	X1
Network name IPC	Local Area Connection	Local Area Connection 2
Network profile	Public	Public
Microsoft Windows Firewall status More information: General information on the settings recommended for Microsoft Windows (Page 225)	Activated	Activated

	System network	Company network
File and printer sharing More information: Activation/deactivation of the file and printer release (Page 231)	Deactivated and blocked by firewall	Deactivated and blocked by firewall
SNMP communication More information: Enabling SNMP communication (Page 226)	Blocked	Blocked
Remote access (via port 5900) More information: Activating remote access to the internal PC system (Page 228)	Blocked	Blocked
Outgoing ICMP ping requests from the internal PC system More information: Activation of the ping execution (ICMP) (Page 240)	Permitted	Permitted
Incoming ICMP ping requests on the internal PC system More information: Activation of the ping execution (ICMP) (Page 240)	Blocked	Blocked

Note

Automatic network share of USB data storage media results in activation of the file and printer sharing

The automatic network share of USB data storage media is activated in the default setting of PCU-Basesoftware /IPC. The file and printer sharing is then activated by Microsoft Windows when a USB data storage medium is connected.

More information: Configuring network access on the USB data storage medium (Page 205)

11.3.14.3 General information on the operating principle of the Microsoft Windows Firewall

Microsoft Windows Firewall rules are structured as follows:

- The firewall rules are divided into Inbound Rules and Outbound Rules.
- Each firewall rule is valid for one or several network profiles (Profiles).
  Each network connection in Microsoft Windows is assigned to a specific network profile. In the factory setting state of the internal PC system, both the system network ("Local Area Connection") and the company network ("Local Area Connection 2") have the network profile "Public".
- Some firewall rules are already assigned to so-called "Groups". As a result, you can more easily activate or deactivate specific related network functionalities (e.g. file and printer sharing).

You can make the Microsoft Windows Firewall settings using the Control Panel and using the prompt or script/batch files. The use of script/batch files is particularly recommended for series commissioning. Alternatively, for series commissioning, you can make all of the Microsoft Windows Firewall settings on an individual IPC, save these settings, and apply them to other devices (Page 242).

11.3.14.4 General information on the settings recommended for Microsoft Windows

Firewall settings recommended by Microsoft Windows are unsuitable for use in the system network

In the Control Panel, under "Windows Defender Firewall", there is a display indicating that the firewall settings do not correspond to the settings recommended and automatically checked by Microsoft Windows. The corresponding sections are highlighted in red:



However, the settings automatically recommended by Microsoft Windows are not suitable for use in the system network, and would restrict the functioning of the plant. The network security in the system network must therefore be ensured by other security precautions. In this regard, observe the information about Industrial Cybersecurity (Page 252).

Note

Do not use firewall settings that are automatically recommended by Microsoft Windows!

The command "Use recommended settings" overwrites the existing firewall settings, which are required for operating PCU-Basesoftware /IPC, and therefore this command must not be used.

Otherwise, the Microsoft Windows Firewall will be activated in the system network and communication of internal services of the PCU Base will be inhibited.

11.3.14.5 Configuration by means of a prompt or script/batch file

You can make most of the settings described in this chapter both using the Control Panel and using the prompt or script/batch files. The use of script/batch files is particularly recommended for series commissioning.

Basic procedure

You can enter these commands either directly into the prompt or save the command in a script or batch file:

- **Direct input of the command:**
  - Call the prompt as the administrator.
  - You can enter the commands either directly or in succession.
- **Calling the command via a script file (or batch file):**
  - Save the command in a text file.
  - Call the prompt as the administrator.
  - Specify the script file as follows:
    `netsh -f <File name of the script file>`

Further information

Descriptions of the commands and of all of the associated parameters of Netsh within the Advfirewall firewall context can be found on the Microsoft website:

- Microsoft Windows Server documentation (https://docs.microsoft.com/en-us/windows-server/index)
- Microsoft TechNet: Netsh (command line program) (https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc785383(v=ws.10)?redirectedfrom=MSDN)
- Microsoft TechNet: Netsh AdvFirewall Firewall Commands (https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd734783(v=ws.10)?redirectedfrom=MSDN#BKMK_3_set)
- Microsoft TechNet: Netsh Commands for Windows Firewall with Advanced Security (https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc771920(v=ws.10)?redirectedfrom=MSDN)

11.3.14.6 Enabling SNMP communication

Some network diagnostic functions use SNMP communication. These are blocked in the plant and company network If you have productively linked your plant in the company network, then SNMP communication is partially blocked:

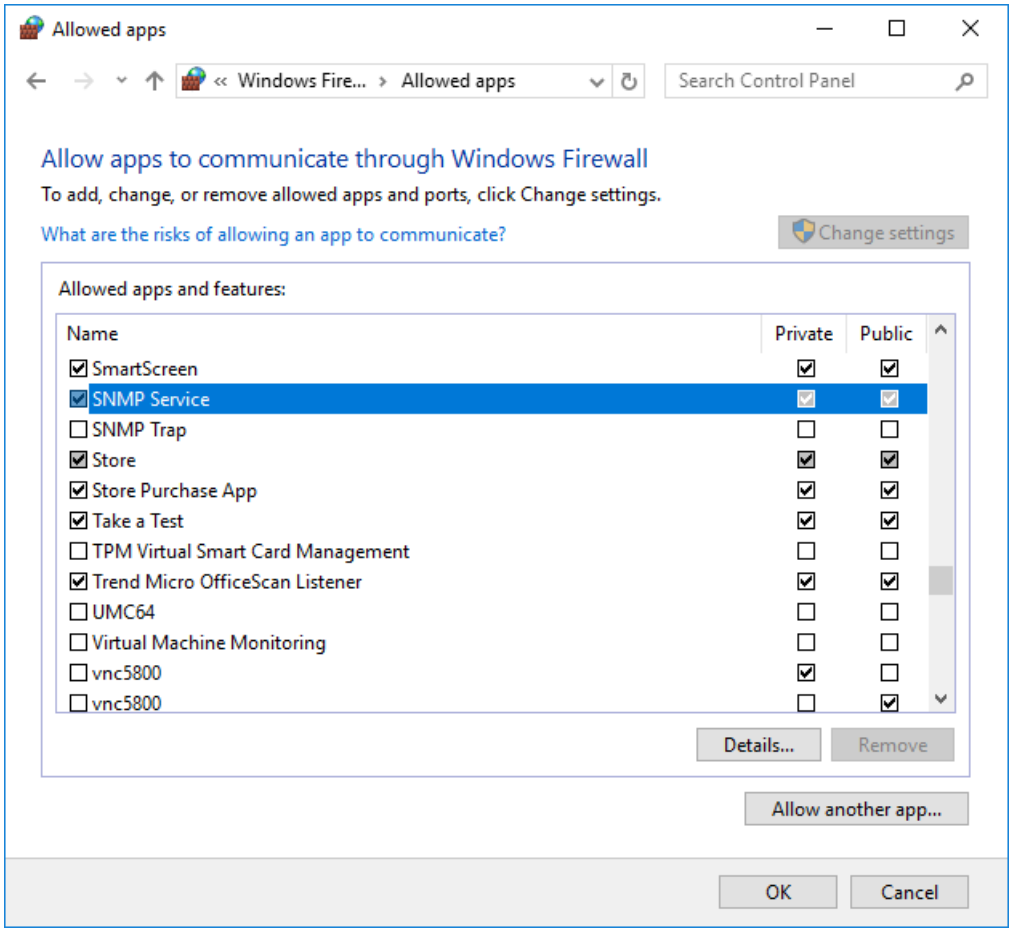
- In the factory settings version of the PCU-Basesoftware /IPC, incoming SNMP communication is blocked in the company network.
- Outgoing SNMP communication in the company network is not blocked.

In the settings for the Microsoft Windows Firewall, you can activate SNMP communication via check box "SNMP Service" for specific network profiles.

Procedure

To permit incoming SNMP communication on the PC system, proceed as follows:

1. Enter "Control Panel" in the search field and then click on "Control Panel" in the search results.
   The desktop App "Control Panel" opens.
2. Click on the display selection and switch from the "Category" view to "Icons".
   The "All Control Panel Items" dialog box opens.
3. Click on "Windows Defender Firewall" > "Allow a app or feature through Windows Defender Firewall".
   The "Allowed apps" dialog box opens. The various checkboxes for "SNMP Service" are checked and displayed with a green or gray background, because the SNMP service is partially activated: Incoming queries are blocked on the PC system, while outgoing queries from the PC system are permitted.



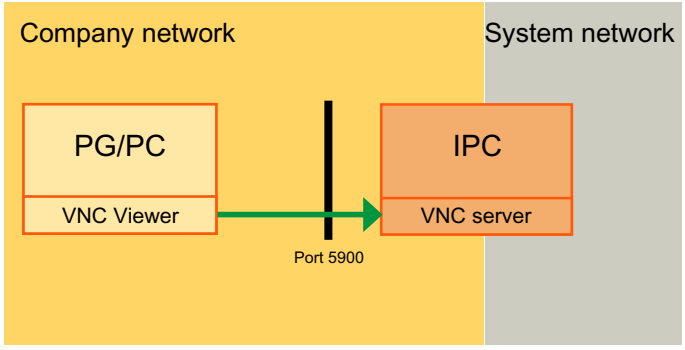
4. Click on "Change Settings" and confirm with "Yes", if applicable.
5. Activate the checkbox of the corresponding network profile completely, e.g. "Public" for the company network (factory setting).
6. Click "OK" to confirm the change.

11.3.14.7 Activating remote access to the internal PC system

Overview

Basically, it is possible to access the MCU-IPC (PC system) via the plant and via the company network through VNC:

Remote access to the internal PC system from a PG/PC in the plant or company network is blocked as a result of the factory setting. For example, if you want to access via the company network, then you must adapt the firewall settings.



The inbound rule "vnc5900", which is deactivated in the factory settings state, is available for this purpose in the expanded settings for the Microsoft Windows Firewall. To activate remote access to the internal PC system in the company network, you can activate this rule either directly in the Control Panel (Page 228), or in the prompt or by using a script/batch file (Page 229).

More information

In addition to the firewall settings, you may have to adapt other settings to establish a remote connection in the company network.

More information on this topic is provided in Chapter Remote access for diagnostics (Page 302), especially under Remotely accessing the MCU for operation and maintenance (Page 303).

More information on the system network: Connection options in the system network (Page 291)

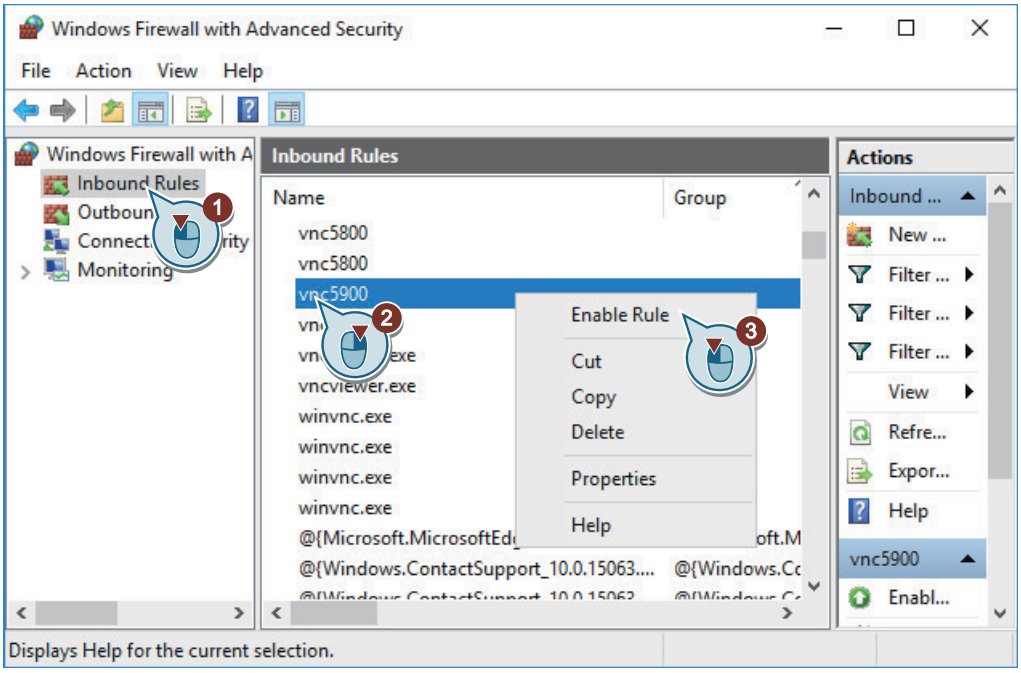
Via the Control Panel

Procedure

Proceed as follows to activate remote access to the internal PC system from the PG/PC in the company network:

1. Enter "Control Panel" in the search field and then click on "Control Panel" in the search results. The desktop App "Control Panel" opens.
2. Click on the display selection and switch from the "Category" view to "Icons". The "All Control Panel Items" dialog box opens.

3. Click on "Windows Defender Firewall".
4. Click on "Advanced settings" and confirm the call of the expanded settings with "Yes" if necessary.
5. In the "Windows Firewall with Advanced Security" dialog, right-click under "Inbound Rules" on the rule "vnc5900", then click on "Enable Rule".



Result

When activating the inbound rule "vnc5900", Port 5900 was enabled in the company network, which allows remote access from a PG/PC to the internal PC system in the company network.

If you want to deactivate remote access in the company network, right-click on the rule "vnc5900" and select "Disable Rule" in the shortcut menu.

More information

You can find general information on remote access to the internal PC system (via VNC Viewer or SSH client) in Chapter Remote access for diagnostics (Page 302).

By prompt, script or batch file

Basic procedure

With a command according to the following scheme, you can activate remote access from the PG/PC in the company network to the internal PC system.

To do this, call the prompt as the administrator and enter the command either completely or successively.

Alternatively, you can save the command and the associated parameters in a script file (Page 225).

Syntax for activating a firewall rule via the prompt

```
netsh advfirewall firewall set rule name="<Name of the firewall rule>" new
enable=yes profile=<Name of the network profile>
```

Table 11-8 Description of the Netsh commands in the context of the advfirewall firewall

Command	Parameter	Description	Value
netsh		Specification of the command line program, which executes the following commands.	-
advfirewall		Defines the context in which the following commands are to be carried out.	-
firewall		Subcontext of "advfirewall".	-
set rule		Adaptation of an existing firewall rule.	-
	name	Name of the firewall rule in quotation marks	"vnc5900" | ... | all
	new	Specifies that the following parameters are to be changed or added.	-
	enable	Activates or deactivates the specified firewall rule.	yes | no
	profile	Name of the network profile for which the corresponding firewall rule is to be activated or deactivated.	public | private | domain | any | ...

Example

Activation of the firewall rule "vnc5900" for the "Public" profile.

```
netsh advfirewall firewall set rule name="vnc5900" new enable=yes profile=public
```

11.3.14.8 Activation/deactivation of the file and printer release

Overview

If you want to access a directory of the internal PC system via the plant or company network, then you must adapt the firewall settings.

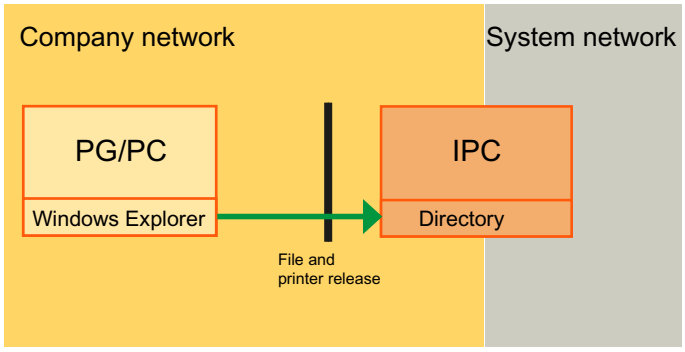


Figure 11-5 An example of an access to a shared directory in the IPC in the company network from a PG/PC

Overview

You can enable the file and printer sharing either for all of the network profiles, for a specific network profile, or for a specific network connection:

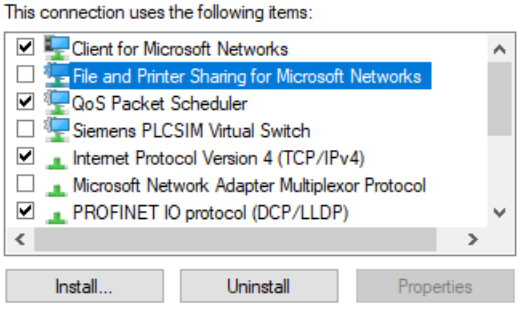
- General activation for all network profiles (Page 232)
  - Via the Control Panel (Page 232)
  - By prompt or script file (Page 234)
- Activation for a specific network profile (Page 235)
  - Via the Control Panel (Page 235)
  - By prompt or script file (Page 237)
- Activation for a specific connection (Page 239)
  - Via the Control Panel (Page 239)
  - By prompt or script file (Page 240)

General information

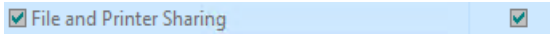
General information on file and printer sharing in Microsoft Windows

In Microsoft Windows, there are settings for the file and printer sharing at two different locations: In the settings of the corresponding network adapter and in the Microsoft Windows Firewall settings.

- The file and printer sharing is blocked in the Microsoft Windows Firewall settings:
  In the plant and company network, the Microsoft Windows Firewall is activated and the file and printer sharing is blocked by the Microsoft Windows Firewall.
  These settings can be changed in various dialog boxes, e.g. in the "Network and Sharing Center" or in the "Allowed apps" dialog box.
- In the settings of the network adapter for the plant or company network, the file and printer sharing is activated using a check box.



If different settings are selected for the network adapter for the plant and company networks, then this can be seen in the corresponding Microsoft Windows Firewall setting dialogs as a result of the partially activated check box (green or gray background).



More information

Further information on file and printer sharing is provided in Microsoft Windows support (https://support.microsoft.com/en-us/hub/4338813/windows-help?os=windows-10).

General activation for all network profiles

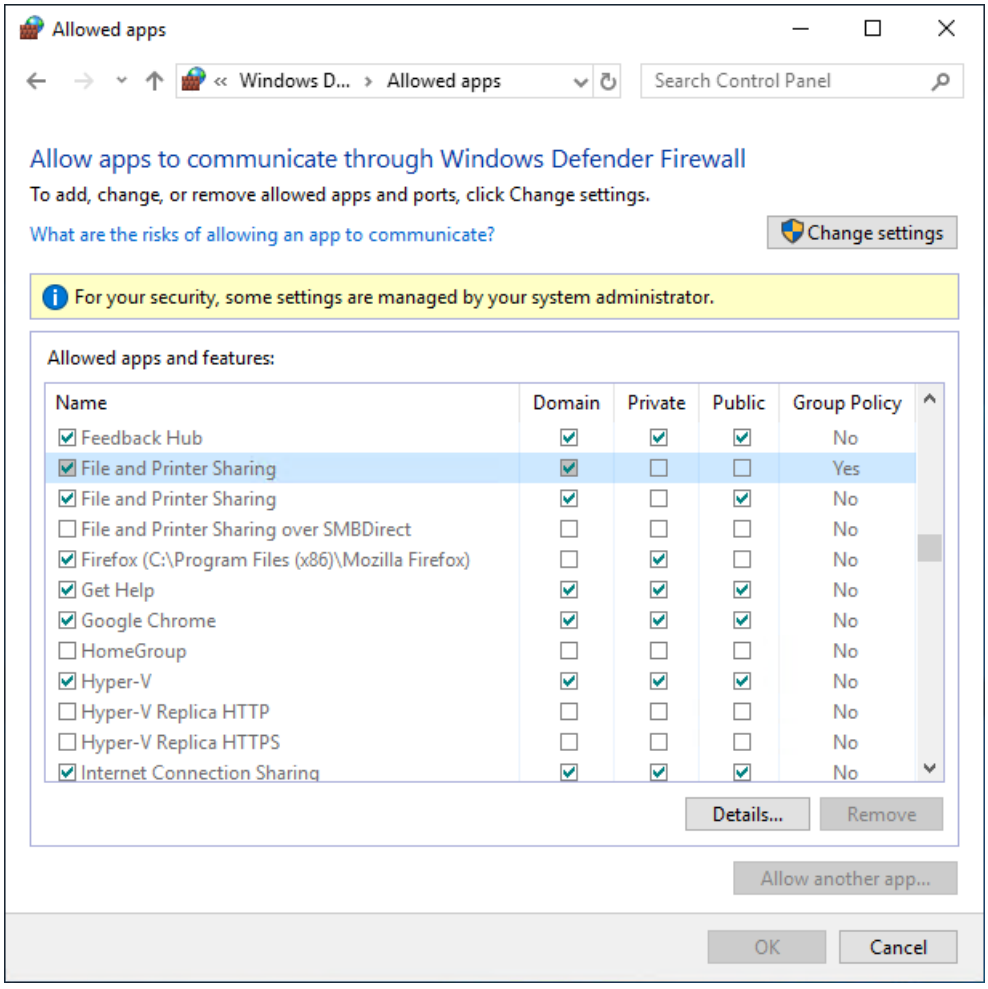
Via the Control Panel

There are several procedures for activating the file and printer sharing for all of the network profiles in the Microsoft Windows Firewall. (For example, there is the alternative procedure via the "Network and Sharing Center" under "Change advanced sharing settings").

Procedure

Proceed as follows, to activate the file and printer sharing on the internal PC system:

1. Enter "Control Panel" in the search field and then click on "Control Panel" in the search results.
   The desktop App "Control Panel" opens.
2. Click on the display selection and switch from the "Category" view to "Icons".
   The "All Control Panel Items" dialog box opens.
3. Click on "Windows Defender Firewall" > "Allow a app or feature through Windows Defender Firewall".
4. Click on "Change Settings" and confirm with "Yes", if applicable.
   The "Allowed apps" dialog box opens.
   Also observe the entry in the column "Group Policy" and the color of the checkboxes (a checkbox with a green or gray background indicates partial activation).



5. Activate the corresponding checkbox for the corresponding entry "File and Printer Sharing" for the desired network profiles.
6. Click "OK" to confirm the change.

By prompt, script or batch file

Basic procedure

With a command according to the following scheme, you can allow the file and printer release in the company network for all of the network profiles together. All of the firewall rules of the group "File and Printer Sharing" are changed for all network profiles.

To do this, call the prompt as the administrator and enter the command either completely or successively.

Alternatively, you can save the command and the associated parameters in a script file (Page 225).

