

# SIEMENS

## SINUMERIK

### SINUMERIK ONE New installation and upgrade

#### Installation Manual

Fundamental safety instructions	1
Introduction	2
Delivery condition of the system	3
New installation	4
Upgrade	5
Device replacement	6
Service tasks	7
Abbreviations	A

Valid for:

CNC software for SINUMERIK ONE V6.15  
Linux basic software V6.00

07/2021

A5E49062488B AC



## 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.

 <b>DANGER</b>
indicates that death or severe personal injury <b>will</b> result if proper precautions are not taken.

 <b>WARNING</b>
indicates that death or severe personal injury <b>may</b> result if proper precautions are not taken.

 <b>CAUTION</b>
indicates that minor personal injury can result if proper precautions are not taken.

<b>NOTICE</b>
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:

 <b>WARNING</b>
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 AG. 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.

# Table of contents

<b>1</b>	<b>Fundamental safety instructions</b> .....	<b>5</b>
1.1	General safety instructions.....	5
1.2	Equipment damage due to electric fields or electrostatic discharge .....	9
1.3	Warranty and liability for application examples .....	10
1.4	Security information .....	11
1.5	Residual risks of power drive systems .....	12
<b>2</b>	<b>Introduction</b> .....	<b>13</b>
2.1	About this documentation .....	13
2.2	Documentation on the internet.....	15
2.3	Service and Support.....	16
2.4	Important product information .....	18
<b>3</b>	<b>Delivery condition of the system</b> .....	<b>19</b>
<b>4</b>	<b>New installation</b> .....	<b>21</b>
4.1	Procedure for new installation.....	21
4.2	This is how you create a SINUMERIK service system .....	22
4.3	How to create a backup of the SSD memory .....	24
4.4	How to create a backup of the SD Card .....	25
4.5	How to create a system restore point.....	26
4.6	How to deactivate the internal SINUMERIK Operate .....	28
<b>5</b>	<b>Upgrade</b> .....	<b>29</b>
5.1	How to check the installed software version .....	29
5.2	How install a software update .....	30
5.3	How to create a defined initial state.....	31
5.4	This is how you load factory settings .....	32
<b>6</b>	<b>Device replacement</b> .....	<b>33</b>
6.1	Procedure for replacing an NCU/PPU .....	33
6.2	Procedure for replacing an SD Card.....	34
6.3	How to check the SD Card .....	35
6.4	How to restore the SSD memory.....	36
<b>7</b>	<b>Service tasks</b> .....	<b>37</b>
7.1	Service shell .....	37

7.1.1	Help .....	39
7.1.2	Clear sdcard .....	40
7.1.3	Disable .....	40
7.1.4	Enable .....	41
7.1.5	Distribute.....	42
7.1.6	Vncpwd .....	42
7.2	Configuration file "basesys.ini" .....	44
7.3	Open source software .....	46
<b>A</b>	<b>Abbreviations.....</b>	<b>47</b>
A.1	Abbreviations .....	47
	<b>Index .....</b>	<b>49</b>

# Fundamental safety instructions

## 1.1 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.

- Be sure to only use screwdrivers which exactly match the heads of the screws.
- 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.

 **WARNING****Spread of fire from built-in devices**

In the event of fire outbreak, the enclosures of built-in devices cannot prevent the escape of fire and smoke. This can result in serious personal injury or property damage.

- Install built-in units in a suitable metal cabinet in such a way that personnel are protected against fire and smoke, or take other appropriate measures to protect personnel.
- Ensure that smoke can only escape via controlled and monitored paths.

 **WARNING****Unexpected movement of machines caused by radio devices or mobile phones**

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

- Therefore, if you move closer than 20 cm to the components, be sure to switch off radio devices or mobile telephones.
- Use the "SIEMENS Industry Online Support app" only on equipment that has already been switched off.

 **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 notices for Safety Integrated functions**

If you want to use Safety Integrated functions, you must observe the safety notices in the Safety Integrated manuals.



**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.

## 1.2 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 or 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).

## 1.3 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 specific customer solutions, but are only intended to provide support for 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.

## 1.4 Security information

Siemens provides products and solutions with industrial security 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 security 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 security measures that may be implemented, please visit

<https://www.siemens.com/industrialsecurity> (<https://www.siemens.com/industrialsecurity>).

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 Security RSS Feed under

<https://www.siemens.com/industrialsecurity> (<https://new.siemens.com/global/en/products/services/cert.html#Subscriptions>).

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 holistic, state-of-the-art industrial security concept for the installation or machine.
- Make sure that you include all installed products into the holistic industrial security concept.
- Protect files stored on exchangeable storage media from malicious software by with suitable protection measures, e.g. virus scanners.
- On completion of commissioning, check all security-related settings.

## 1.5 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 installer 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 and/or software errors in the sensors, control system, actuators, and cables 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, including open flames, as well as emissions of light, noise, particles, gases, etc., can occur inside and outside the components under fault conditions caused by, for example:
  - Component failure
  - Software errors
  - Operation and/or environmental conditions outside the specification
  - External influences/damage
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 communication systems, e.g. ripple-control transmitters or data communication via the network

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

# Introduction

## 2.1 About this documentation

### About SINUMERIK

From basic standard machines to modular premium machines, SINUMERIK CNC controls offer the optimum solution for every machine concept. SINUMERIK is the highly productive automation solution for all areas of production:

- Production of individual parts or mass production
- Simple or complex workpieces
- Prototype production
- Tool and mold making
- Large series production

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

### Target group

This documentation addresses planners, project engineers and commissioning engineers, and enables the target group to professionally commission the system. Re-installation of the CNC software on the control and upgrade with the SINUMERIK service system.

### Standard scope

This documentation only describes the functionality of the standard version. The standard scope may deviate from the functionality of the system 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 of the 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.

## Definition of terms

FW (visible as FW version on the SINUMERIK Operate) is the so-called **coreboot** and contains the boot software including the system bootloader. The system bootloader version is displayed on the SINUMERIK Operate, but is always part of the FW and cannot be upgraded separately.

**OnboardSW** is the initNCU and is mainly used to import the CNC software and other software packages.

## Notation

The **SINUMERIK service system (eboot)** is also known as the emergency boot system for NCU and is available via the usual sales channels. The term "SINUMERIK service system" is used in the description.

## 2