Syntax for activating a group of firewall rules via the prompt

```
netsh advfirewall firewall set rule group="<group name>" new enable=yes
```

Table 11-9 Description of the Netsh commands in the context of the advfirewall firewall

Command	Parameter	Description	Value
netsh		Specification of the command line program, which executes the following commands.	-
advfirewall		Defines the context in which the following commands are to be carried out.	-
firewall		Subcontext of "advfirewall".	-
set rule		Adaptation of existing firewall rules.	-
	group	Name of the group with firewall rules	"File and Printer Sharing" | ...
	new	Specifies that the following parameters are to be changed or added.	-
	enable	Activates or deactivates the specified group of firewall rules.	yes | no

Example

Activation of the firewall rule "File and printer release" for the "Public" profile.

```
netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=yes
```

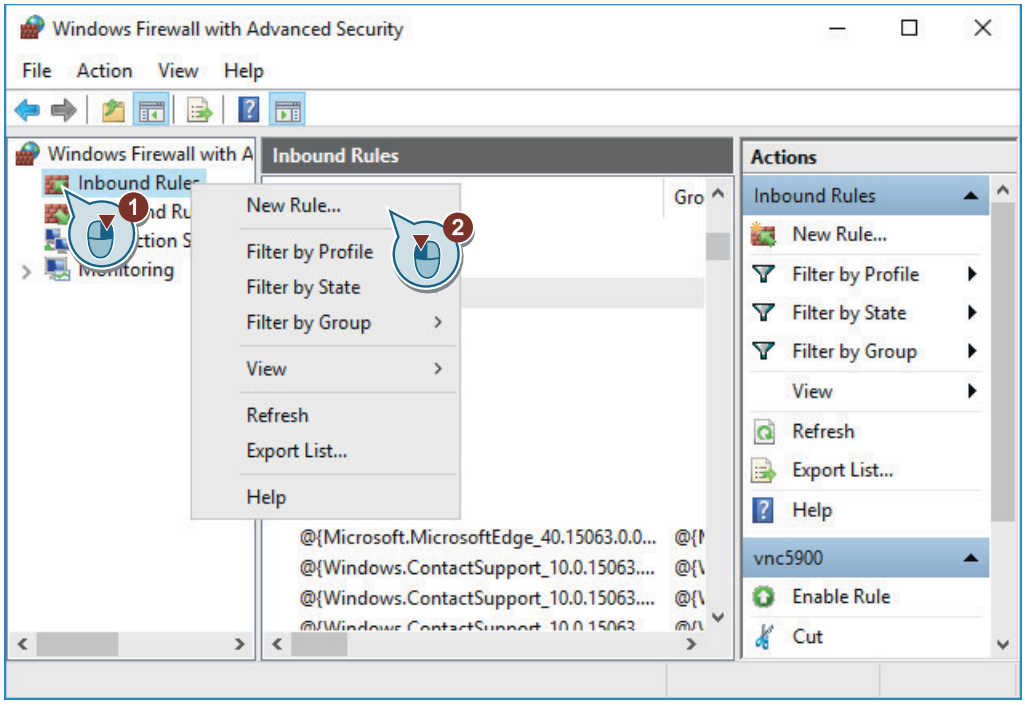
Activation for a specific network profile

Via the Control Panel

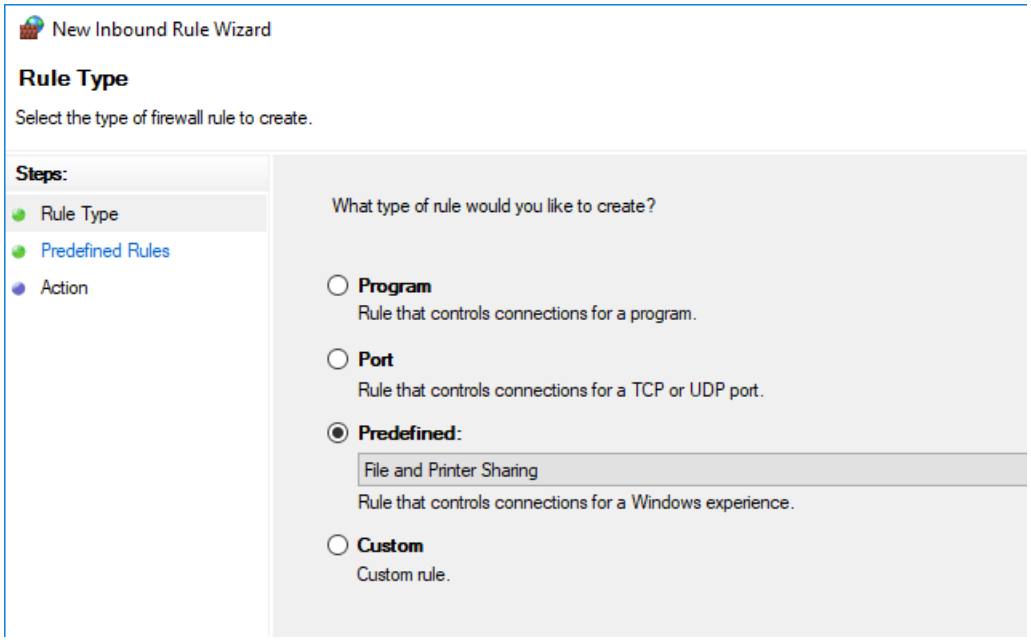
Procedure

From the PG/PC in the company network, proceed as follows to share a file and printer on the MCU-IPC for a specific network profile:

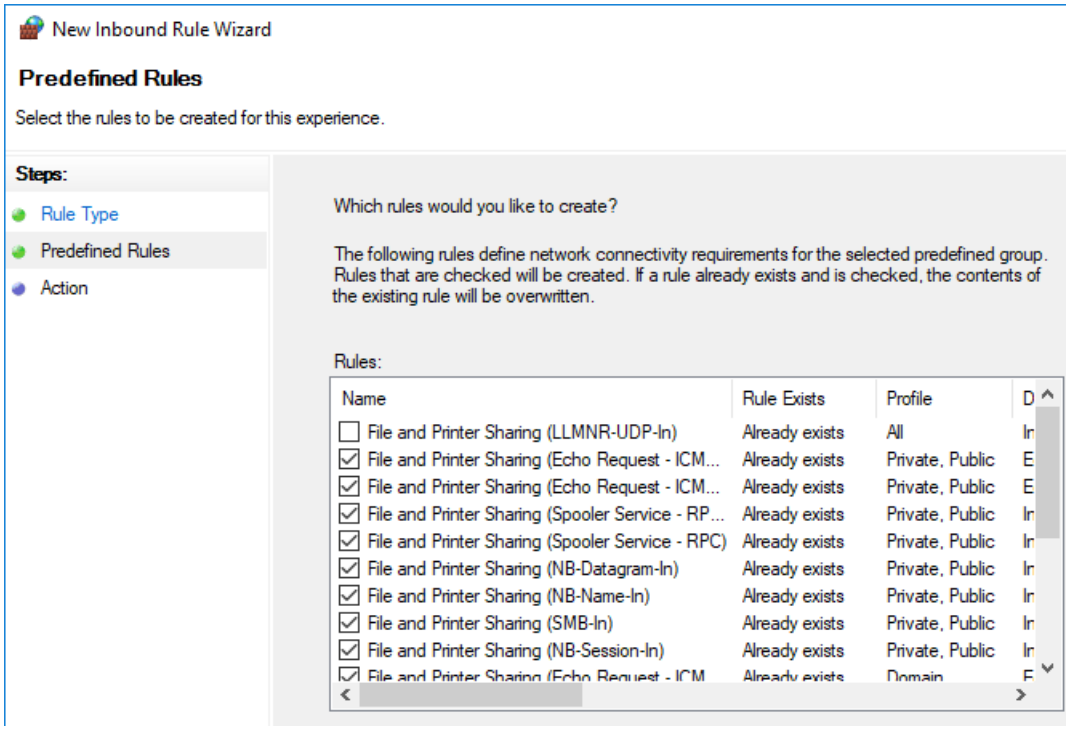
1. Enter "Control Panel" in the search field and then click on "Control Panel" in the search results.
   The desktop App "Control Panel" opens.
2. Click on the display selection and switch from the "Category" view to "Icons".
   The "All Control Panel Items" dialog box opens.
3. Click on "Windows Defender Firewall".
4. Click on "Advanced settings" and confirm the call of the expanded settings with "Yes" if necessary.
5. In the "Windows Defender Firewall with Advanced Security" dialog, right-click on the rule "Inbound Rules", then click on "New Rule..."



6. In the "New Inbound Rule Wizard" dialog, select the option button "Predefined", select in the "File and Printer Sharing" drop-down list, and click on "Next".



7. Depending on the network profile (e.g. Public or Domain) for which the file and printer sharing is to be activated, check the corresponding checkbox.



8. Click on "Next".
9. Select the option button "Allow the connection" and click on "Finish".

By prompt, script or batch file

Basic procedure

Using a command with the following syntax, you can deactivate the blocking of file and printer sharing by the Microsoft Windows Firewall for a special network profile.

To do this, call the prompt as the administrator and enter the command either completely or successively.

Alternatively, you can save the command and the associated parameters in a script file (Page 225).

Syntax for the activation of all firewall rules regarding file and printer sharing

```
netsh
advfirewall firewall
set rule name="File and Printer Sharing (NB-Session-In)" new enable=yes
profile=<profile>
set rule name="File and Printer Sharing (NB-Session-Out)" new enable=yes
profile=<profile>
set rule name="File and Printer Sharing (SMB-In)" new enable=yes
profile=<profile>
set rule name="File and Printer Sharing (SMB-Out)" new enable=yes
profile=<profile>
set rule name="File and Printer Sharing (NB-Name-In)" new enable=yes
profile=<profile>
set rule name="File and Printer Sharing (NB-Name-Out)" new enable=yes
profile=<profile>
set rule name="File and Printer Sharing (NB-Datagram-In)" new enable=yes
profile=<profile>
set rule name="File and Printer Sharing (NB-Datagram-Out)" new enable=yes
profile=<profile>
set rule name="File and Printer Sharing (Spooler Service - RPC)" new
enable=yes profile=<profile>
set rule name="File and Printer Sharing (Spooler Service - RPC-EPMAP)" new
enable=yes profile=<profile>
set rule name="File and Printer Sharing (Echo Request - ICMPv4-In)" new
enable=yes profile=<profile>
set rule name="File and Printer Sharing (Echo Request - ICMPv4-Out)" new
enable=yes profile=<profile>
set rule name="File and Printer Sharing (Echo Request - ICMPv6-In)" new
enable=yes profile=<profile>
set rule name="File and Printer Sharing (Echo Request - ICMPv6-Out)" new
enable=yes profile=<profile>
set rule name="File and Printer Sharing (LLMNR-UDP-In)" new enable=yes
profile=<profile>
set rule name="File and Printer Sharing (LLMNR-UDP-Out)" new enable=yes
profile=<profile>
```

Table 11-10 Description of the Netsh commands in the context of the advfirewall firewall

Command	Parameter	Description	Value
netsh		Specification of the command line program, which executes the following commands.	-
advfirewall		Defines the context in which the following commands are to be carried out.	-
firewall		Subcontext of "advfirewall".	-
set rule		Adaptation of existing firewall rules.	-
	name	Name of the firewall rule in quotation marks.	"File and Printer Sharing (NB-Session-In)" | ...
	new	Specifies that the following parameters are to be changed or added.	-
	enable	Activates or deactivates the specified firewall rule.	yes | no

Example

Example for the activation of all firewall rules regarding file and printer sharing

```
netsh
advfirewall firewall
set rule name="File and Printer Sharing (NB-Session-In)" new enable=yes
profile=public
set rule name="File and Printer Sharing (NB-Session-Out)" new enable=yes
profile=public
set rule name="File and Printer Sharing (SMB-In)" new enable=yes
profile=public
set rule name="File and Printer Sharing (SMB-Out)" new enable=yes
profile=public
set rule name="File and Printer Sharing (NB-Name-In)" new enable=yes
profile=public
set rule name="File and Printer Sharing (NB-Name-Out)" new enable=yes
profile=public
set rule name="File and Printer Sharing (NB-Datagram-In)" new enable=yes
profile=public
set rule name="File and Printer Sharing (NB-Datagram-Out)" new enable=yes
profile=public
set rule name="File and Printer Sharing (Spooler Service - RPC)" new
enable=yes profile=public
set rule name="File and Printer Sharing (Spooler Service - RPC-EPMAP)" new
enable=yes profile=public
set rule name="File and Printer Sharing (Echo Request - ICMPv4-In)" new
enable=yes profile=public
set rule name="File and Printer Sharing (Echo Request - ICMPv4-Out)" new
enable=yes profile=public
set rule name="File and Printer Sharing (Echo Request - ICMPv6-In)" new
enable=yes profile=public
set rule name="File and Printer Sharing (Echo Request - ICMPv6-Out)" new
enable=yes profile=public
set rule name="File and Printer Sharing (LLMNR-UDP-In)" new enable=yes
profile=public
set rule name="File and Printer Sharing (LLMNR-UDP-Out)" new enable=yes
profile=public
```

Activation for a specific connection

Via the Control Panel

Procedure

To activate the file and printer release for a specific connection (e.g. company network), proceed as follows:

1. Enter "Control Panel" in the search field and then click on "Control Panel" in the search results. The desktop App "Control Panel" opens.
2. Click on the display selection and switch from the "Category" view to "Icons". The "All Control Panel Items" dialog box opens.
3. Click on "Network and Sharing Center".

4. Click on the desired connection, e.g. "Local Area Connection 2" (company network).
5. Click on "Properties" and confirm the call of the properties with "Yes" if applicable.
6. In the "Networking" tab, check the checkbox "File and Printer Sharing for Microsoft Networks" and confirm the change with "OK".

By prompt, script or batch file

In Microsoft Windows, enabling file and printer sharing for a specific connection via the command prompt or script/batch file is not supported. However, this is possible using the special command line program "Hyper-V Network VSP Bind (nvspbind)", which is free of charge:

Example: Enabling the file and printer sharing for "Local Area Connection 2" (company network)

```
nvspbind -e "Local Area Connection 2" ms_server
```

More information

More information, for example for nvspbind, is available at Hyper-V Network Microsoft TechNet-Wiki (https://social.technet.microsoft.com/wiki/contents/articles/191.hyper-v-tools-nvspbind.aspx).

11.3.14.9 Activation of the ping execution (ICMP)

Via the Control Panel

In the factory setting state, incoming ping requests are blocked at the company network interface (X1) of the internal PC system. Outgoing ping requests are permitted.

Note

Dependency for the file and printer sharing

If you activated the file and printer sharing in the company network, incoming ping requests are already permitted because they are required for the file and printer sharing.

Procedure

To permit ICMP pings that are received at the company network interface (X1) of the internal PC system, proceed as follows:

1. Enter "Control Panel" in the search field and then click on "Control Panel" in the search results. The desktop App "Control Panel" opens.
2. Click on the display selection and switch from the "Category" view to "Icons". The "All Control Panel Items" dialog box opens.
3. Click on "Windows Defender Firewall".
4. Click on "Advanced settings" and confirm the call of the expanded settings with "Yes" if necessary.

5. In the "Windows Defender Firewall with Advanced Security" dialog, click on "Inbound Rules".
6. Select the corresponding rule for the relevant network profile:
   – File and Printer Sharing (Echo Request - ICMPv4-In) - Profile "Domain"
   – File and Printer Sharing (Echo Request - ICMPv4-In) - Profile "Public"
   – File and Printer Sharing (Echo Request - ICMPv4-In) - Profile "Private"

   In the factory setting state, the network profile "Public" is assigned to the company network.

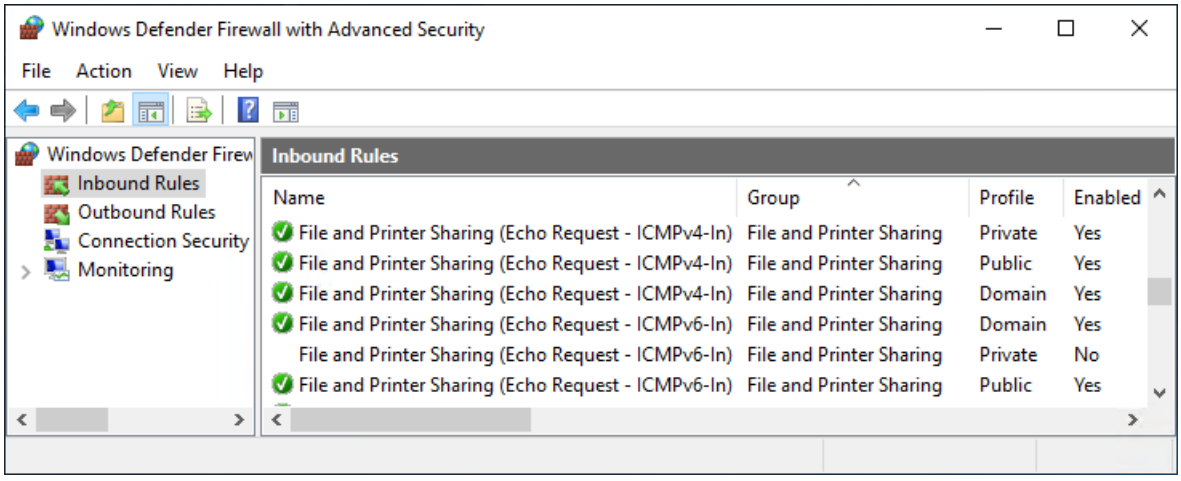


Figure 11-6 Rules for incoming ICMP pings, separate for each network profile

7. Right-click on the selected rule, then click "Enable Rule".

By prompt, script or batch file

Basic procedure

Using a command with the following syntax, you can permit ICMP pings that are received at the company network interface (X1) of the internal PC system. Outgoing pings from the PC system are already activated.

Note

Dependency for the file and printer sharing

If you activated the file and printer sharing in the company network, incoming ping requests are already permitted because they are required for the file and printer sharing.

The name of the relevant firewall rule is "File and Printer Sharing (Echo Request - ICMPv4-In)". To do this, call the prompt as the administrator and enter the command either completely or successively.

Alternatively, you can save the command and the associated parameters in a script or batch file (Page 225).

Syntax for activating a firewall rule via the prompt

```
netsh advfirewall firewall set rule name="<Name of the firewall rule>" new enable=yes
profile=<Name of the network profile>
```

Table 11-11 Description of the Netsh commands in the context of the advfirewall firewall

Command	Parameter	Description	Value
netsh		Specification of the command line program, which executes the following commands.	-
advfirewall		Defines the context in which the following commands are to be carried out.	-
firewall		Subcontext of "advfirewall".	-
set rule		Adaptation of existing firewall rules.	-
	name	Name firewall rule	"File and Printer Sharing (Echo Request - ICMPv4-In)" | ...
	new	Specifies that the following parameters are to be changed or added.	-
	enable	Activates or deactivates the specified firewall rule.	yes | no
	profile	Name of the network profile for which the firewall rule is to be changed.	

Example

Activation of incoming ping requests

```
netsh advfirewall firewall set rule name="File and Printer Sharing (Echo Request - ICMPv4-
In)" new enable=yes profile=public
```

11.3.14.10 Saving and restoring firewall settings

Overview

You can save all Microsoft Windows Firewall settings of the internal PC system as a policy file with file extension ".wfw". Policy files are saved in the binary format, and are dependent on the specific Microsoft Windows version.

You have the following options for backing up or restoring the firewall settings:

- Backup of firewall settings (Page 243)
  - Via the Control Panel (Page 243)
  - By prompt, script or batch file (Page 243)
- Restoring of firewall settings (Page 244)
  You can restore the firewall settings on the same PC system or import the same policy file to different PC systems for the purpose of series commissioning.
  - Via the Control Panel (Page 244)
  - By prompt, script or batch file (Page 245)

Backup of firewall settings

Via the Control Panel

Procedure

To back up the Microsoft Windows Firewall settings of the internal PC, proceed as follows:

1. Enter "Control Panel" in the search field and then click on "Control Panel" in the search results.
   The desktop App "Control Panel" opens.
2. Click on the display selection and switch from the "Category" view to "Icons".
   The "All Control Panel Items" dialog box opens.
3. Click on "Windows Defender Firewall".
4. Click on "Advanced settings" and confirm the call of the expanded settings with "Yes" if necessary.
5. Right-click on the master object "Windows Defender Firewall with Advanced Security on Local Computer" and then click on "Export Policy...".
6. In the "Save As" dialog, select a save location and file name and confirm with "Save".

By prompt, script or batch file

Basic procedure

Using a command with the following syntax, you can back up the Microsoft Windows Firewall settings in a policy file (.wfw).

To do this, call the prompt as the administrator and first define the save location of the policy memory, then enter a file path for backing up the policy file.

Alternatively, you can save the commands and the associated parameters in a script or batch file (Page 225).

Syntax of the Netsh commands for defining the policy memory and for exporting the policy file

```
netsh advfirewall set store local
export <File path and file name>.wfw
```

Table 11-12 Description of the Netsh commands for defining the policy memory and for exporting the policy file

Command	Parameter	Description	Value
netsh		Specification of the command line program, which executes the following commands.	-
advfirewall		Defines the context in which the following commands are to be carried out.	-
set store		Definition of the save location of the policy memory for the following commands.	-
	local	Defines that the work is to be done with the local policy memory.	-
export		Backup of all firewall settings in a policy file (.wfw).	<File path and file name>.wfw

Example

Example of the Netsh commands for defining the policy memory and for exporting the policy file

```
netsh advfirewall set store local
export D:\Backup\DefaultSettings.wfw
```

Restoring of firewall settings

Via the Control Panel

Procedure

Note

Importing a policy file overwrites all existing firewall rules

When the firewall settings are restored, all of the existing firewall rules are overwritten. You cannot undo the import of firewall rules via a policy file.

Therefore, back up (export) the existing firewall settings before you import a policy file.

To restore the Microsoft Windows Firewall settings of the internal PC system, proceed as follows:

1. Enter "Control Panel" in the search field and then click on "Control Panel" in the search results. The desktop App "Control Panel" opens.
2. Click on the display selection and switch from the "Category" view to "Icons". The "All Control Panel Items" dialog box opens.
3. Click on "Windows Defender Firewall".
4. Click on "Advanced settings" and confirm the call of the expanded settings with "Yes" if necessary.
5. Right-click on the master object, then click "Windows Defender Firewall with Advanced Security on Local Computer", then click on "Import Policy..." and confirm the command with "Yes".
6. In the "Open" dialog, select the policy file and confirm with "Open".

By prompt, script or batch file

Basic procedure

Note

Importing a policy file overwrites all existing firewall rules

When the firewall settings are restored, all of the existing firewall rules are overwritten. You cannot undo the import of firewall rules via a policy file.

Therefore, back up (export) the existing firewall settings before you import a policy file.

Using a command with the following syntax, you can restore the Microsoft Windows Firewall settings from a policy file (.wfw).

To do this, call the prompt as the administrator and first define the save location of the policy memory, then enter a file path for backing up the policy file.

Alternatively, you can save the commands and the associated parameters in a script or batch file (Page 225).

Syntax of the Netsh commands for defining the policy memory and for importing the policy file

```
netsh advfirewall set store local
import <File path and file name>.wfw
```

Table 11-13 Description of the Netsh commands for defining the policy memory and for importing the policy file

Command	Parameter	Description	Value
netsh		Specification of the command line program, which executes the following commands.	-
advfirewall		Defines the context in which the following commands are to be carried out.	-
set store		Definition of the save location of the policy memory for the following commands.	-
	local	Defines that the work is to be done with the local policy memory.	-
import		Restoration of firewall settings from a policy file (.wfw).	<File path and file name>.wfw

Example of the Netsh commands for defining the policy memory and for importing the policy file

```
netsh advfirewall set store local
import D:\Backup\DefaultSettings.wfw
```

11.3.15 Using the BitLocker drive encryption

Introduction

The BitLocker is a security feature of Microsoft Windows that provides encryption for all data storage media of the PC system and eliminates the dangers of data theft or disclosure through lost, stolen or inappropriately decommissioned devices. The data storage media can only be used with the assigned PC system. If the data storage media is used in another PC system, all data remains encrypted and cannot be used.

You can set up the BitLocker function via the Control Panel under "BitLocker Drive Encryption". Alternatively, you can configure BitLocker encryption using a script.

Note

The setup for BitLocker drive encryption is deactivated by default on the PC system with the PCU base software /IPC installed. To use BitLocker encryption, activate the setup in Microsoft Windows (Page 247).

NOTICE

Data loss

An active BitLocker always requires a restore password for data storage media decryption in the case of servicing or emergency.

Always save the password **outside the system** to prevent data loss or data misuse.

NOTICE
Unencrypted backup data You can create a backup using a BitLocker-protected data storage medium with the **Paragon Hard Disk Manager**™ application. The backup data are archived unencrypted with the application by default. In the event of data theft, the backup is unprotected and can be manipulated. Protect the backup through manual password encryption.

Note

Remote access to the PC system is not possible when BitLocker is active.

Requirement

The following is a prerequisite for using the Bitlocker functions:

- PCU base software /IPC version 15 SP3 or higher, including Paragon Hard Disk Manager software™ 17 Suite
- Administration rights for the PC system

Displaying the BitLocker status

Open the Microsoft Windows Explorer and click on "This PC". All drives connected to the PC system are displayed.

The status of the Bitlocker encryption is indicated by a lock symbol:



BitLocker active



BitLocker inactive

Note

Other data storage media icons without an integrated lock symbol indicate that Microsoft Windows BitLocker drive encryption is deactivated.

11.3.15.1 Activating BitLocker setup

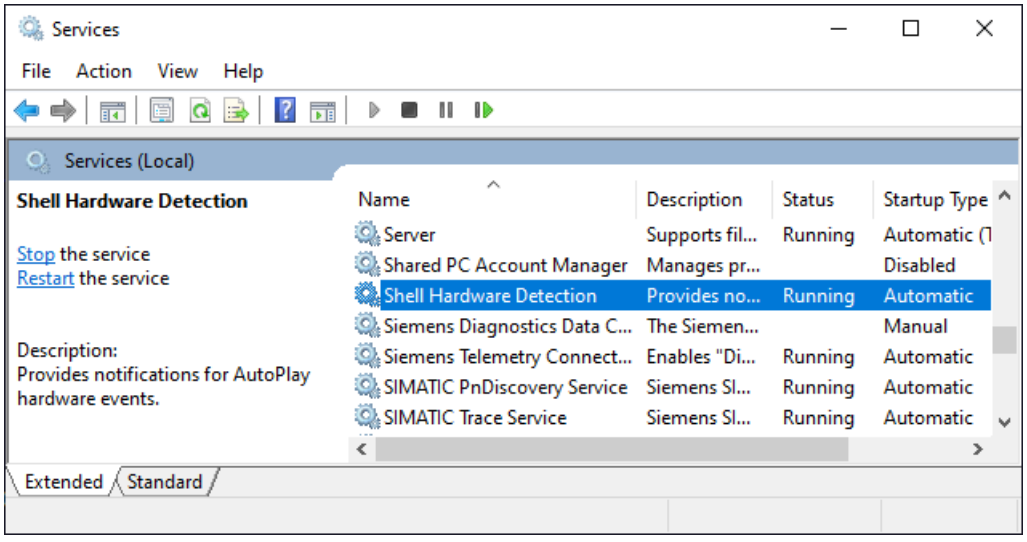
The setup for Microsoft Windows BitLocker drive encryption is disabled by default on the PC system with PCU Base installed. To use the BitLocker setup, activate the corresponding service as follows:

Procedure

1. Enter "services" in the Microsoft Windows search bar and open the Services application with "Run as Administrator".
2. Confirm the confirmation prompt with "Yes".
   The Microsoft Windows Services application opens.
3. In the Extended tab, search for the "Shell Hardware Detection" service and double-click on the entry.
   The "ShellHWDetection" service function opens.
4. In the General tab under "Startup type", switch to "Automatic" and click "Start".
   The service is activated.
5. Confirm the setting with "Ok".

Result

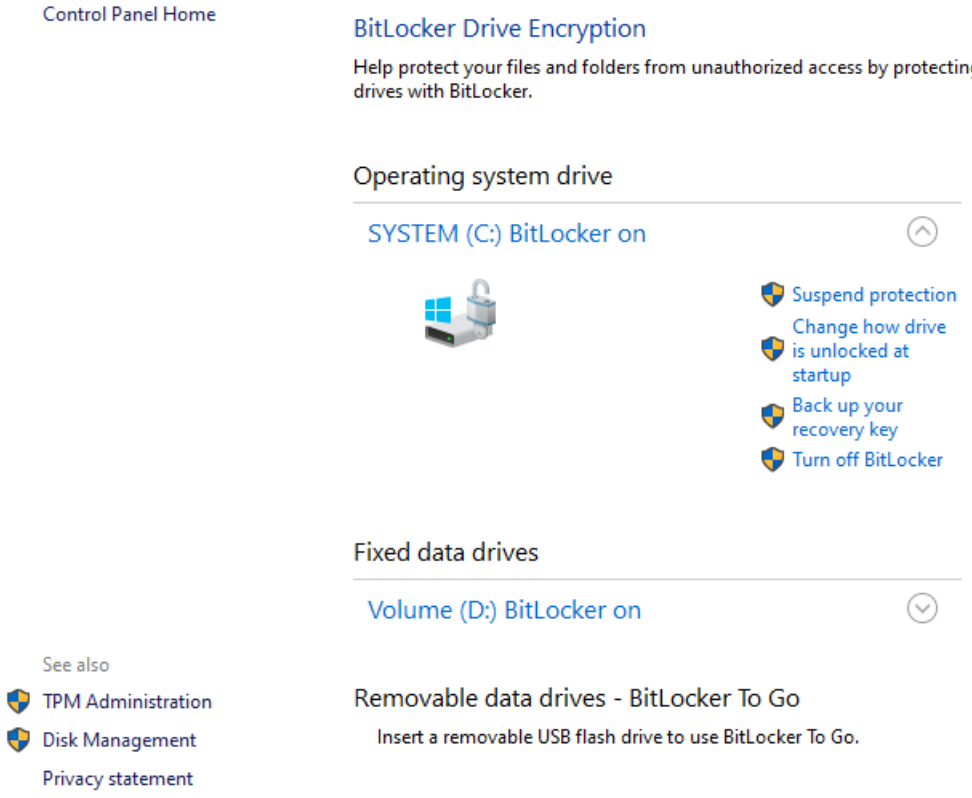
The "Shell Hardware Detection" is active. "Running" appears in the Status column.



The setup is active, BitLocker drive encryption can now be used under Microsoft Windows.

11.3.15.2 Configuring BitLocker via Microsoft Windows

With the Microsoft Windows user interface **BitLocker Drive Encryption**, you can set up BitLocker encryption for each drive individually. Each drive receives its own encryption and recovery password. The BitLocker Drive Encryption user interface is an application from the Control Panel.



Procedure

1. The PC system has started up, you are logged in.
2. Open the Microsoft Windows Explorer and click on "This PC".
   All drives connected to the PC system are displayed.
3. In the drive overview, right-click on the drive, then on "Manage BitLocker".
   - or -
   If no BitLocker is active, select "Turn on BitLocker" and follow the instructions.
   The BitLocker Drive Encryption user interface opens.
4. Configure the drive:
   - Activate BitLocker, e.g. after an SSD backup has been restored on the IPC with Paragon.
   - Save the recovery key on **an external data storage medium**, e.g. on a USB flash drive.
   - Deactivate BitLocker if you do not need protection.

More information on BitLocker encryption can be found under Microsoft Learn (https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/).

Result

BitLocker encryption is active/inactive separately for each drive in the PC system.

11.3.15.3 Configuring BitLocker using a script

You have the option of using a script with which you can automatically protect the drives of the PC system with the same Bitlocker encryption, e.g. for series commissioning. A uniform recovery password applies to the drives.

You will find the BitLocker script example for your configuration in the annex (Page 315).

NOTICE
Data loss Always save the script and the recovery password **outside the system** to prevent data loss or misuse.

Creating a script file

1. Open a text editor.
2. Copy the **BitLocker script example** (Page 315) in the annex into the text editor.
3. Save the script example as a ps1 file (character encoding ASCII or ANSI) on a USB flash drive, for example:
   `E:/enableIPCBitlocker.ps1`
4. Close the script.

Applying the script file

1. Open the **Microsoft Windows PowerShell** application. Enter the term "powershell" in the search field and open the application as administrator.
   The Microsoft Windows PowerShell application opens.
2. Enter the following command in PowerShell:
   `Set-ExecutionPolicy -Scope Process -ExecutionPolicy Unrestricted`
   A confirmation prompt is displayed.
3. Respond to the confirmation prompt with "Y" for yes.
   The provisions for script usage are changed.

4. Navigate to the storage directory of the script file, e.g. on the USB flash drive with the following command:
   `e:`
   PowerShell displays drive E: `E:\>`
5. Enter the following command for BitLocker activation in PowerShell:
   `.\enableIPCBitlocker -RecoveryPasswordFile "E:\BitlockerRecoveryPassword.txt"`
   BitLocker encryption is activated and a random recovery password is saved as TXT file:
   `E:/BitlockerRecoveryPassword.txt`

Result

BitLocker encryption is active for the drives in the PC system.

The uniform recovery password applies to the drives.

Note

Use the **Service Center** (Page 287) if you wish to deactivate BitLocker encryption.

11.4 Installing and configuring updates and automation software

11.4.1 Overview

After you have completed the installation of PCU-Basesoftware /IPC and configured the network settings as required, you can set up the handling of security updates, patches and software installations or install them directly.

- Information about Microsoft Windows updates and network security of an automation system is provided in Chapter Patch management and security updates (Page 252).
- The PCU Installer (Page 257) will assist you with automatic installation of setup packages.
- To prevent the operating software from being interrupted by key combinations such as CTRL+ALT+DEL, you can activate and configure the key filter (Page 253).
- If you want to transfer existing data to the newly installed automation software, read Chapter Creating and importing archives using SINUMERIK ONE Commissioning (Page 179).

11.4.2 Patch management and security updates

Microsoft regularly eliminates security vulnerabilities in Microsoft Windows 10, and makes these updates available on its "Windows Update" website.

"Start > Settings > Update & Security"

As a solution for managing and making Microsoft Windows updates available in a network, Microsoft offers the components in the Microsoft Update Catalog (http://www.catalog.update.microsoft.com).

Industrial cybersecurity

Information about network security for an automation system and a comprehensive protection concept under industrial cybersecurity is provided on the SIEMENS website:

Industrial cybersecurity (https://www.siemens.com/industrialsecurity)

SINUMERIK-specific information is also available in the following documentation:

SINUMERIK/SIMOTION/SINAMICS Configuration Manual Industrial Security (https://support.industry.siemens.com/cs/document/108862708?lc=en-WW)

Compatibility with automation software

Information about the compatibility of a Microsoft Windows update with specific application software of SIEMENS may possibly be available on the product pages of the application software involved in the Service&Support portal:

SiePortal (https://support.industry.siemens.com/)

Generally, it is recommended that you check the compatibility of updates in a dedicated project test environment before installing it in a productive environment.

11.4.3 Configuring saving Windows log files

As a result of Microsoft Windows updates and other operations, larger quantities of data can accumulate that are no longer required, e.g. temporary update and system files or Microsoft Windows log files (`CBS.log`).

PCU-Basesoftware /IPC contains 2 batch files, which you can use to configure how files such as these are saved:

- Deactivate saving
  - Saving new log files `CBS.log` is deactivated, and existing files are deleted: `C:\Windows\Logs\CBS`
  - The temporary directory is cleared once: C:\Windows\Temp
  - The data storage medium cleanup is carried out.
- Activate saving
  - Reactivates that new log files `CBS.log` are saved for diagnostics.

You can refer to the information file in the following directory to identify whether the log files are being saved or not: `C:\Windows\Logs\CBS`

Requirement

- You require administrator rights to run batch files.

Procedure

1. Switch to directory `D:\etc .`
2. Double-click on the appropriate batch file.

11.4.4 Configuring a key filter for HMI software

To prevent unwanted interruption of the operating software, you can specify that certain keyboard entries are filtered out and therefore ignored.

You can configure the key filter in the pcuhwsvc.ini configuration file:

- This key filter is not activated as delivered.
- You can activate the key filter and individually select which of the 20 filterable keyboard entries will be ignored. During this, you can deactivate known shortcut keys, for example, or even deactivate individual add-on keys, such as the left (SeqActive_16) or right (SeqActive_17) Windows key.
  You cannot configure any additional keyboard entries to be filtered.
- You can also completely deactivate the repeat function of the F1-F12 keys and all hard keys with the key filter. When the repeat function is deactivated, a key held pressed is considered as pressed once and not as pressed repeatedly.
  Per default, the repeat function is activated during Service or Desktop operation.

Precondition

- The Microsoft Windows Service Desktop is active
- Hidden directories are visible
  Further information: Directory structure and file conventions (Page 198)

Procedure

To configure the key filter, proceed as follows:

1. Switch to the template directory: `C:\ProgramData\Siemens\MotionControl\siemens\System\etc\`
   The settings can be viewed in the template `pcuhwsvc.ini`.
2. Save a copy of the template `pcuhwsvc.ini` to one of the user directories:
   - `C:\ProgramData\Siemens\MotionControl\user\System\etc\`
   - `C:\ProgramData\Siemens\MotionControl\oem\System\etc\`
   - `C:\ProgramData\Siemens\MotionControl\addon\System\etc\`
3. In the new file (e.g. `...\oem\System\etc\pcuhwsvc.ini`), delete all data except for the section name `[KEYB_FILTER]` and the keys that are to differ from the template.
   All data and keys that do not occur in your file are automatically taken over from the template in the `siemens` directory.
4. Save your file.

Example: Activating the key filter, but allowing use of the NUM-lock key.

This example activates the key filter (`KeySequencesEnable = 1`) and filters all possible keyboard entries except the NUM-lock key.

`KEYB_FILTER`	Section name (mandatory):
`KeySequencesEnable = 1`	Activate key filter
`SeqActive_19= 0`	Do not filter NUM-lock key

In the adapted file in the user directory (e.g. `...\oem\System\etc\`) therefore only the section name `[KEYB_FILTER]` is mandatory as well as the settings that you want to adapt. All other settings and values are taken over from the template.

Template of the key filter in the delivery condition

The template is located in directory `C:\ProgramData\Siemens\MotionControl\siemens\System\etc\`

Do not overwrite this template, but save a copy of this template `pcuhwsvc.ini` in one of the user directories.

- `C:\ProgramData\Siemens\MotionControl\`**`user`**`\System\etc\`
- `C:\ProgramData\Siemens\MotionControl\`**`oem`**`\System\etc\`
- `C:\ProgramData\Siemens\MotionControl\`**`addon`**`\System\etc\`

How the configuration file works

You can configure the key filter in section `[KEYB_FILTER]`. The lines identified by a number sign (#) are comments as to which line further down deactivates a particular keyboard entry.

- To activate a particular keyboard entry, find the key in the comment and then set the value to 0.
- To allow all keyboard entries and thus deactivate the key filter (factory setting), set the value to 0 in the `KeySequencesEnable` key.
  If the value 0 is set for this key, all other keys will be ignored and the key filter is deactivated.
- To completely deactivate the repeat function of the F1-F12 keys and all hard keys, set the value 1 at the `AutorepeatSuppression` key.

Table 11-14 Overview: Key filter in the configuration file pcuhwsvc.ini

Section	[KEYB_FILTER]
Key	SeqActive_x
Value	0 = specific keyboard entry activated 1 = specific keyboard entry will be filtered and is deactivated
Factory setting	1

pcuhwsvc.ini (Vorlage im Verzeichnis ...\siemens\System\etc)

```
[GLOBAL]
# ------------------------
# SIEMENS GLOBAL SECTION
# ------------------------
# enable logfile PCUHardwareservice.log
EnableLogFile=0
#  Emulating of "Mode-Switch" from Sinumerik PCU50 Box.
# "Mode-Switch" is a rotary switch, which is attached to the rear side of the PCU50 V5 Box.
#  About this, different methods of booting the computer are controlled.
# 0  Normal mode
# 3  Desktop mode (welcome screen)
ModeSwitch=0
[SERVER]
FTP=hmisvr_PCU_betaftpd
DHCP=hmisvr_PCU_udhcpd
TFTP=hmisvr_PCU_netkit-tftpd
TCUHWS=hmisvr_TCU_hardware_services
VNC=uvnc_service

[APPLICATION]
# ---------------------------------------
# STARTUP APPLICATION DIAGNOSTIC SECTION
# ---------------------------------------

[KEYB_FILTER]
```

pcuhwsvc.ini (Vorlage im Verzeichnis ...\siemens\System\etc)

```
# ----------------------------------------
# SIEMENS KEYBOARD-FILTER DRIVER SECTION
# ----------------------------------------

# Filtering Key Sequences
# =======================
# Activation of Key-Sequences to be ignored
# SeqAct_x
# The following 20 sequences are implemented
# 0  CTRL-ALT-DEL
# 1  ALT-F4
# 2  ALT-TAB
# 3  LEFTSHIFT-ALT-TAB
# 4  RIGHTSHIFT-ALT-TAB
# 5  CTRL-ESC
# 6  ALT-ESC
# 7  ALT-SPACE
# 8  (SHIFT)-CTRL-F1
# 9  (SHIFT)-CTRL-F2
# 10 (SHIFT)-CTRL-F3
# 11 (SHIFT)-CTRL-F4
# 12 (SHIFT)-CTRL-F5
# 13 (SHIFT)-CTRL-F6
# 14 (SHIFT)-CTRL-F7
# 15 (SHIFT)-CTRL-F8
# 16 M$_1
# 17 M$_2
# 18 CAPSLOCK
# 19 NUMLOCK
# 20 (reserved)

KeySequencesEnable = 0

SeqActive_0= 1
SeqActive_1= 1
SeqActive_2= 1
SeqActive_3= 1
SeqActive_4= 1
SeqActive_5= 1
SeqActive_6= 1
SeqActive_7= 1
SeqActive_8= 1
SeqActive_9= 1
SeqActive_11= 1
```

pcuhwsvc.ini (Vorlage im Verzeichnis ...\siemens\System\etc)

```
SeqActive_12= 1
SeqActive_13= 1
SeqActive_14= 1
SeqActive_15= 1
SeqActive_16= 1
SeqActive_17= 1
SeqActive_18= 1
SeqActive_19= 1
SeqActive_20= 1

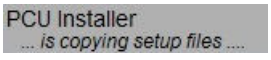
# Autorepeat-Suppression of Function Keys F1-F12 and Hardkeys
#============================================
AutorepeatSuppression = 0
```

11.4.5 PCU Installer

11.4.5.1 Overview

The PCU Installer assists you with the installation of setup packages on PC systems:

- The PCU Installer checks definable setup directories on the PC system, on removable data storage media, or in the network.
  These setup directories must not be write-protected.
- If setup packages exist, they are automatically installed one after the other. The order in which these packages are installed can be parameterized (Page 261).
- On the top right of the screen, a status display is displayed while the PCU Installer carries out such activities.



For further information on the activities of the PCU Installer, see Chapter Procedure example of an installation with the PCU Installer (Page 266).

Overview of the configuration and operation

- In the delivery state of PCU-Basesoftware /IPC, the PCU Installer is disabled. You can activate the PCU Installer during the unsupervised installation of PCU Base for IPC via the response file or activate it manually after the supervised installation (Page 258).
- After you have made all of the settings for the PCU Installer, using program application Configure for CMC you can also activate or deactivate the PCU Installer (Page 268).
- You can make all settings in the PCU Installer in the associated configuration file (Page 261).

- Copy the setup packages to the defined directories to start the installation (Page 266).
- The PCU Installer consists of a client and a service, whereby setup packages can also be installed for a user account without administrator rights.

11.4.5.2 Activating the PCU Installer

Overview

In the delivery condition of the PCU-Basesoftware /IPC, the PCU Installer is deactivated.

If you are supervising the installation of PCU-Basesoftware /IPC with Microsoft Windows 10, then you must manually activate PCU Installer. To do this, use one of the following procedures:

- Copy a preconfigured template of the PCUInst.ini to the "user" directory (Page 258)
- Create your own version of the PCUInst.ini in one of the user directories and set the appropriate values
  See: Reference to the PCUInst.ini configuration file (Page 261)

Activating via a configuration template

Precondition

- The PCU Installer is deactivated
- The Service Desktop is active
- The PCU Installer has not been configured yet and there is no adapted PCUInst.ini configuration file

Procedure

To activate the PCU Installer by copying a preconfigured template, proceed as follows:

1. Copy the following file to the clipboard: `D:\etc\Template_PCUInst.ini`
2. Paste the file into the following directory: `C:\ProgramData\Siemens\MotionControl\user\system\etc`
3. Rename the copied file to PCUInst.ini

Result

The PCU Installer was activated and checks the setup directories while the PC system runs up, but not while the system is operational.

The copied configuration file only differs from the default configuration file by the following value:

```
[processing_loginphase]

StartState=activated
```

The settings of the copied configuration file are used because they are in a directory with higher priority than the default configuration file.

See: Directory structure and file conventions (Page 198)

To also use the PCU Installer during system operation, you must make an additional setting in the copied configuration file (Page 261):

```
[processing_systemphase]
StartState=activated
```

11.4.5.3 Deactivating the PCU Installer

In the delivery state of PCU-Basesoftware /IPC, the PCU Installer is disabled.

Note

Troubleshooting for incorrect installation routines

If completion of an installation requires a restart, but the installation cannot be completed after the restart, the Service Desktop is not started.

In this case, restart the internal PC system in the protected mode to prevent the PCU Installer from starting.

Then reconfigure the PCU Installer or remove the setup packages.

Requirement

- The Service Desktop is active
- Hidden directories are visible (at least `C:\ProgramData\`)
  Further information: Directories hidden in delivery condition (Page 198).
- A copy of the `PCUInst.ini` configuration file is stored in the `user` directory:
  `C:\ProgramData\Siemens\MotionControl\`**`user`**`\System\etc\PCUInst.ini`
- The `PCUInst.ini` configuration file in the `user` directory is not write-protected

Procedure

To partly or completely deactivate the installation of the setup files by means of the PCU Installer, proceed as follows:

1. Open the `PCUInst.ini` configuration file in the `C:\ProgramData\Siemens\MotionControl\`**user**`\System\etc\PCUInst.ini` directory.
2. Deactivate the start of the PCU Installer in the desired phase:
   - To deactivate the PCU Installer during system operation, change the relevant key value in the `[processing_systemphase]` section: `StartState=stopped`.
   - To only deactivate the PCU Installer while a specific application is being executed (e.g. SINUMERIK ONE Commissioning), enter the file name of the relevant application in the `[noactivation]` section, e.g. `APP001=run_hmi.exe`.
     (You can specify any number of applications, e.g. `APP002=Siemens.Automation.Portal.exe`)
   - To deactivate the PCU Installer during run-up, change the relevant key value in the `[processing_loginphase]` section: `StartState=stopped`.
3. Save and close the file.

More information

- For information on all configuration options, see Reference to the PCUInst.ini configuration file (Page 261).
- Microsoft Windows support: Start Windows 10 in the safe mode (https://support.microsoft.com/en-us/help/12376/windows-10-start-your-pc-in-safe-mode)

11.4.5.4 Copying and adapting the configuration file

You can define PCU Installer operation in the associated configuration file. To do this, you must first copy the configuration file to a user directory.

Alternatively, you can copy a template in which the PCU Installer has already been activated (Page 258).

For example, you can configure the following in the configuration file:

- Which directories have been checked how many times for new setup packages.
- That installations are not started automatically while certain software is active.

A list of all setting options can be found under Reference to the PCUInst.ini configuration file (Page 261).

Precondition

- The Service Desktop is active
- The PCU Installer has not been configured yet and there is no adapted PCUInst.ini configuration file

Procedure

To copy and adapt the configuration file of the PCU Installer, proceed as follows:

1. Switch to the template directory: `C:\ProgramData\Siemens\MotionControl\siemens\System\etc\`
   The settings can be viewed in the template `PCUInst.ini`.
2. Save a copy of the template `PCUInst.ini` to one of the user directories:
   - `C:\ProgramData\Siemens\MotionControl\user\System\etc\`
   - `C:\ProgramData\Siemens\MotionControl\oem\System\etc\`
   - `C:\ProgramData\Siemens\MotionControl\addon\System\etc\`

   Note

   Storage of the configuration file in the setup directory

   Alternatively, a configuration file can also be located directly with an installation setup.

   In other words, if, for example, `E:\Setup` is a setup directory, this (or one of the direct subdirectories) can be the location of a configuration file. Settings made in this configuration file have a higher weighting than the settings in configuration files in the above-mentioned directories.

3. Adapt the values of the keys. You will find information about the syntax and setting options at Reference to the PCUInst.ini configuration file (Page 261) or in the comments of the configuration file.

   Note

   The factory setting is taken if key pairs are missing

   All key pairs that are not available in your file are taken automatically from the template in the `siemens` directory.

   Therefore, in the new file (e.g. `...\oem\System\etc\PCUInst.ini`), delete all the data except the section names and the keys that are to differ from the template.

   Further information: Directory structure and file conventions (Page 198), Reference to the PCUInst.ini configuration file (Page 261)

4. Save and close the file.

Result

The configuration file has been copied to a user directory and can be adapted.

Further information on the various setting options is provided in the following Chapters.

11.4.5.5 Reference to the PCUInst.ini configuration file

You can define PCU Installer operation in the associated `PCUInst.ini` configuration file.

For example, you can configure the following:

- Which directories have been checked how many times for new setup packages.
- That installations are not started automatically while certain software is active.

The priority concept of this configuration file is the same as that of the other configuration files. **More information:** Directory structure and file conventions (Page 198)

You can also deactivate settings in `PCUInst.ini` by deleting the value of the key in the higher priority configuration file. For example, to deactivate `DIR002=C:\Setup` in a file of lower priority, enter `DIR002=` in the file with higher priority.

Note

Maximum length of the file path

The file path to a setup must not exceed 255 characters (including the file name).

Table 11-15 Setting options in the configuration file of the PCU Installer

Section	Setting	Description

`[local_setupdirs]`	`DIR001=`
	`DIR002=`
	`...`
		Specifies the local setup directories on the internal PC system to be checked.
		The directories must not be write-protected.
		You can specify several directories, which are then checked in the specified order.
		You define the order with a number after "`DIR`".
		Subdirectories at the first level are also scanned.

`[removable_ setupdirs]`	`DIR001=`
	`DIR002=`
	`...`
		Specifies the setup directories on removable data storage media to be checked.
		The directories must not be write-protected.
		You can specify several directories, which are then checked in the specified order.
		You define the order with a number after "`DIR`".
		Subdirectories at the first level are also scanned.
		If you do not know the drive letters to be checked, use the `<REMOVABLE_MEDIA>` drive variable, e.g.:
		`DIR001=<REMOVABLE_MEDIA>:\Install`
		The drive variable then represents all the interchangeable data storage media that are known at the time in Microsoft Windows. You can also specify fixed drive letters without the directories being checked twice.
		The drive variable is only valid in the [removable_setupdirs] section.

`[net_setupdirs]`	`DIR001=`
	`DIR002=`
	`...`
		Specifies the setup directories on network drives to be checked.
		The directories must not be write-protected.
		More information: Creating a shortcut to the network drive (Page 300)
		You can specify several directories, which are then checked in the specified order.
		You define the order with a number after "`DIR`".
		Subdirectories at the first level are also scanned.

Section	Setting	Description
[setupdirs_ settings]	deleteTmpLocal SetupDirs=	Temporary directories are created during installation of a setup from a removable data storage medium, network drive or the default setup directory D:\Install **More information:** Procedure example of an installation with the PCU Installer (Page 266) Here you can specify whether these temporary directories are to be deleted again after installation. Possible values: yes; no
	keepDInstall SubdirsWithPrefix=	You can specify that subdirectories of D:\Install with a particular prefix in the directory name are not to be deleted after setup is completed.
[setupnames]	NAME001= NAME002= ...	Specifies which files are setup packages and are to be included in the check of setup directories. You can specify entire file names with their file extensions or represent individual parts of them with wildcard character *.
[setupexecution]	checkSetupLogFile=	Specifies whether a check is to be performed as to whether the file has already been installed before the installation of a setup file. The check is performed based on the computer name and the setup name of the setup-specific log file. Possible values: yes; no
	copyToTmp LocalSetupDir=	You can specify whether setup files on removable data storage media are to be copied to a temporary, local directory before installation. Setup files on network drives are always copied before installation. Possible values: yes; no
[noactivation]	APP001= APP002=	Specifies which applications of the PCU Installer are inactive during operation. This setting is required to prevent operation of the HMI software or another application from being interrupted during execution of a setup.

Section	Setting	Description
[processing_ loginphase]	StartState=	Specifies whether the PCU Installer is active before the Desktop run-up. The setting StartState=activated is required, in particular, if an installation requires a cold start. Possible values: • activated PCU Installer starts setups • stopped PCU Installer is stopped completely
	continueSetups=	Some setups can only be completed after the system has been restarted. In this case, the PCU Installer waits until you restart the internal PC system. Here, you can specify whether setups such as these should be continued after a restart. **More information:** Note: Troubleshooting for incorrect installation routines (Page 266) Possible values: yes; no
	scanSetupDirs=	Specifies whether setup directories are to be checked and, if required, setup files executed before the Desktop run-up. The following directories are checked if this setting has been activated: • Local setup directories from the [local_setupdirs] setting are always checked. • You can define separately whether additional directories on removable data storage media or in the network are to be checked. (See settings "scanRemovableDriveSetupDirs" and "scanNetworkDriveSetupDirs") If you deactivate this setting, neither local directories, nor directories on removable data storage media or in the network are checked, i.e. the setting scanSetupDirs=no overwrites, for example, scanNetworkDriveSetupDirs=yes. Possible values: yes; no
	scanRemovableDrive SetupDirs=	Specifies whether directories on removable data storage media are to be checked from the setting [removable_setupdirs] and, if required, setup files executed before the Desktop run-up. The setting "scanSetupDirs" must also be activated so that these directories are checked. Possible values: yes; no
	scanNetworkDrive SetupDirs=	Specifies whether network directories are to be checked from the setting [net_setupdirs] and, if required, setup files executed before the Desktop run-up. The setting "scanSetupDirs" must also be activated so that these directories are checked. Possible values: yes; no
	waitTimeDevicesDetection=	Specifies the maximum wait time for device detection (removable data storage media) in the system run-up. This setting is only relevant if the PCU Installer searches for setups on removable data storage media prior to the desktop run-up. (See settings "scanSetupDirs", "scanRemovableDriveSetupDirs" in the section [processing_loginphase] and section [removable_setupdirs]) Possible values: • Positive integer (milliseconds) • infinite
	waitTimeDriveLettersAssignment=	Specifies how long the PCU Installer will wait during the system run-up until the system has assigned a drive letter to all of the logical drives. This setting is only relevant if the PCU Installer searches for setups on removable data storage media prior to the desktop run-up. (See settings "scanSetupDirs", "scanRemovableDriveSetupDirs" in the section [processing_loginphase] and section [removable_setupdirs]) Possible values: • Positive integer (milliseconds) • infinite

Section	Setting	Description
[processing_ systemphase]	StartState=	Specifies whether the PCU Installer is active during operation of the Desktop. Possible values: • activated PCU Installer starts setups • stopped PCU Installer is stopped completely You can define exceptions in Section [noactivation].
	scanSetupDirs=	Specifies whether setup directories are to be checked and, if required, setup files executed during Desktop operation. The following directories are checked if this setting has been activated: • Local setup directories from the [local_setupdirs] setting are always checked. • You can define separately whether additional directories on removable data storage media or in the network are to be checked. (See settings "scanRemovableDriveSetupDirs" and "scanNetworkDriveSetupDirs") If you deactivate this setting, neither local directories, nor directories on removable data storage media or in the network are checked, i.e. the setting scanSetupDirs=no overwrites, for example, scanNetworkDriveSetupDirs=yes. Possible values: yes; no
	scanRemovableDrive SetupDirs=	Specifies whether directories on removable data storage media are to be checked from the setting [removable_setupdirs] and, if required, setup files executed during Desktop operation. The setting "scanSetupDirs" must also be activated so that these directories are checked. Possible values: yes; no
	scanNetworkDrive SetupDirs=	Specifies whether network directories are to be checked from the setting [net_setupdirs] and, if required, setup files executed during Desktop operation. The setting "scanSetupDirs" must also be activated so that these directories are checked. Possible values: yes; no
	numberOfScanCycles	Specifies whether and how often the setup directories check for new setup packages. Possible values: • infinite Infinite • Integer You can define the waiting time between checks in key waitTimeBetweenScanCycles
	waitTimeBetween ScanCycles	Specifies how long the PCU Installer waits after the setup directories have been checked before checking them again. Enter the waiting time in milliseconds. In key numberOfScanCycles, you can specify how often the setup directories will be checked.
report	InfoLevel	Specifies how detailed the information is to be which is stored in the log files. Possible values: • 1: Only basic information on the actions of the PCU Installer is logged • 2: All PCU Installer-specific information is logged • 3: All PCU Installer-specific information and some trace information is logged • 4: All PCU Installer-specific information and additional trace information is logged • 5: All PCU Installer-specific information and all trace information is logged

11.4.5.6 Installing software with the PCU Installer

Precondition

- The PCU Installer is activated
- If you want to install multiple setup packages one after the other, you must have defined multiple setup directories in the configuration file
- The setup directories to be used are empty and not write-protected

Procedure

To make the PCU Installer accessible to setup packages, proceed as follows:

1. Copy the setup packages to be installed into the setup directories. Copy each setup package into a separate directory.

   Note

   Maximum length of the file path

   The file path to a setup must not exceed 255 characters (including the file name).

Result

The installation of the setup packages is started.
After a setup has been completed or cancelled, a specific log file is stored in the associated setup directory. The general log files of the PCU Installer are also supplemented in the log directory.

More information

- Log files (.log) (Page 267)
- Procedure example of an installation with the PCU Installer (Page 266)

Note

Troubleshooting for incorrect installation routines

If completion of an installation requires a restart, but the installation cannot be completed after the restart, the Service Desktop is not started.

In this case, restart the internal PC system in the protected mode to prevent the PCU Installer from starting.

Then reconfigure the PCU Installer or remove the setup packages.

11.4.5.7 Procedure example of an installation with the PCU Installer

The following example describes the activities of the PCU Installer if you have stored a setup file on a removable data storage media or network drive after the activation and configuration of the PCU Installer.

In this procedure example, it is assumed that you have already performed the following steps:

- You have activated the PCU Installer
- You have activated the checking of the network directories in the settings of the PCU Installer and defined an additional setup directory on a network drive.
  In the example: F:\Setup with F: as network drive.
- You have stored a setup file in this additional setup directory (e.g. F:\Setup\Update.exe).
- The setup directory is not write-protected.

Example: Activities of the PCU Installer during installation of a network drive

- The defined setup directories are checked.
- The Update.exe file is found in the F:\Setup directory.
  As the Update.exe file has not been installed yet, there is no setup-specific log file in the directory.
- The Update.exe file is copied to a local temporary directory, e.g. D:\Install39\Update.exe
- The copied setup file is executed from the local temporary directory, e.g. D:\Install39\Update.exe.
- Log files are created after completion of the installation:
  - The general log files are extended
  - The setup-specific log file is created in the original setup directory F:\Setup and in the local temporary directory D:\Install39

  Further information: Log files (.log) (Page 267)

11.4.5.8 Log files (.log)

In order to be able to track which setup packages and updates have been installed at any time, the activities of the PCU Installer are recorded in various log files.

Setup-specific log files

A separate setup-specific log file is created for each setup package that is executed by the PCU Installer. The name of the setup and the name of the computer are entered in the file name of the log.

Archiving	The setup directory in which the associated setup file was originally located, and (if copied by the setup) the local temporary directory.
File name	The log file is designated according to the following scheme: <name of the setup file>@<computer name>.log, e.g. Update@MyIPC.log

If you activate the checkSetupLogFile= setting in the "PCUInst.ini" configuration file (Page 261), then the setup-specific log file prevents the same setup being installed several times on the same computer. The check is performed based on the computer name and the setup name.

In the delivery condition of the base software, this setting is deactivated. The setting should remain deactivated for the series start-up of devices with the same name or for the repair of an installation.

General log files

The general PCU Installer log files record the operation and the communication of the PCU Installer client and PCU Installer service. There are therefore separate files for the client and service.

Archiving	`C:\ProgramData\Siemens\MotionControl\User\System\Log\`
File name	PCU Installer client: `PCUInstaller_C.log`
	PCU Installer service: `PCUInstaller_S.log`

11.4.5.9 Program application Configure for CMC

Overview

Using Configure for CMC you can activate or deactivate the PCU Installer, and therefore execute setup packages on the internal PC system, removable data storage medium or network without having to make any manual changes to `PCUInst.ini`.

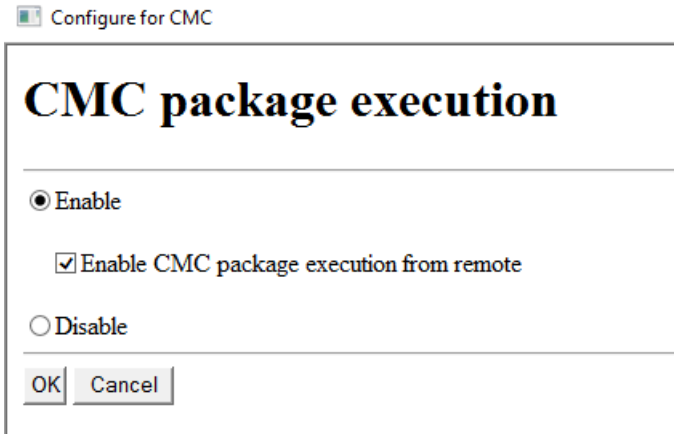


Figure 11-7 Program application Configure for CMC

Precondition

- The PCU Installer was configured.
- An adapted configuration file `PCUInst.ini` exists.

Procedure

1. Open the program application using icon "Configure for CMC" on the desktop.
2. Using the option box, activate or deactivate the check for setup packages.
3. Confirm with OK to accept the setting.
   The setting becomes active after restarting Windows.

11.5 Backing up and restoring data

11.5.1 Overview

You can perform installation and commissioning work on the internal PC system in the Service Center, which is based on Microsoft Windows PE.

When the Desktop is active, configuration of the Service Center is possible via the "ServiceCenter Backup-Restore" (Page 219) icon.

Most of the functions of the Service Center are available in the main menu (Page 271).

In particular, you can create or restore disk images in the Service Center. The following options are available:

- If required, decrypt BitLocker protected partitions (Page 287)
- Create a disk image of the SSD (Page 275)
- Restore a disk image of the SSD (Page 278)
- Create a disk image of a partition (Page 280)
- Restore a disk image of a partition (Page 283)

More information

The Service Center uses the software **Paragon Hard Disk Manager™ 17 Suite**, which you can also call separately (Page 288).

11.5.2 Starting the Service Center

To start the Service Center, proceed in one of the following ways:

- To call up the Service Center on the SSD while the internal PC system is running up, select the "Booting Service System" while running up in the Microsoft Windows boot menu.
- To call the emergency boot system on a USB flash drive during startup of the internal PC system, press F12 or Esc during the boot process to display the boot selection.
- To switch to the Service Center while the Service Desktop (Microsoft Windows 10) is active, click the "ServiceCenter Backup-Restore" icon on the Desktop and then click "Start ServiceSystem".

11.5.3 Functions of the Service Center

Overview

In the upper section of the Service Center main menu, you can select one of five tasks. Buttons for additional functions are available in the lower section.

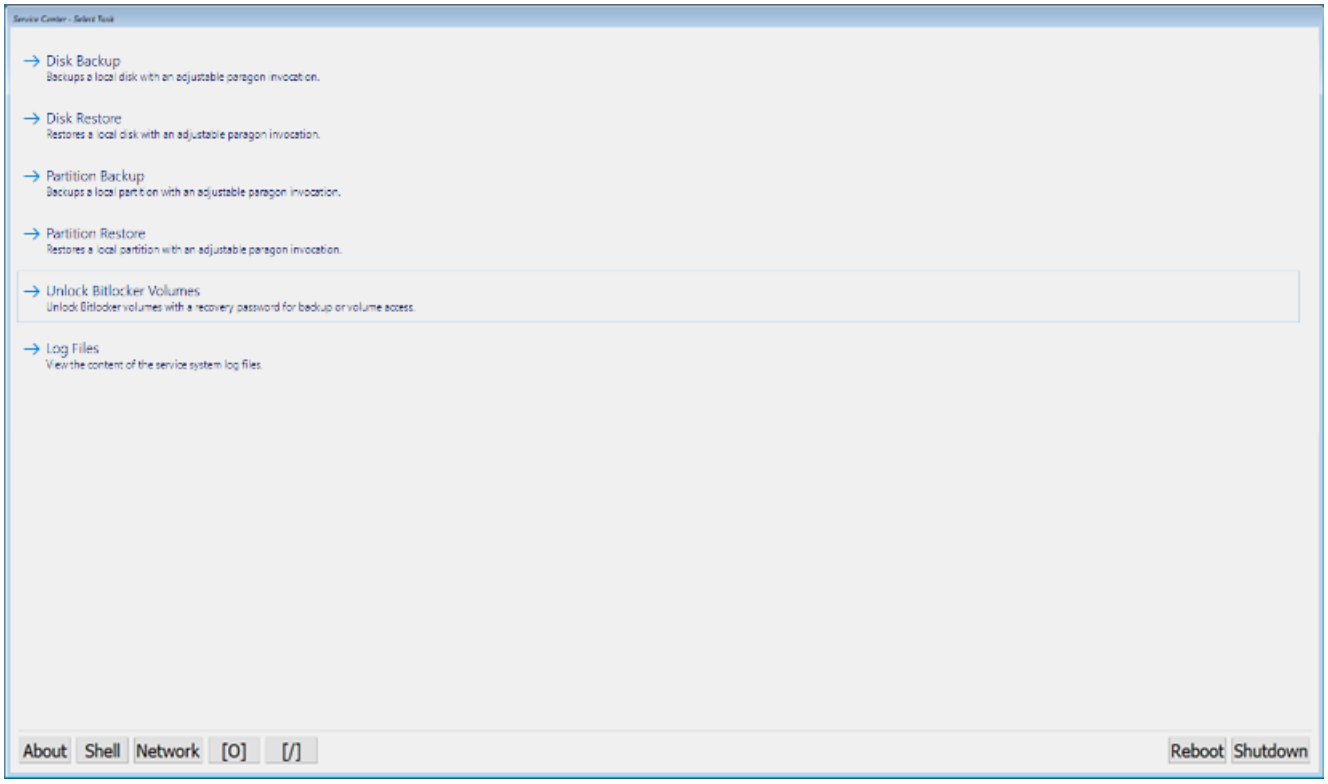


Figure 11-8 Service Center - Main menu

Table 11-16 Functions in the main menu of the Service Center

Element of the window	Purpose
Disk Backup	Create a disk image of the local SSD. With this command, you can create a disk image of the entire SSD (with all partitions).
Disk Restore	Restore the local SSD with an existing disk image. With this command, you can restore the complete SSD (with all partitions) with a previously created disk image.
Partition Backup	Create a disk image of a partition on the local SSD. With this command, you can create a disk image of an individual partition of the SSD.
Partition Restore	Restore a partition on the local SSD with a disk image. With this command, you can restore an individual partition of the SSD with a previously created disk image.
Log Files	View and save log files.
Unlock Bitlocker Volumes	Decrypts BitLocker protected partitions. Decrypt the BitLocker protected partitions with the separately stored restore password to be able to create data storage medium images.
About	Viewing information about the Service Center.

Element of the window	Purpose
Shell	Open the Prompt. Here you can enter commands for executing tasks on the PC system without using a graphic user interface.
Network	Making network settings (Page 272). Any network settings you make in this dialog box are temporary. To change network settings permanently, switch to the Service Desktop.
Rotate	Rotates the screen through 90° in the clockwise direction.
Reboot	Restarts an internal PC system.
Shutdown	Shuts down the PC system.

11.5.4 Network settings in the Service Center

You can make network settings in the main menu of the Service Center by clicking "Network":

- IP settings at the enterprise network interface X1 (Local Area Connection 2)
- IP settings at the plant network interface X2 (Local Area Connection)
- Configuration of the host
- Configuration of IP routing

Note

Temporarily storing network settings in the Service Center

Any network settings you make in this dialog box are immediately effective, but temporary.

To change network settings permanently, switch to the Service Desktop.

Further information can be found in Chapter Configuration of the Service Center (Page 219).

Overview

IP settings

You can make the following IP settings in the "Network Settings" dialog box:

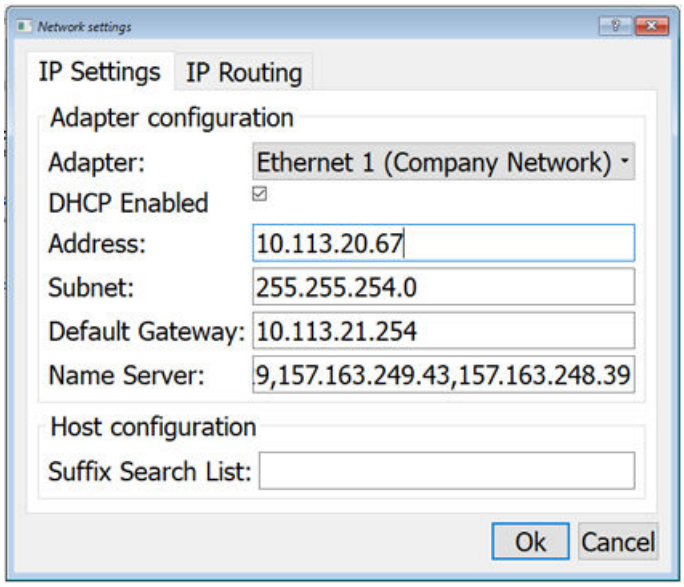


Figure 11-9 Service Center - IP settings

Note

The IP settings can only be parameterized with a connected network interface.

Table 11-17 IP settings in the "Network Settings" dialog box

Section	Setting	Purpose
Adapter configuration	Adapter	Select the Ethernet interface that you want to configure. All settings in Section "Adapter configuration" refer to the selected Ethernet interface.
	DHCP Enabled	Select whether the addresses are to be fetched dynamically from the DHCP server. If the checkbox is deactivated, you must make the settings manually.
	Address	Set the IP address of the NCU. You can specify an IP address from the following range: 192.168.214.250 - 254
	Subnet	Specify a subnet mask, e.g. 255.255.255.0
	Default Gateway	Set the IP address of the standard gateway. A standard gateway creates a standard route in the IP routing table for all destinations that are not in the subnet.
	Name Server	Set the IP address of the name server. A name server answers questions asked about a domain name zone using a DNS database.
Host configuration	Suffix Search List	Parameterize a search list for DNS suffix, e.g. "network.com". The factory setting of the Ethernet interface "Local Area Connection" is ".local".

Routing settings

You can make the following routing settings in the "Network Settings" dialog box:

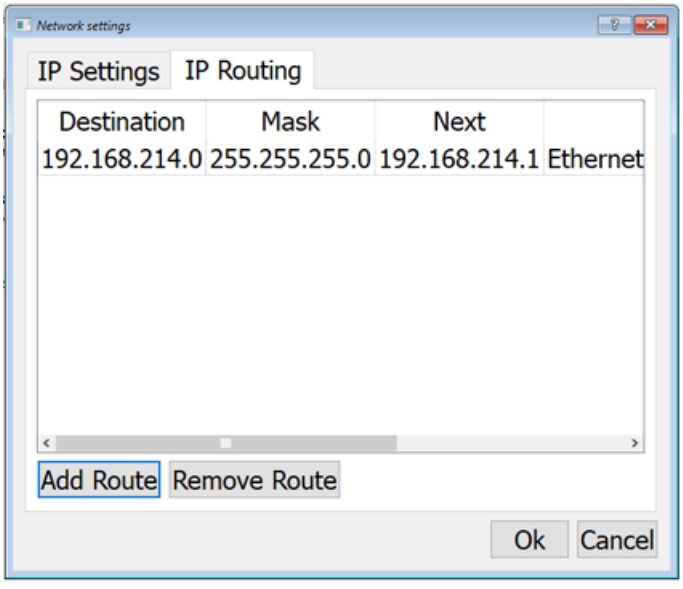


Figure 11-10 Service Center - IP routing

Table 11-18 Routing settings in the "Network Settings" dialog box

Setting	Purpose
Add Route	Add a new route.
Remove Route	Delete a selected route.
Destination	Specify the network destination of the route as an IP address.
Mask	Subnet mask of the specified IP addresses.
Next	Next hop or forwarding IP address via which the network destination can be accessed.
Interface	Select an interface to which the configured IP routing applies: • Enterprise network interface X1 (Local Area Connection 2) • Plant network interface X2 (Local Area Connection)
Metric	Integer cost metric (1 to 9999). Required if several routes for sending a packet to a network destination are possible in the routing table.

11.5.5 Create a disk image of the SSD

You can create a disk image of the entire SSD in the Service Center with the "Disk Backup" function.

Procedure

To save the SSD as a disk image, proceed as follows:

1. Start the Service Center, e.g. from the Microsoft Windows boot menu.
   More information: Starting the Service Center (Page 270)
2. If required, decrypt BitLocker protected partitions.
   More information: Decrypting BitLocker-protected partitions (Page 287)

3. In the main menu of the Service Center, click "Disk Backup".
   The "Service Center - Disk Backup" dialog box opens.

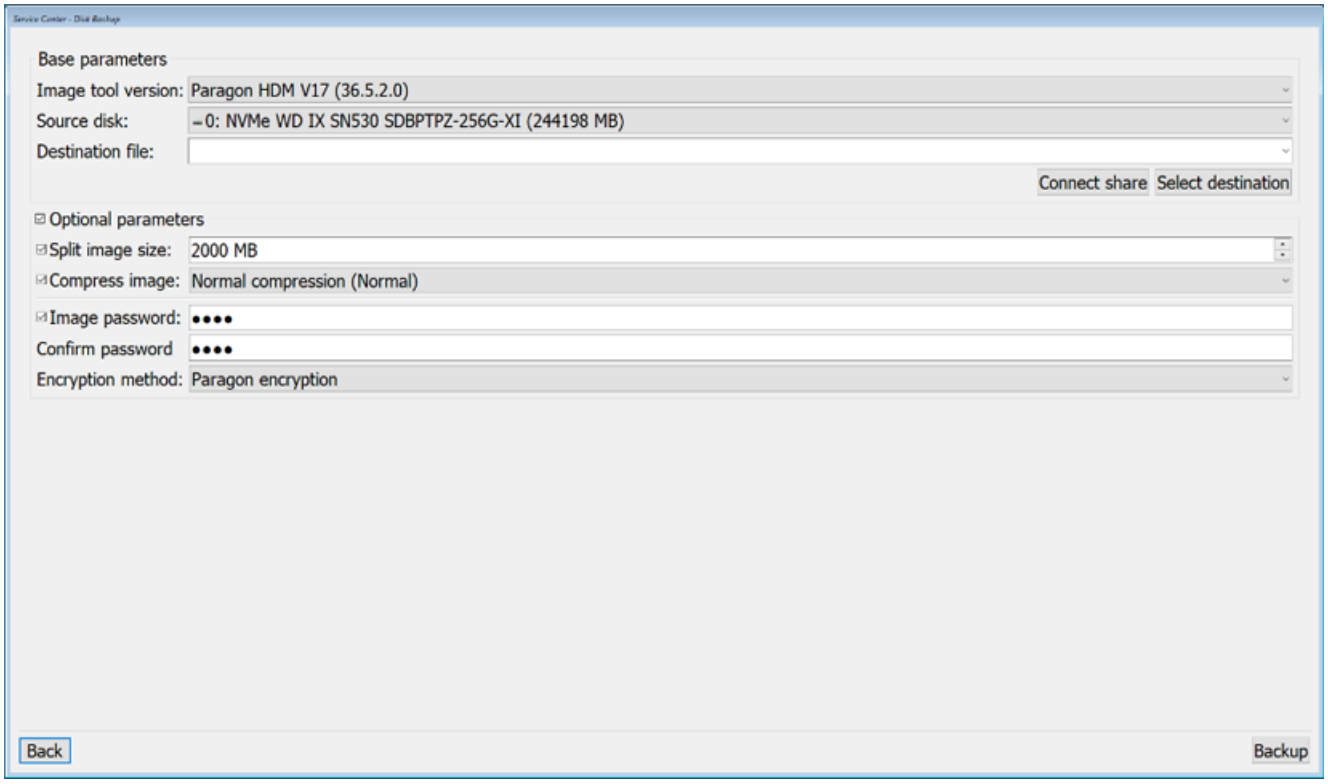


Figure 11-11 Service Center - Disk Backup

4. Make the required settings here:

Section	Setting	Purpose
Base parameters	Image tool version	Select the Paragon Hard Disk Manager™ version that is to be used when creating the disk image. Version for Microsoft Windows 10: "Paragon HDM V17 (36.5.2.0)"
	Source disk	Select a data storage medium of which you want to create a disk image.
	Destination file	Specify the target directory and file name. Disk images can be stored either locally or in the network.
Base parameters > Destination file	Connect share	Open the "Connect a Share" dialog box (Page 285). You can set up a shared resource (e.g. a directory in the network), to which you can store the disk image.
	Select destination	Open the "Select Destination File" dialog box. You can navigate through a local directory of the internal PC system and enter a file name.
Optional parameters	Split image size	Split the disk image and select a split image size. You can split the disk image into several files of a defined size. Split the disk image size in the following cases: • If the file system (e.g. FAT32) can only manage files of a certain size. • If the disk image is to be archived onto multiple data storage media, for example, when using CDs.
	Compress image	Activate Compression or select a compression level. Higher compression results in a smaller file size, but increases the time needed to compress or decompress the data.
	Image password	Encrypt the data storage medium image with a password protection. Re-enter the password to rule out typos.
	Encryption method	Select an encryption method. Standard encryption: "Paragon encryption".

5. Confirm your settings with "Backup" to start generation of the disk image.

NOTICE

Inactive BitLocker key

The BitLocker key on the PC system is inactive for the data storage medium image creation.

Activate the BitLocker again after the backup has been created.

11.5.6 Restore a disk image of the SSD

If your system is no longer functioning stably, you can restore it with a disk image.

NOTICE
Inactive BitLocker key The BitLocker key on the PC system is inactive after a data storage medium image has been restored. Activate the BitLocker after an SSD backup has been restored.

Note

Restoring replaces all current files

When you restore the internal PC system from a data storage medium image, all programs, settings and files are completely replaced by the disk image. Use the Paragon Hard Disk Manager™ software directly if you want to recover only individual files or exclude them from recovery (Page 288).

Requirement

A disk image in *.pvhd (Paragon HDM virtual image) format exists

More information: Create a disk image of the SSD (Page 275)

Procedure

To restore a disk image, proceed as follows:

1. Start the Service Center, e.g. from the Microsoft Windows boot menu.
   More information: Starting the Service Center (Page 270)
2. In the main menu of the Service Center, click "Disk Restore".
   The "Disk Restore" dialog box opens.

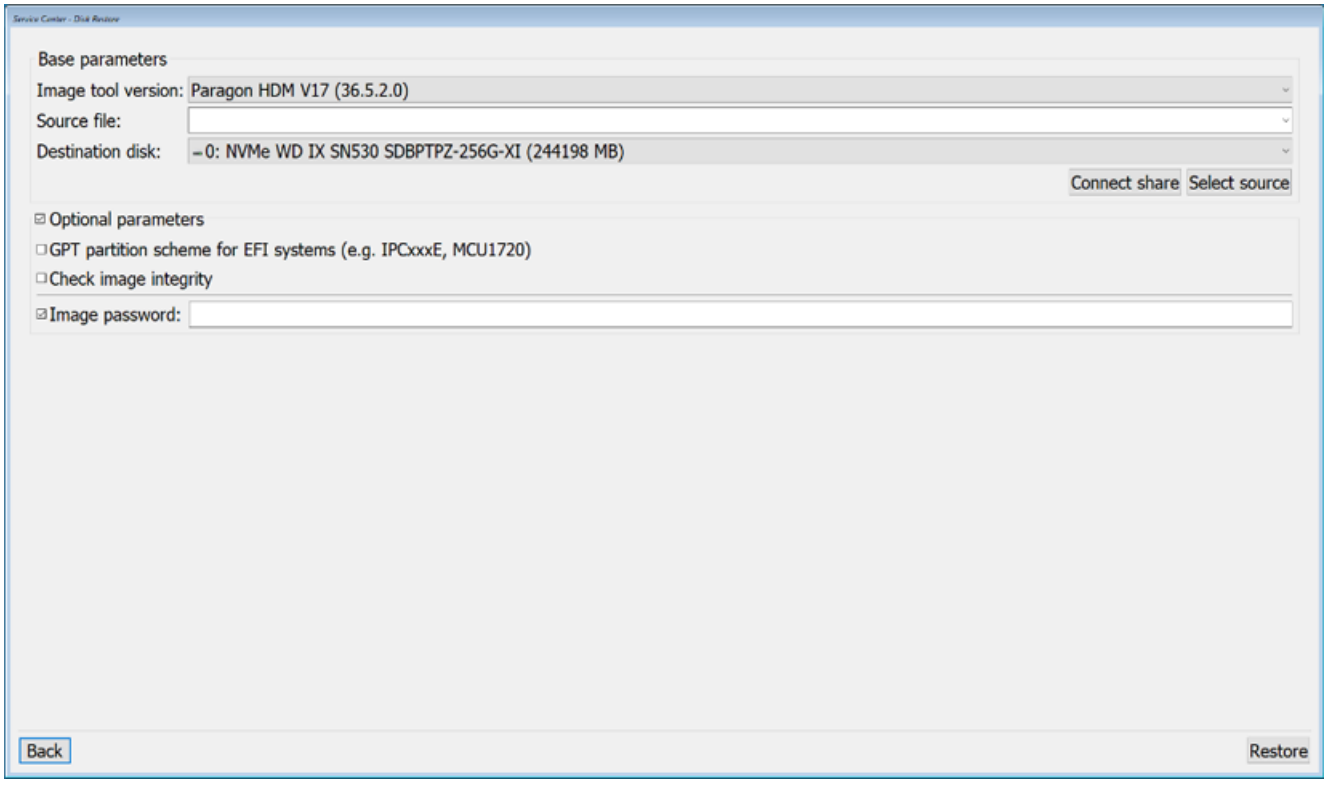


Figure 11-12 Service Center - Disk Restore

3. Make the required settings here:

Section	Setting	Purpose
Base parameters	Image tool version	Select the Paragon Hard Disk Manager™ version to be used when restoring the data storage medium. Version for Microsoft Windows 10: "Paragon HDM V17 (36.5.2.0)"
	Source file	Select the disk image from which the SSD is to be restored. You can use local disk images or disk images stored in the network.
	Destination disk	Select the SSD to be restored from the disk image.
Base parameters > Destination disk	Connect share	Open the "Connect a Share" dialog box (Page 285). You can manage a shared resource (e.g. a directory in the network), to use a disk image stored on the network to restore the SSD.
	Select source	Open the "Select Source File" dialog box. You can navigate through a local directory of the internal PC system and select a data storage medium image for restoration.
Optional parameters	GPT partition scheme for EFI systems	If necessary, use the GUID partitioning scheme (GPT) for EFI systems when restoring the disk image on MCU 1760 or IPCxxE systems.
	Check image integrity	Checks the data storage medium integrity before restoring.
	Image password	Use the password to decrypt the protected data storage medium image.

4. To start the restore process and entirely replace the existing data on the SSD with the disk image, confirm the settings with "Restore".

Result

The restore process is started.

Note

Troubleshooting if reading in of the disk image fails

If data transfer is interrupted during the restore process, the internal PC system will have no runnable system.

In this case, use a USB flash drive with Service Center to read the disk image in again.

11.5.7 Create a disk image of a partition

You can create a disk image of an individual partition of the SSD in the Service Center with the "Partition Backup" function.

Procedure

To save a partition of the SSD as a disk image, proceed as follows:

1. Start the Service Center, e.g. from the Microsoft Windows boot menu.
   More information: Starting the Service Center (Page 270)
2. If required, decrypt the BitLocker protected partition.
   More information: Decrypting BitLocker-protected partitions (Page 287)
3. In the main menu of the Service Center, click "Partition Backup".
   The "Service Center - Partition Backup" dialog box opens.

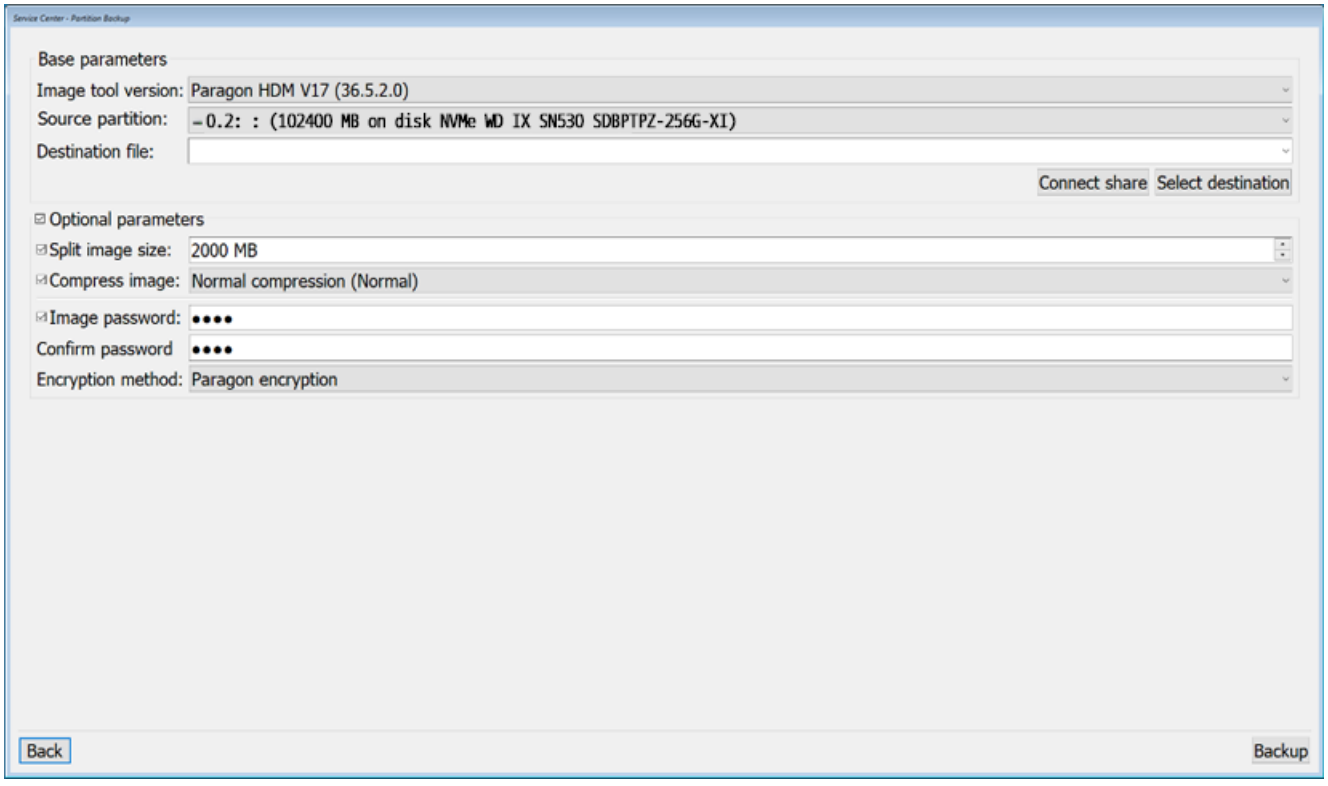


Figure 11-13 Service Center - Partition Backup

4. Make the required settings here:

Section	Setting	Purpose
Base parameters	Image tool version	Select the Paragon Hard Disk Manager™ version that is to be used when creating the disk image. Version for Microsoft Windows 10: "Paragon HDM V17 (36.5.2.0)"
	Source partition	Select a data storage medium of which you want to create a disk image.
	Destination file	Enter a destination directory and file name. Disk images can be stored either locally or in the network.
Base parameters > Destination file	Connect share	Open the "Connect a Share" dialog box (Page 285). You can set up a shared resource (e.g. a directory in the network), to which you can store the disk image.
	Select destination	Open the "Select destination file" dialog box. You can navigate through a local directory of the internal PC system and enter a file name.
Optional parameters	Split image size	**No MCU setting**, only PCU 50.x: Split the disk image and select a split image size. If you are using a PCU 50.5, you can split the disk image into several files of a defined size. Split the disk image size in the following cases: • If the file system (e.g. FAT32) can only manage files of a certain size. • If the disk image is to be archived onto multiple data storage media, for example, when using CDs. If you are using a different PC system than the PCU 50.5, you must deactivate the "Split image size" setting.
	Compress image	Activate Compression or select a compression level. Higher compression results in a smaller file size, but increases the time needed to compress or decompress the data.
	Image password	Encrypt the data storage medium image with a password protection. Re-enter the password to rule out typos.
	Encryption method	Select an encryption method. Standard encryption: "Paragon encryption".

5. Confirm your settings with "Backup" to start generation of the disk image.

NOTICE
Inactive BitLocker key
The BitLocker key on the PC system is inactive for the data storage medium image creation.
Activate the BitLocker again after the backup has been created.

11.5.8 Restore a disk image of a partition

If your system is no longer functioning stably, you can restore it with a disk image.

NOTICE
Inactive BitLocker key The BitLocker key of the partition is inactive after a data storage medium image has been restored. Activate the BitLocker after a backup has been restored.

Note

Restoring replaces all current files

When you restore a partition from a disk image, all programs, settings, and files are completely replaced on this partition by the disk image. Use the Paragon Hard Disk Manager™ software directly if you want to recover only individual files or exclude them from recovery (Page 288).

Requirement

A disk image of a partition in *.pvhd (Paragon HDM virtual image) format exists

More information: Starting the Service Center (Page 270)

Procedure

To restore a partition from a disk image, proceed as follows:

1. Start the Service Center, e.g. from the Microsoft Windows boot menu.
   More information: Create a disk image of a partition (Page 280)
2. In the main menu of the Service Center, click "Partition Restore".
   The "Partition Restore" dialog box opens.

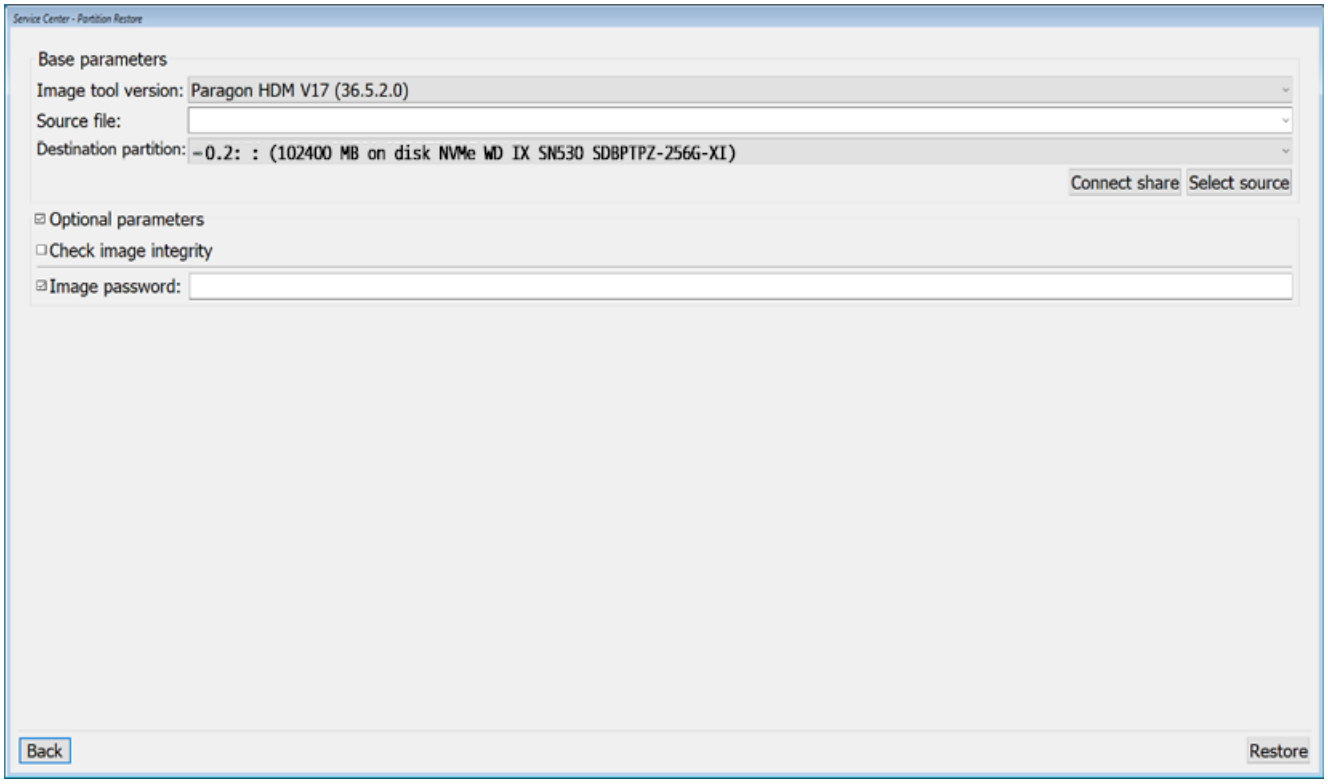


Figure 11-14 Service Center - Partition Restore

3. Make the required settings here:

Section	Setting	Purpose
Base parameters	Image tool version	Select the Paragon Hard Disk Manager™ version to be used when restoring the disk partition. Version for Microsoft Windows 10: "Paragon HDM V17 (36.5.2.0)"
	Source file	Select the disk image from which the partition is to be restored. You can use local disk images or disk images stored in the network.
	Destination partition	Select the partition to be restored from the disk image.
Base parameters > Destination partition	Connect share	Open the "Connect a Share" dialog box (Page 285). You can manage a shared resource (e.g. a directory in the network), to use a disk image stored on the network to restore the SSD.
	Select source	Open the "Select source file" dialog box. You can navigate through a local directory on the internal PC system and select a data storage medium image for restoration.
Optional parameters	Check image integrity	Checks the data storage medium integrity before restoring.
	Image password	Use the password to decrypt the protected data storage medium image.

4. To start the restore process and entirely replace the existing data on the partition with the disk image, confirm the settings with "Restore".

Result

The restore process is started.

Note

Troubleshooting if reading in of the disk image fails

If data transfer is interrupted during the restore process, the internal PC system will have no runnable system.

In this case, use a USB flash drive with Service Center to read the disk image in again.

11.5.9 Network settings in the Service Center

To manage a data storage medium image in the network, you can display a shared network directory on the internal PC system as a drive.

In the Service Center, you configure network drives in the "Connect a share" dialog box. You can call this dialog box directly from the relevant dialog boxes to both create (Page 275) and restore (Page 278) disk images.

Precondition

The network directory is shared with the relevant user accounts in the domain and on the internal PC system.

More information: Release directory of the PC/PC in the network (Page 297)

Overview

The setting options in the "Connect a share" dialog box have the following meaning:

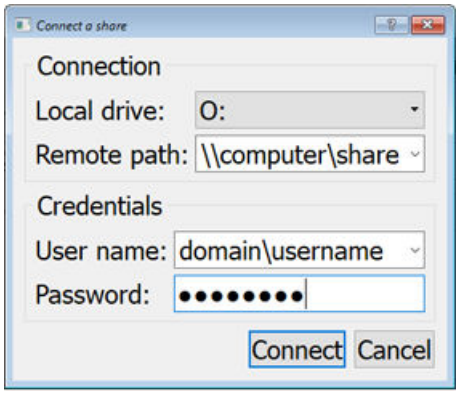


Figure 11-15 "Connect a Share" dialog box

Table 11-19 Settings in the "Connect a Share" dialog box in the Service Center

Section	Setting	Purpose
Connection	Local drive	Select drive letters under which the network directories are to be accessible on the internal PC system. The drive letters Z, Y and X are assigned to USB interfaces at the operator panels. Do not use these drive letters for other purposes in order to avoid problems when using these USB interfaces.
	Remote path	Specify the device in the network and share name of the resource. Syntax: `\\Name of the server\share name of the network directory` Example: `\\Backup_Server\PCU_Backup`
Credentials	User name	Enter the user account under which the resource in the network can be accessed. If you have shared the resource on the server for certain users only, you must enter one of these user accounts here.
	Password	Enter the password of the user account.

More information

You will find information about sharing directories in the network and network drives in the following chapters:

- Release directory of the PC/PC in the network (Page 297)
- Creating a shortcut to the network drive (Page 300)

11.5.10 Decrypting BitLocker-protected partitions

Decrypt BitLocker-protected partitions with the separately stored recovery password to be able to create disk images.

Requirement

You need the encrypted recovery password in a text file (*.txt).

More information: Using the BitLocker drive encryption (Page 246)

Key statement

To decrypt BitLocker-protected partitions, proceed as follows:

1. Start the Service Center, e.g. from the Windows boot menu.
   More information: Starting the Service Center (Page 270)
2. In the main menu of the Service Center, click "Unlock Bitlocker Volumes".
   The "Unlock Volumes" dialog box opens.

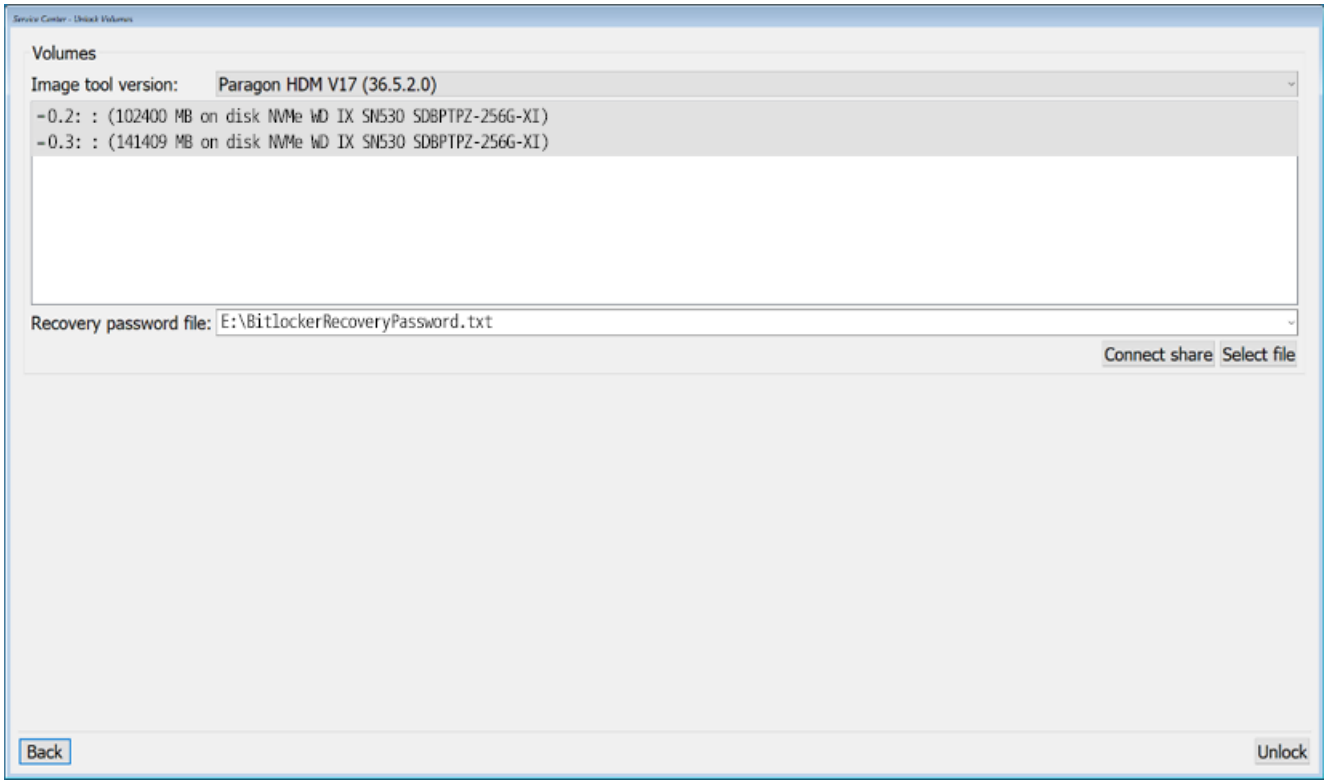


Figure 11-16 Service Center - Unlock Volumes

3. Make the required settings here:

Section	Setting	Purpose
Volumes	Image tool version	Select the Paragon Hard Disk Manager™ version that is to be used when creating the disk image. Version for Microsoft Windows 10: "Paragon HDM V17 (36.5.2.0)"
	Select BitLocker-protected partitions to be decrypted. **Note:** Unencrypted partitions are not displayed in the selection box.	
	Recovery password file	Specifies the storage location of the password file.
	Connect share	Open the "Connect a Share" dialog box (Page 285). You can use a shared resource (e.g. a directory in the network).
	Select file	Open the "Select file" dialog box. You can navigate to a local directory on the PC system and select a password file for decryption.

4. To decrypt the partitions, confirm the settings with "Unlock".
   The BitLocker-protected partitions are decrypted.
   The operation may take several minutes.

11.5.11 Starting the Paragon Hard Disk Manager directly

Using the **Paragon Hard Disk Manager™ 17 Suite** software, you can store the entire contents of an SSD as a disk image. Disk images can be kept on various storage media for subsequent restoration of the data on the SSD.

Paragon Hard Disk Manager™ is included in the PCU-Basesoftware /IPC scope of delivery and on the replacement SSD for the IPC. Paragon Hard Disk Manager™ is used by the components of PCU base software /IPC to back up or restore data.

You can also launch Paragon Hard Disk Manager™ directly from the Microsoft Windows desktop to perform backup tasks in the application's user interface.

Procedure

To start Paragon Hard Disk Manager™ directly on the PC system, proceed as follows:

1. In the Microsoft Windows 10 desktop, double-click the "Paragon Hard Disk Manager™ 17 Suite" icon.
2. Acknowledge the confirmation prompt by clicking "Yes".

To start Paragon Hard Disk Manager™ directly on the USB flash drive with Service Center, proceed as follows:

1. The PC system is switched off. Shut down the PC system if necessary.
2. Connect the USB flash drive to the PC system.
3. Switch on the PC system.

4. Immediately after switching on the device, press and hold the <Esc> key.
   The firmware selection menu is opened.
5. Select "Boot Manager".
   The "Boot Manager" with the "Boot Options Menu" overview is opened.
6. Under "EFI USB Boot Device", select the USB flash drive and confirm the entry.
7. Confirm the following message "Microsoft Windows Preinstallation Environment".
   The "SIMATIC IPC Image & Partition Creator" application interface is displayed under Microsoft Windows PE (Service Center).
8. Select the option "Hard Disk Manager 17 Suite" and click "Run".

Result

The application Paragon Hard Disk Manager™ 17 Suite is opened.

Example: Restoring individual files from the disk image

The Paragon Hard Disk Manager™ 17 Suite software allows you to select and restore individual data from a disk image:

1. Start the Paragon Hard Disk Manager directly.
   The application is opened.
2. Click the "Restore from file" tab in the "Backup & Recovery" view.
3. Select an existing disk image under the sidebar option "Explore and export files".
   The "View backup contents" dialog box opens.
4. Select the required settings. Locate and mark the required individual data and directories.
5. Select your target details.
6. Transfer the data from the disk image.

More information

On the Internet, you can find more information about the application on the website www.paragon-software.com (https://kb.paragon-software.com/home-home-office-manuals).

For more information on how to operate the application with SIMATIC IPC, refer to the SIMATIC IPC Image & Partition Creator Operating Manual (https://support.industry.siemens.com/cs/document/109780775/simatic-ipc-image-partition-creator-v3-6?dti=0&lc=en-WW).

11.5.12 Creating an emergency boot system USB flash drive

Usage

You can generate a Service Center (emergency boot system) based on Microsoft Windows PE on a USB flash drive as preventive measure in the case of a defect.

The image for the creation of the USB flash drive is on the installed PCU Base under: `D:\Eboot\eboot.zip`.

Requirement

- The Microsoft Windows Service Desktop is active
- A 32 GB USB flash drive in FAT32 format is available (e.g. SIMATIC PC USB flash drive)

Preparation

If necessary, format the data storage medium:

1. Connect the USB flash drive to a USB interface of the PC system.
2. Open the application in Microsoft Windows Explorer.
3. In the drive overview, right-click on the USB flash drive, then on "Format...".
4. If required, acknowledge the system event message with "Yes".
   The formatting dialog is opened.
5. Select the FAT32 format and insert the EBOOT volume designation.
6. Start the formatting process.

Procedure

To create a USB flash drive, proceed as follows:

1. Connect the USB flash drive to a USB interface of the PC system.
2. Open the application in Microsoft Windows Explorer.
3. Copy the `eboot.zip` image from the `D:\Eboot\` directory to the USB flash drive.
4. Extract the contents of the ZIP file directly to the root directory of the USB flash drive, e.g. under `E:\`.
   Use Microsoft Windows, for example, right-click on the ZIP file, then "Extract all...".
   Follow the instructions on how to extract the data.

Result

The emergency boot system has been installed on the USB flash drive and the data storage medium has been renamed to EBOOT. The Service Center on the USB flash drive can be used.

11.5.13 Operating a service PC/PC in the network

11.5.13.1 Overview

System network

In the following applications, you will need, for example, a connection between the MCU-IPC and a PG/PC in the system network:

- Save the disk image of the SSD to a PG/PC
- Restore the SSD via the DVD drive of a PG/PC
- Start up the replacement SSD
- Install the software on the MCU-IPC via the DVD drive of a PG/PC

Company network

If you want to connect the service PG/PC via a company network (Local Area Connection 2; interface X1), contact your network service center.

Further information on the Windows Firewall settings in the company network can be found in the Chapter Adapting the firewall settings (Page 222).

11.5.13.2 Connection options in the system network

Overview

The following figures show the typical connection options in the system network:

- Service PG/PC with (crossover) Ethernet cable directly to the interface "X2" of the MCU-IPC.
- Service PG/PC with (non-crossed over) Ethernet cable via switch to the interface "X2" of the MCU-IPC.

Configuration with PG/PC directly at the internal PC system

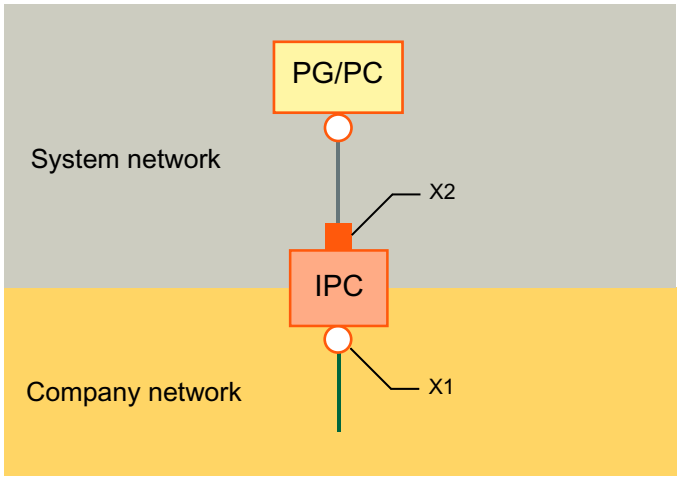


Figure 11-17 Connecting a PG/PC directly at the MCU-IPC

Configuration with PG/PC and switch directly at the internal PC system

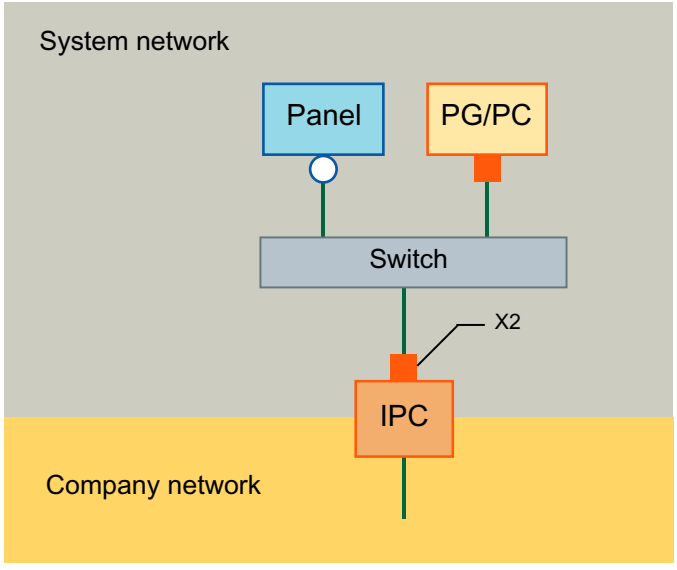


Figure 11-18 Connecting a PG/PC at the MCU-IPC using a switch

Basic procedure

On the PG/PC with Microsoft Windows 10:

- Connect a PG/PC to an internal PC system according to one of the configurations shown above.
- The network protocol used is: TCP/IP.
  TCP/IP is already pre-configured on the internal PC system.

- Set up IP addresses on the same subnetwork.
- Share a directory on the PG/PC for network access.

On the internal PC system in the Service Center:

- Start the Service Center.
- Establish a network connection to the shared directory of the PG/PC.
  More information: Functions of the Service Center (Page 271)

11.5.13.3 Configuring routing in the network

Overview

If you have connected a PG/PC at the NC interface X127 of the MCU, configure the network routing to establish the connection between the PG/PC and the MCU-IPC.

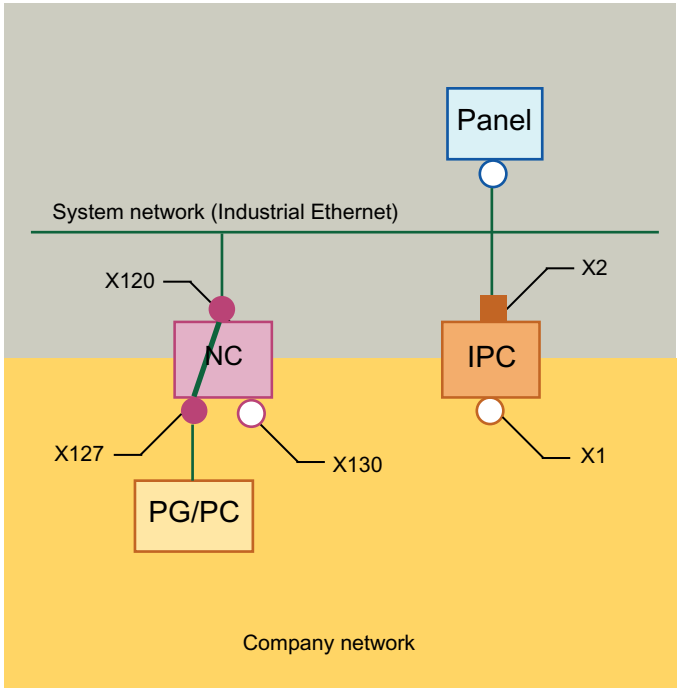


Figure 11-19 A networking example using IP routing

Preconditions

The following conditions must be met in order to use this function:

- The PG is connected to NC interface X127 in the system network.
- NC and IPC are connected.

- On the NC the routing is activated in one of the following ways:
  - In SINUMERIK ONE Commissioning, the routing is configured in the user interface "System network settings".
  - In the configuration file basesys.ini, key EnableSysNetToIBNForwarding=1 is set.
- If you wish to access a network directory, it must be shared.
- The user account in question is known to the PG/PC.
- The Service Center is active.

Procedure

To configure the IP routing in the Service Center, proceed as follows:

1. In the main menu of the Service Center, click "Network".
2. In the "Network Settings" dialog box, click the "IP Routing" tab.

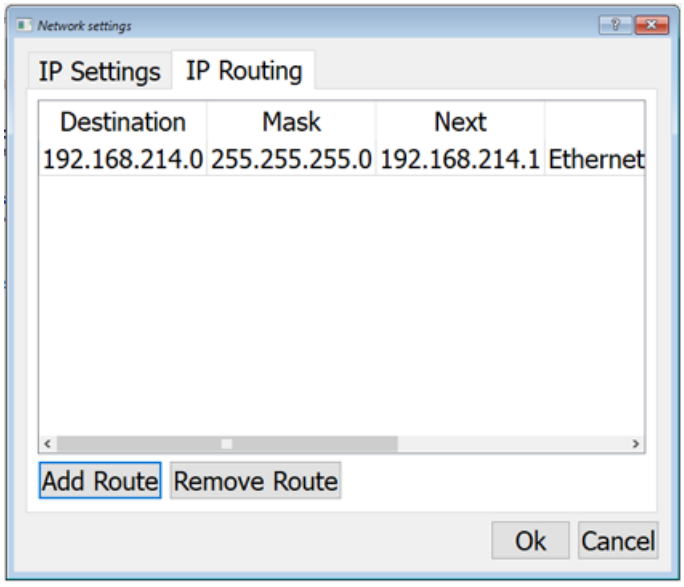


Figure 11-20 Service Center - IP routing

3. Configure the necessary routes.
   More information: Network settings in the Service Center (Page 272)

Result

The routing was configured and the PG/PC and internal PC system are connected via the NC.

Now, perform the desired steps, for example, a Restore a disk image of the SSD (Page 278).

11.5.13.4 Configure the network settings of the PG/PC

Once you have connected a PG/PC in the network, make the network settings on the PG/PC.

The basic procedure for setup under Microsoft Windows 10 or Microsoft Windows 7 is described below. More information from Microsoft can be found on the internet:

Microsoft Windows support (https://support.microsoft.com/en-us/hub/4338813/windows-help?os=windows-10)

Precondition

- The PG/PC is linked with the MCU-IPC in one of the following ways:
  - The PG/PC is connected to the internal PC system using an Ethernet cable (either directly or via a switch).
    More information: Connection options in the system network (Page 291)
  - The PG/PC is networked with the internal PC system via an interface of the NC and the routing is configured.
    More information: Configuring routing in the network (Page 293)
- A current Microsoft Windows operating system is installed on the PG/PC.
- The PG/PC is switched on.

Procedure

To configure the network settings of the PG/PC to connect with the internal PC system in the system network, proceed as follows:

1. Open the "network connections" window:
   - To do this under Microsoft Windows 7, click in the Control Panel in category "Network and Internet > View network status and tasks," select "Change adapter settings".
   - To do this under Microsoft Windows 10: enter "Control Panel" in the search field, then click on "Control Panel > Network and Sharing Center > Change Adapter Settings".
2. Right-click on the network adapter you want to configure, then in the shortcut menu click on "Properties".
   Dialog "Properties of <connection>" opens.

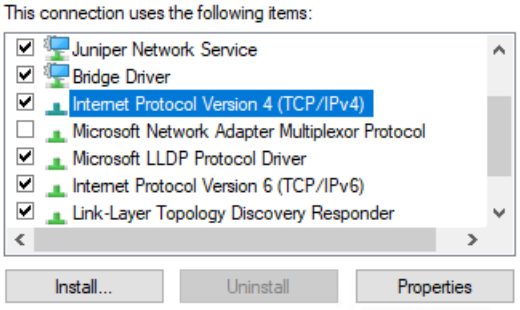


Figure 11-21 Properties of <connection>

3. Make the following settings:
   - Click "File and Printer Sharing for Microsoft Networks."
   - To change the IP address of the PG/PC, double-click "Internet Protocol Version 4 (TCP/IPv4)", then configure the settings as follows:

Section	Element	Setting
Use the following IP address	IP address	The following IP addresses in the system network of the MCU 1720 (X2) can be used for the PG/PC: • 192.168.0.250 • 192.168.0.251 • 192.168.0.252 • 192.168.0.253 • 192.168.0.254
	Subnet mask	• 255.255.255.0

Result

The network settings of the PG/PC are now configured for use with the MCU-IPC.

11.5.13.5 Release directory of the PC/PC in the network

If you want, for example, to store data storage medium images on a PG/PC that you have linked to the internal PC system via the network, set up a network drive.

As soon as it has been set up, a new drive will appear on the internal PC system, which is really a directory on the PG/PC.

The basic procedure for setup under Microsoft Windows 10 or Microsoft Windows 7 is described below. More information from Microsoft can be found on the internet: Microsoft Windows support (https://support.microsoft.com/en-us/hub/4338813/windows-help?os=windows-10)

Precondition

- The PG/PC is switched on.
- There is sufficient free storage space on the PG/PC to save data storage medium images of the MCU-IPC, for example.
- The user accounts to which you want to grant share rights are known in the domain or on the MCU-IPC.

Procedure

Proceed as follows to share a directory for use in the network:

1. On the PG/PC, in the Control Panel call up Computer Management.
2. Under "System > Shared Folders" select the file "Shares."
3. In the "Action" menu, click the "New File Share..." command.
   The "Create A Shared Folder Wizard" opens.

4. Under step "Name, Description, and Settings," make a note of the Share path, which is a combination of the computer name and the share name. You will have to specify this name when you create a link to the network drive on the PC system.

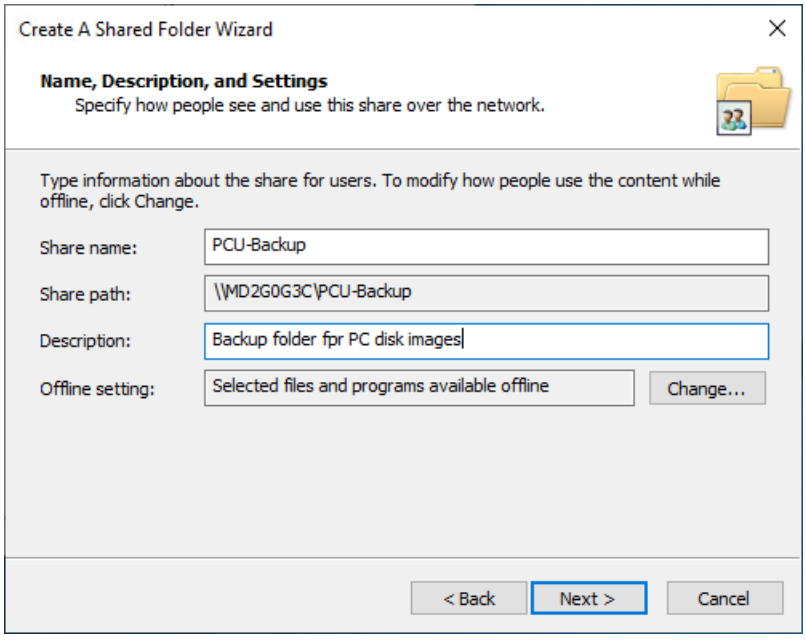


Figure 11-22 Create A Shared Folder Wizard - Name, Description, and Settings

5. Under step "Shared Folder Permissions," select the "Customize permissions" option button, then click "Custom..."

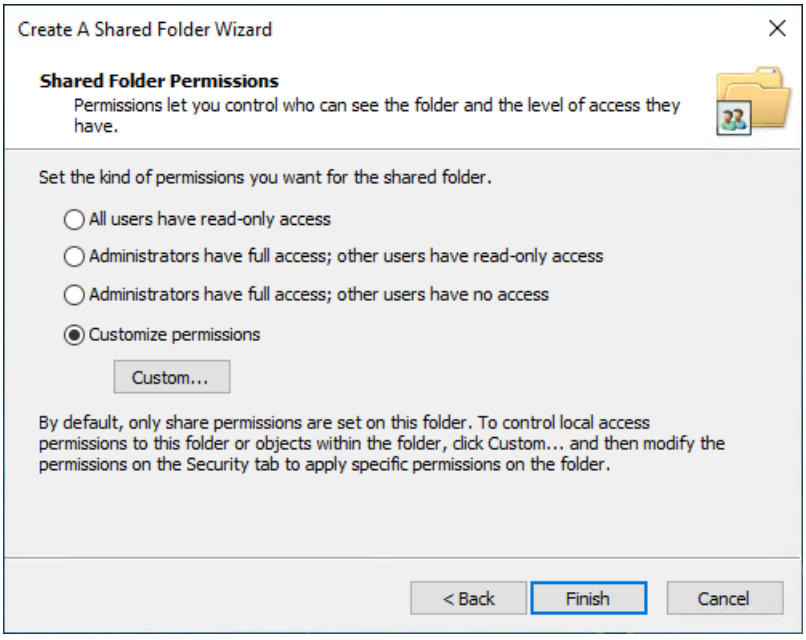


Figure 11-23 Create a Shared Folder Wizard - Shared Folder Permissions

The "Customize Permissions" dialog box opens.

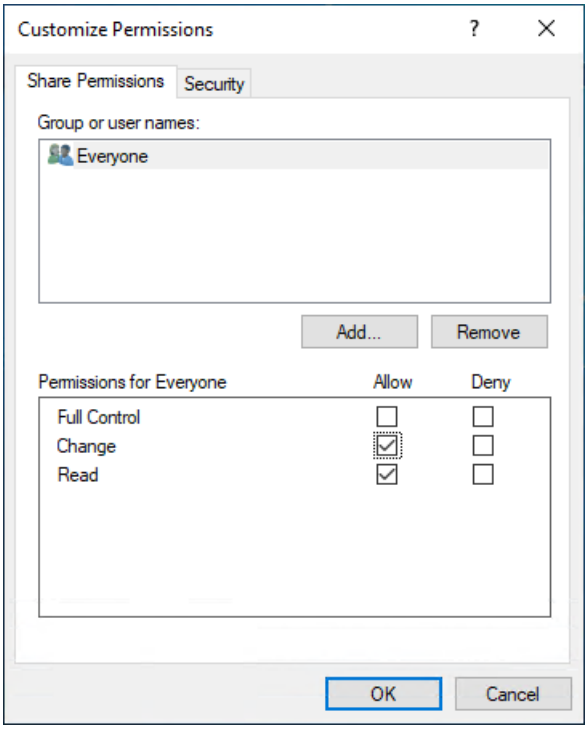


Figure 11-24 "Customize Permissions" dialog box

6. In section "Group or user names," click "Add..."
   The "Select Users, Computers, Service Accounts, or Groups" opens.

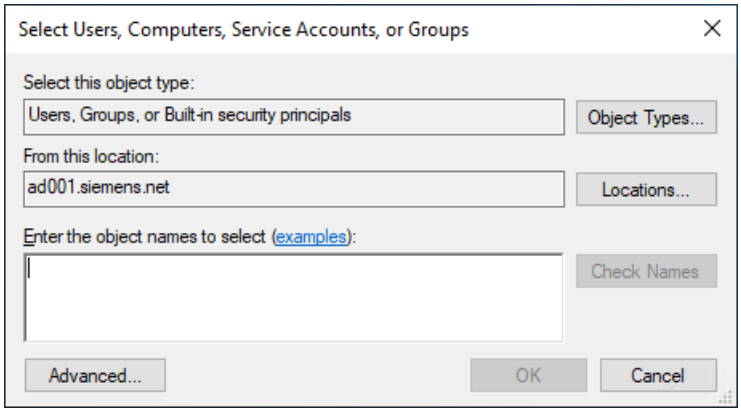


Figure 11-25 "Select Users, Computers, Service Accounts, or Groups" dialog box

7. In section "Permissions for <user name>," under column "Allow," click the "Change" checkbox.
8. Confirm these settings in the "Customize Permissions" dialog box with "OK".
9. In the next steps of the wizard, make all the settings you require and confirm the share with "Finish".

11.5.13.6 Creating a shortcut to the network drive

To be able to access the shared directory on the PG/PC from the internal PC system after you have connected and configured the PG/PC in the network, you must set up the shared folder on the MCU-IPC as a network drive.

As soon as it has been set up, a new drive will appear on the internal PC system, which is really a directory on the PG/PC.

The basic procedure for setup under Microsoft Windows 10 or Microsoft Windows 7 is described below. More information from Microsoft can be found on the internet: Microsoft Windows support (https://support.microsoft.com/en-us/hub/4338813/windows-help?os=windows-10)

Precondition

- The PG/PC is switched on.
- The Service Desktop is active.
- The folder on the PG/PC is shared for the relevant user accounts on the domain and on the MCU-IPC.

Procedure

Proceed as follows to connect a shared directory as a network drive:

1. Start the Microsoft Windows Explorer and click the "Map network drive" button.
2. Make the following settings in the "Map network drive" dialog box:

Setting	Purpose
Drive	Select drive letters under which the network directories are to be accessible on the internal PC system. The drive letters Z, Y and X are assigned to USB interfaces at the operator panels. Do not use these drive letters for other purposes in order to avoid problems when using these USB interfaces.
Folder	Specify the device in the network and share name of the resource. Syntax: `\\Name of the server\share name of the network directory` Example: `\\Backup_Server\PCU_Backup`
Reconnect at logon	Activate this checkbox to automatically connect the network drive while running up.
Connect using different credentials	Activate this checkbox if you have not shared the directory in the network with the user for whom you would like to set up the network drive. In the next dialog box "Enter Network Password," enter the log-on information of a user with whom the network directory is shared.

3. Confirm your settings with "Finish".

11.5.14 Starting up the replacement SSD

More information

More information on the replacement or installation of an SSD is provided in the hardware documentation for the MCU hardware in the
SINUMERIK MC Equipment Manual MCU 1720.

Note

Troubleshooting if reading in of the disk image fails

If data transfer is interrupted during the reading process, there will be no executable operating system available on the internal PC system.

In this case, use a USB flash drive with Service Center to read the disk image in again.

More information on restoring a disk image is provided under Restore a disk image of the SSD (Page 278).

11.6 Remote access for diagnostics

11.6.1 Overview

You can use a remote connection to access other devices via the network:

- Access to maintenance with prompt (SSH) via PuTTY.
- Access via VNC Viewer with all of the operating and service options, which are also provided directly on the MCU-IPC.

More information: Setting up and using SSH (Page 304)

11.6.2 Searching for devices in the system network

The "sc_show_net" command shows devices available in the system network in the prompt and offers more information about these devices.

As both these functions rely on SNMP (Simple Network Management Protocol), only SNMP-capable devices will be found. In the case of Microsoft Windows-based devices, this depends on the software version. If a simple call is made without any additional options, a list of the devices found will appear showing the relevant IP address, DNS name (if known), and a short description (module name).

sc_show_net command

This command is executed in the prompt:

Syntax:	sc_show_net [-xml] [[-hw] [-tco] [-sw | -swfull] [-loc] [-panel] [-dhcp] [-switch] | -all] [HOSTS...]
Authorization level:	None

11.6.3 Display of accessible nodes in SINUMERIK ONE Commissioning

You can use the network diagnostics function in SINUMERIK ONE Commissioning to display accessible nodes in the system network.

Procedure

Proceed as follows to show accessible nodes:

1. Select "MENU SELECT" to open the menu.
2. In the horizontal softkey menu, select "Diagnostics > Bus."
3. In the vertical softkey menu, select "TCP/IP Diagnostics > Diagnostics Network > Accessible nodes".
   The "Accessible nodes" user interface opens showing all nodes that use the SNMP or DCP protocol.

11.6.4 Remotely accessing the MCU for operation and maintenance

You can connect via remote access to MCU components that have an active VNC server.

- If you want to remotely access the internal PC system from a PG/PC in the system network (Page 291) or via the company network, then you must adapt the firewall settings (Page 228) and define a password.

  Note

  Accessing the MCU-IPC requires a secure password

  A password is required to access the internal PC system via remote access. The password is not yet defined in the factory settings. You must specify a password if the internal PC system is to be accessed.

- The factory setting only enables you to monitor the internal PC system via an external VNC Viewer.
  To operate the system from another station, the system in question must grant permission. You make the necessary settings in the **tcu.ini** in section `[VNCViewer]`.

Defining the password

To define passwords to remotely access the internal PC system, call the command prompt and enter the "sc_vncpwd" command.

Command	Parameter	Value	Meaning
sc_vncpwd	set	companynetwork|systemnetwork [password]	Sets the specified password and activates the password prompt for remote access
	reset	companynetwork|systemnetwork	Deactivates the password prompt (remote access without password)

- Example for company network (X1):
  `sc_vncpwd set companynetwork mypasswd`
- Command for system network (X2):
  `sc_vncpwd set systemnetwork mypasswd`

The password may contain a maximum of 8 characters. Passwords are saved in encrypted form in the following file:

C:\ProgramData\Siemens\MotionControl\user\System\etc\sinumerikvnc.ini

Options for the VNC Viewer

Note

Do not change the factory settings!

To ensure that the VNC Viewer works properly, the following options must not be changed.

Table 11-20 Connection settings in the start dialog of the VNC Viewer

Option	Factory setting
server:port	192.168.0.241

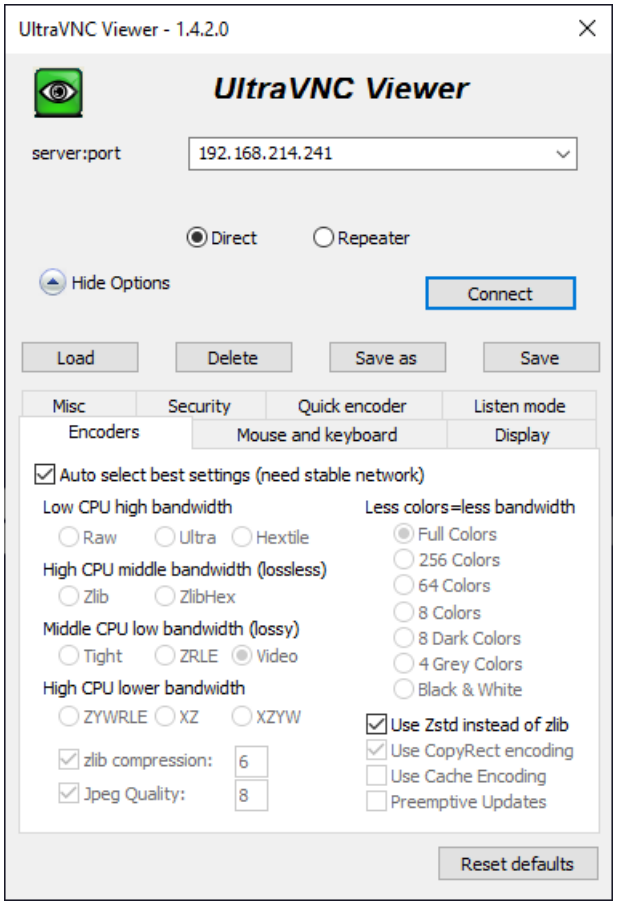


Table 11-21 More connection settings ("Show Options" button)

Tab	Factory setting
Quick encoder	AUTO (Auto select best settings)
Encoders	Auto select best settings (need stable network)
Security	Share the Server, allow other to connect.
Mouse and keyboard	Emulate 3 Buttons (with 2-button click)
	Let remote server deal with mouse cursor
Display	Show Toolbar.

11.6.5 Setting up and using SSH

You can use remote access to access devices from the internal PC system.

An SSH environment is initially set up when installing PCU-Basesoftware /IPC for Microsoft Windows 10. You can log on with PuTTY.

You can use an SSH key to log on. A script for setting up the infrastructure on devices is provided. However, for security reasons no previously generated keys have been stored.

More information: Encryption via SSH protocol (Page 305)

Setting up remote access with SSH and key pair

The procedure for setting up users and using remote access is the same as the usual procedure for remote access with SSH.

Table 11-22 Support with setting up remote access

Task	Recommended application	Storage path	Help
Generate key pair	PuTTY Key Generator	C:\Program Files (x86)\PuTTY\puttygen.exe	Online help in PuTTY (Chapter *Public key for pasting into authorized_keys file*)

Set up infrastructure on devices	Supplied script ssh_key_login.bat	C:\ProgramData\Siemens\Motion Control\siemens\System\etc.\ssh_key_login.bat	Call up the script via the prompt. To do this, enter user name and file name of the public key as the parameters.
			Syntax:
			`ssh_key_login.bat <user name> <public key>`
			Example:
			`ssh_key_login.bat username publicKey.pub`

Access devices via remote connection	PuTTY	C:\Program Files (x86)\PuTTY\putty.exe	Online help in PuTTY The IP address is taken from the DHCP server

11.6.6 Encryption via SSH protocol

Security

The security of SSH is ensured by a series of cryptographic algorithms for encryption and authentication.

Authentication

The server identifies itself to the client with an RSA, DSA or ECDSA certificate, which enables detection of manipulation in the network (no other server can identify itself as a known server).

The client can authenticate itself either by public key authentication with a private key whose public key is stored on the server, or with a normal password. While in the latter case, user interaction is always necessary (unless the password is stored unencrypted on the client computer), public key authentication allows client computers to log on to SSH servers

without user interaction, without a password having to be stored in plain text on the client. However, for added security the private SSH keys can also be protected with a password.

Subsystems

In the case of Secure Subsystem Execution, subsystems that were defined in an SSH server installation can be executed remotely without knowing the precise path of the program executed on the server. SFTP is the most common subsystem.

Further information

- Chapter Setting up and using SSH (Page 304)
- Description of PuTTY

HT 2 and HT 10 handheld terminals

12

12.1 Handheld terminals overview

HT 2 overview

The mobile SINUMERIK HT 2 handheld terminal is designed for the manual and flexible operation of machine tools. It enables convenient work during monitoring and operation.



(1) Emergency stop button (stop button)
(2) Rotary override switch
(3) Display
(4) Keyboard
(5) Handwheel
(6) Enabling button (left)
(7) Enabling button (right)
(8) Opening for the cable entry
(9) Cable duct cover
(10) Type plate
(11) Standard position mounting bracket (optional: Retaining magnet)
(12) Standard position retaining magnet (optional: Mounting bracket)
(13) Key-operated switch

More information

More information on commissioning the handheld terminal can be found in Chapter "Handheld terminals" in the
Equipment Manual Operating components HT 2 handheld terminals (https://support.industry.siemens.com/cs/document/109783841/technical-documentation-for-sinumerik-operator-components?dti=0&lc=en-WW).

HT 10 overview

The HT 10 mobile handheld terminal combines the functions of an operator panel and a machine control panel in one device. It therefore provides the option of being able to completely operate and monitor a machine.



① Emergency stop button
② Display / touch screen
③ Handwheel (optional)
④ Rotary override switch
⑤ LED function keys

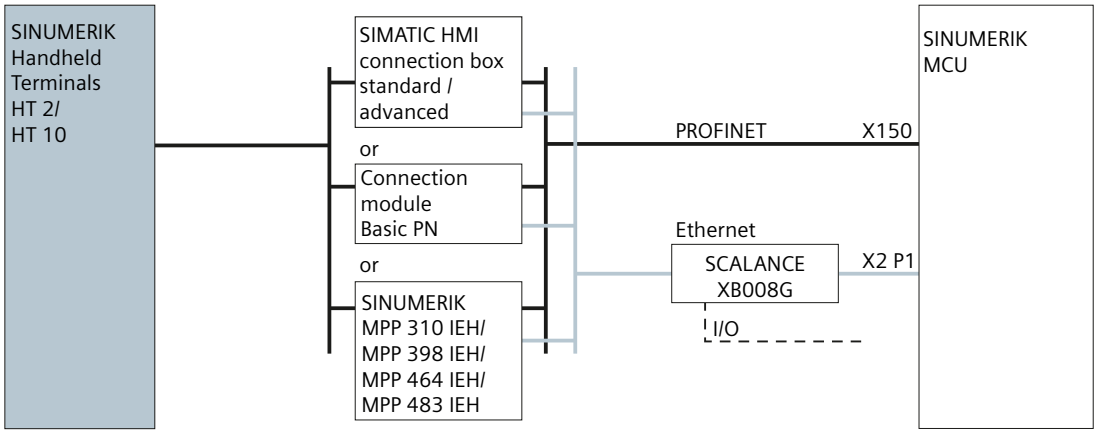
More information

More information on commissioning the handheld terminal can be found in the Equipment Manual Operating components HT 10 handheld terminals (https://support.industry.siemens.com/cs/document/109783841/technical-documentation-for-sinumerik-operator-components?dti=0&lc=en-WW).

More information on calibration and operation of the handheld terminal is provided in the online help under
Operate Universal/Turning/Milling/Grinding.

12.2 Connecting handheld terminals to the MCU

Connection overview



Note

Bridge X2 P1 with X150 via a switch when connecting an HT 2 or HT 10.

The handheld terminals are designed for communication via Industrial Ethernet. Connection via X150 and X2 P1 enables a reliable connection of the SINUMERIK I/O to the PLC independent of a restart of the MCU-IPC system..

HT connection options:

- SIMATIC HMI connection box Standard / connection box Advanced,
- Connection module Basic PN (for control cabinet installation), or
- SINUMERIK MPP 310 IEH / MPP 398 IEH / MPP 464 IEH / MPP 483 IEH

Note

Use the switch, e.g. SCALANCE XB008G, also for further I/O devices (SIMATIC ITC V3, SINUMERIK MCP, handwheels, etc.).

Note

It is possible to use the mini handheld terminal in combination with the MCU.

To do so, connect the handheld terminal to the SINUMERIK MCU via the SINUMERIK MCP Interface PN or the MCP 398C PN.

12.3 Setting up the PLC configuration for the HT function

Introduction

Communication for the devices involved, e.g. handheld terminals, takes place via the Ethernet and PROFINET interfaces.

So that all participants are addressed via the MCU, the IP address of the PLC device configuration and the PROFINET communication path must be correctly preset.

Requirements

- The application PCU-Basesoftware /IPC from V15.0 SP1 is installed on the MCU IPC system.
- The blocks for handheld terminals, Ethernet communication and other I/O devices are created and configured in the TIA Portal project.

More information

For more information on the function and block configuration of handheld terminals, refer to the Function Manual PLC Basic Program.

More information on configuration is also provided in the online help of TIA Portal.

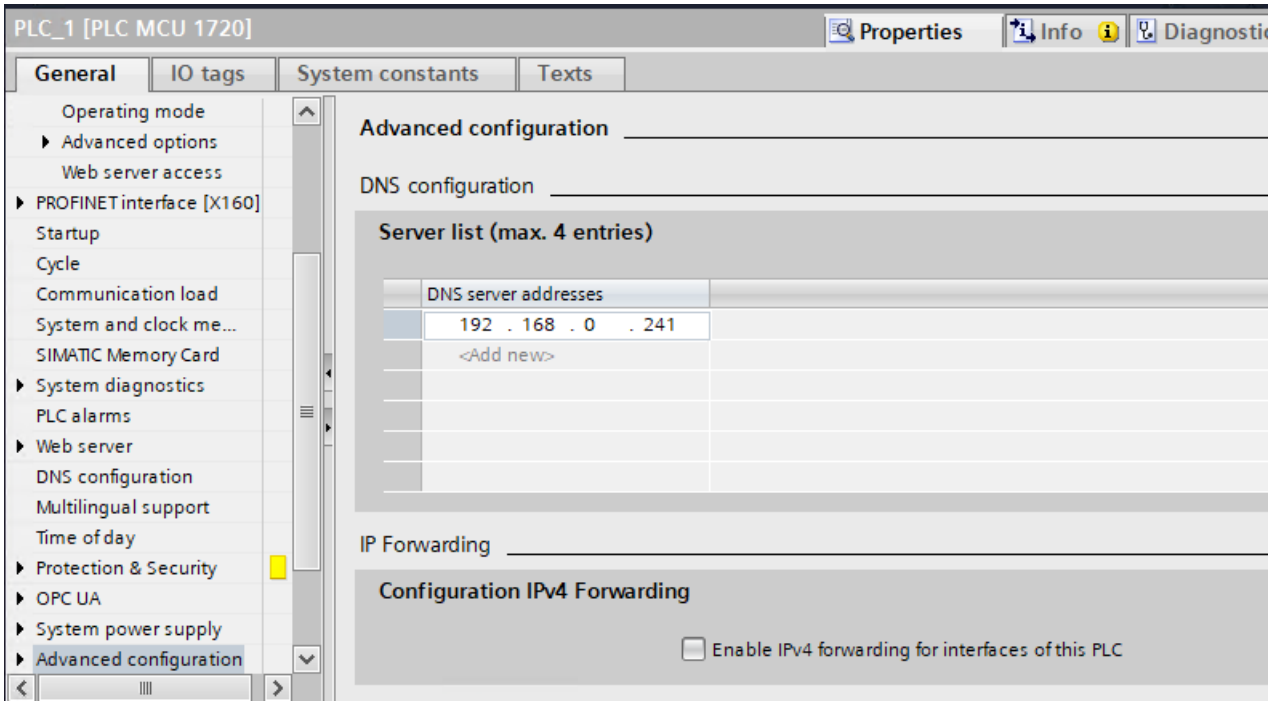
An HT 2 example of connection and key control can be found in the SiePortal (https://support.industry.siemens.com/cs/document/109783834/ht2-on-sinumerik-one?dti=0&lc=en-WW).

Procedure for PLC device configuration

Store the IP address of the Ethernet interface **X2 P1** as DNS server address:

1. In the network view, click the PLC in the basic rack of the SINUMERIK MCU.
2. Switch to Inspector window "Properties > General".

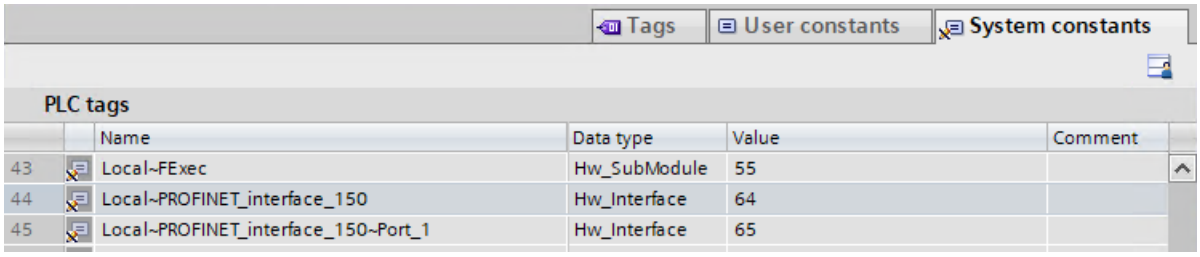
Under "Advanced configuration", insert the DNS server address **192.168.0.241**.



Procedure for parameterizing PROFINET communication

Parameterize the communication path for **LBP_OpUnitComm** in the PLC basic program for the PROFINET interface **X150**:

1. Open the "PLC tags" editor in the "System constants" tab and check the value for the PROFINET interface **X150**, e.g. the **value 64**.



2. In **Startup [OB100]**, call **LBP_ConfigBP [FC1]**.
3. In the called **LBP_ConfigBP [FC1]**, insert the program code for **LBP_OpUnitComm** with the value for the PROFINET interface **X150**:
   `OpUnitInterfaceId:=64, // Local~PROFINET_interface_150`

Example of HT 10 connection

```
...
HTIf:=5, // SINUMERIK HT
HTIn:="HT10-Data".HT10in,
HTOut:="HT10-Data".HT10out,
HTAdr:=14, // Box-ID - Connection Box of HT10
HTStop:="HT10-Data".HtMcpStop,
```

```
HTNotSend:="HT10-Data".HtMcpNotSend,
...
OpKeyNum:=1, // Direct Keys
Op1KeyIn:="HT10-Data"."HT10-VDCKin",
Op1KeyOut:="HT10-Data"."HT10-VDCKout",
Op1KeyBusAdr:=14, // Box-ID - Connection Box of HT10
...
Op1KeyStop:="HT10-Data".HtDckStop,
...
Op1KeyNotSend:="HT10-Data".HtDckNotSend,
...
OpUnitInterfaceId:=64, // Local~PROFINET_interface_150
...
```

Result

The SINUMERIK PLC basic program is set up for the use of handheld terminals or other I/O devices with the MCU.

Appendix

A

A.1 Script example for BitLocker activation

Script for ps1 format

Use the script example for BitLocker encryption in the Microsoft Windows PowerShell (Page 250) application.

```
#!pwsh

#Requires -Version 5.1
#Requires -RunAsAdministrator

# Script params and variables
[CmdletBinding()]
param(
    [Parameter(Mandatory=$false)][string]$RecoveryPassword=$null,
    [Parameter(Mandatory=$false)][string]$RecoveryPasswordFile=$null,

    [Parameter(Mandatory=$false)][string[]]$Partitions=@()
)

# enable BitLocker for volumes
function enableBitlockerForVolumes
{
    trap { continue }
    # enable bitlocker for volume system drive
    $bitlockerSystemVolume = Enable-BitLocker -MountPoint "${env:SystemDrive}"
-EncryptionMethod XtsAes256 -TpmProtector -SkipHardwareTest -ErrorAction SilentlyContinue
    if (-not $bitlockerSystemVolume) {
        # error activating bitlocker on system drive
        return $false
    }
    # add recovery password to volume system drive
    if ($RecoveryPassword) {
       $bitlockerSystemVolume = Add-BitLockerKeyProtector -MountPoint "${env:SystemDrive}"
-RecoveryPasswordProtector -RecoveryPassword "$RecoveryPassword" -ErrorAction
SilentlyContinue
    }
    else {
       $bitlockerSystemVolume = Add-BitLockerKeyProtector -MountPoint "${env:SystemDrive}"
-RecoveryPasswordProtector -ErrorAction SilentlyContinue
    }
```

```
    if (-not $bitlockerSystemVolume) {
        # couldn't add recovery password to system drive
        return $false
    }
    # get recovery password from volume info
    $foundRcvPwd = $false
    foreach ($protector in $bitlockerSystemVolume.KeyProtector) {
        if ($protector.KeyProtectorType -eq "RecoveryPassword") {
            $script:RecoveryPassword = $protector.RecoveryPassword
            $foundRcvPwd = $true
            break
        }
    }
    if (-not $foundRcvPwd) {
        # no recovery password for system volume
        return $false
    }
    # enable bitlocker for additional volumes
    $bitlockerVolumes = Enable-BitLocker -MountPoint $Partitions -EncryptionMethod
XtsAes256 -RecoveryPasswordProtector -RecoveryPassword "$RecoveryPassword"
-SkipHardwareTest -ErrorAction SilentlyContinue
    if (-not $bitlockerVolumes) {
        # error activating bitlocker on additional volumes
        return $false
    }
    # enable auto unlock for additional volumes
    $bitlockerVolumes = Enable-BitLockerAutoUnlock -MountPoint $Partitions -ErrorAction
SilentlyContinue
    if (-not $bitlockerVolumes) {
        # error enabling auto unlock bitlocker for additional volumes
        return $false
    }
    # save recovery password in file if specified
    if ($RecoveryPasswordFile) {
        $RecoveryPassword | Out-File -FilePath $RecoveryPasswordFile -Encoding ASCII
-ErrorAction SilentlyContinue -ErrorVariable saveRcvPwdError
        if ($saveRcvPwdError) {
            # couldn't save recovery password in file
        }
        else {
            # saved recovery password in file
        }
    }

    return $true
}

$ret = enableBitlockerForVolumes
```

A.2 Abbreviations

ACX	Compressed format for XML
ALM	Active Line Module
APC	Advanced Position Control (SINUMERIK option M13)
AUTO	AUTO mode: Continuous and automatic execution of programs
BERO	Proximity limit switch
BI	Binector Input
BICO	Binector Connector
BO	Binector Output
CFast	CF + AST (CompactFlash ATA Serial Transfer)
CI	Connector Input
CNC	Computerized Numerical Control: Computerized numerical control
CO	Connector Output
CoL	Certificate of License
CP	Communication Processor: Communications processor
CPU	Central Processing Unit: Central processing unit
CU	Contol Unit
DHCP	Dynamic Host Configuration Protocol: Protocol for automatic assignment of IP addresses from a DHCP server to a client computer.
DO	Drive Object: Drive object
DP	Distributed I/O
DRAM	Dynamic Random Access Memory
DRF	Differenzial Resolver Funktion: Differential function for rotary resolver
DRIVE-CLiQ	Drive Component Link with IQ
DSC	Dynamic Stiffness Control: Dynamic stiffness control
DWORD	Doubleword
EBS	Emergency Boot System
ESD	Electrostatic Sensitive Device
EMC	Electro-Magnetic Compatibility
EN	European standard
EPos	Basic positioning (SINAMICS S120)
GECOS	General Electric Comprehensive Operating System: Information about the identity of a user under Linux
GSD	Device master file
GUD	Global User Data
IPC	Industrial PC
IPO	Interpolator
IRT	Isochronous Real-Time communication
JOG	JOG mode: manual mode for setting up the machine
LAN	Local Area Network
LED	Light-Emitting Diode: Light-emitting-diode display
LUD	Local User Data
MCU	Motion Control Unit

MD	Machine Data
MDI	MDI mode (Manual Data Automatic): Enter program blocks manually and execute
MM	Motor Module
MCP	Machine Control Panel
NC	Numerical Control: Numerical control
NCK	Numerical Control Kernel: Numeric kernel with block preparation, traversing range, etc.
PIO	Process Image Output
PII	Process Image Input
PCU	PC Unit: computer unit
PELV	Protective Extra Low Voltage
PG	Programming device
PLC	Programmable Logic Control: (component of the CNC)
PM	Power Module
PUD	Program global User Data
RAM	Random Access Memory: Program memory that can be read and written
REF POINT	Function for approaching the reference point in JOG mode.
REPOS	Function for repositioning in JOG mode
SD	Setting Data
SD card	SecureDigital Card: SD Card
SLM	Smart Line Module
SMC	Sensor Module Cabinet Mounted
SME	Sensor Module Externally Mounted
TEACH IN	Function for creating programs in interactive mode with the machine in MDI and AUTO modes
TCU	Thin Client Unit
USB	Universal Serial Bus
WAL	Work Area Limits
XML	Extensible Markup Language

A.3 Information about third-party software used

Copyright 1995 Sun Microsystems, Inc.

Printed in the United States of America.

All Rights Reserved.

This software product (LICENSED PRODUCT), implementing the Object Management Group's "Internet Inter-ORB Protocol", is protected by copyright and is distributed under the following license restricting its use. Portions of LICENSED PRODUCT may be protected by one or more U.S. or foreign patents, or pending applications.

LICENSED PRODUCT is made available for your use provided that you include this license and copyright notice on all media and documentation and the software program in which this product is incorporated in whole or part. You may copy, modify, distribute, or sublicense the LICENCED PRODUCT without charge as part of a product or software program developed by you, so long as you preserve the functionality of interoperating with the Object Management Group's "Internet Inter-ORB Protocol" version one. However, any uses other than the foregoing uses shall require the express written consent of Sun Microsystems, Inc.

The names of Sun Microsystems, Inc. and any of its subsidiaries or affiliates may not be used in advertising or publicity pertaining to distribution of the LICENSED PRODUCT as permitted herein. This license is effective until terminated by Sun for failure to comply with this license. Upon termination, you shall destroy or return all code and documentation for the LICENSED PRODUCT.

LICENSED PRODUCT IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

LICENSED PRODUCT IS PROVIDED WITH NO SUPPORT AND WITHOUT ANY OBLIGATION ON THE PART OF SUN OR ANY OF ITS SUBSIDIARIES OR AFFILIATES TO ASSIST IN ITS USE, CORRECTION, MODIFICATION OR ENHANCEMENT. SUN OR ANY OF ITS SUBSIDIARIES OR AFFILIATES SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY LICENSED PRODUCT OR ANY PART THEREOF.

IN NO EVENT WILL SUN OR ANY OF ITS SUBSIDIARIES OR AFFILIATES BE LIABLE FOR ANY LOST REVENUE OR PROFITS OR OTHER SPECIAL, INDIRECT AND CONSEQUENTIAL DAMAGES, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

SunOS, SunSoft, Sun, Solaris, Sun Microsystems and the Sun logo are trademarks or registered trademarks of Sun Microsystems, Inc.

SunSoft, Inc.
2550 Garcia Avenue
Mountain View, California 94043

Copyright (c) 1991 by AT&T.

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.
THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTY.

IN PARTICULAR, NEITHER THE AUTHOR NOR AT&T MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

This product includes software developed by the University of California, Berkeley and its contributors.
QLocale's data is based on Common Locale Data Repository v1.6.1.

Note

You can find additional information on the product DVD in the Readme_OSS file about the third-party software used.

Index

A

Access levels, 57
Actual values
  Cyclic communication, 142
ARC archive
  Importing, 183
Archiving, 180
Autologon
  Switch to Service Desktop, 51
Autologon mode, 52
AutoRepeat, 253
Axis assignment, 168

B

Backup time, 217
Basic PLC program
  Execution structure, 86
Batch file
  USVShutdown.bat, 211, 214
Batch processing file, (Batch file)
BitLocker, 246
  Activate setup, 248
  Activate via script, 250
  Activating via Microsoft Windows, 249
Block
  Conflicts during copying, 107
Blocks
  editing, 97
  open, 97
Boot stick, 289

C

Certificate of License (CoL/eCoL), 64, 68
Channel axes, 167
Color depth, 209
Command
  control userpasswords2, 52
  sc_show_net, 302
  sc_usb disable, 205
  sc_usb enable, 205
  sc_vncpwd reset, 303
  sc_vncpwd set, 303
Communications
  establishing, 79
Company network
  Defining the password, 303
Compile
  Hardware, 78
Configuration file
  Archiving, 198
  basesys.ini, 205, 293
  pcuhwsvc.ini, 253
  PCUInst.ini, 258, 259, 260, 261
  servicesystem.ini, 219, 220, 221
  setup.ini, 200
  sinumerikvnc.ini, 303
  slrs.ini, 53
  tcu.ini, 207, 209, 303
  Templates, 198
Configure for CMC, 268

D

Data backup, 180
Device configuration detection
  Correcting the resulting topology, 124
  Creating the determined topology in the Startdrive project, 125
DHCP, 197
Dialog box
  netplwiz, 52
  ServiceCenter Backup/Restore, 219, 220, 221
Directory
  C:\ProgramData, 198
Disk image
  Restoring, 278, 283
  Troubleshooting, 280, 285
Drive
  Isochronous IO device, 137
  Sync domains, 131
  Sync master, 135
Drives
  Cyclic data exchange, 139
DSF archive
  adapt, 188
  Creating, 186
  Importing, 183

E

Emergency Boot System, 191, 289
Extended download, 84

F

FBD, 97
File and printer sharing, 205

G

Geometry axes, 167
GSDML file, 148

H

Handheld terminal
  Configuration of the connection, 311
  Connecting, 310
  HT 10, 308
  HT 2, 307
Hard disk
  Replacing, 301
Hardware
  compile, 78
Hardware reference, 63
Hardware serial number, 63, 68

I

Initialization files, (Configuration file)
Input area scheme, (Keyboard layout)
Insert
  MCU, 74
Installation, 189
Interface
  Ethernet, 197
  X1, 197
  X2, 197
  X3, 197
  X4, 197

K

Key, (Repeat function)
  Key filter, 253
Key filter, 253
Keyboard layout, 206

L

LAD, 97
Language
  Configuring the keyboard layout, (Keyboard layout)
Language bar, (Keyboard layout)
License, 68
License database, 66
License information, 63
License key, 63, 69
License number, 69
Log file
  CBS.log, 253
  PCUHardwareservice.log, 255, 256, 257
  PCUInstaller_C.log, 265, 266, 267, 268
  PCUInstaller_S.log, 265, 266, 267, 268
  Setup-specific, 267
Log File, (Log file)

M

Machine axes, 167
MCU
  Insert, 74
MCU components
  checking, 45
  Communication settings, 45
  Configuring, 45
  Installing the PCU base, 45
MCU Interfaces, 39
Measuring probe
  Central, 177
  Distributed, 176

N

NCK commissioning switch, 41
Network
  Adapting settings, 204, 220, 221
  Company network, 197
  Domain, 204
  IP address, 204
  System network, 197
Network protocol
  SNMP, (SNMP)
Network security
  Define password for VNC server, 303
Network share
  Driven on PG/PC, 297
Number range
  for user program, 108

O

Option, 69

P

Password
Administrator account, 203
Authentication for SSH encryption, 305
change, 61
Configure for VNC server, 303
enter, 58
For network drive, 285
Rules, 60
Security, 58
PCU Installer
Activating, 258, 259
Configure for CMC, 268
Configuring, 260, 261
Log file, 267, (Log file)
PCUInst.ini, 261
Troubleshooting, 259, 266
Using, 266
PLC
Communication setup, 79
Mode selector switch, 41
PLC basic program
Assignment overview, 108
Blocks with user-specific adaptations, 97
PROFINET
Configuring, 77
PROFINET connection, 173
PROFINET interface
Configuring, 76
PROFIsafe
Address, 142, 144
Programming language
FBD, 97
LAD, 97
STL, 97

R

Remote access, 303
Via VNC server, 303
With SSH encryption, 304
Runtime
Software, 75

S

Screen resolution, 207
SD Card, 63, 68
Serial number
Readout, 62
Service Center
Decrypting BitLocker, 287
Service Desktop, 51
Service system
Creating for the MCU, 191
Service system for PCU Base, 289
Set PG/PC interface, 53
Setpoints
Cyclic communication, 144
Shutdown, 210
SIMOTION
Interconnecting ports, 133
SINUMERIK ONE Commissioning
Communication settings, 54
Installing, 47
Starting, 55
SINUMERIK ONE Commissioning Tool, 18
SINUMERIK Operate /PCU Modular
Autologon mode, 50
Communication settings, 54
Configuring the display size, 53
Installing, 49
SINUMERIK Operate /PCU Modular
Starting, 55
SINUMERIK Operate /PCU Modular
Benefits, 48
SITOP UPS, 210
Software configuration
load, 84
Software product, 63
SSD
Replacing, 301
SSH encryption, 304, 305
Startdrive, 120
STL, 97

T

Technology
Milling, 166
Turning, 166
Telegram
105, 140
136, 140

370, 140
391, 140
Telegram configuration, 140, 141
Telegrams
Adding, 146
Extending, 146
Rules, 19
Troubleshooting
PCU Installer, 259, 266
Restore failure, 280, 285

U

Uninterruptible power supply, 210
Update, 189
Upgrade, 189
USB flash drive
Deactivate network access, 205
with emergency boot system, 289
USB interface
Activating, 205
Disabling, 205
User account, (Setting up for autologon mode)
Setting up, 203
User administration, 203
User views, 166

V

VNC Viewer, 303

W

Web License Manager, 65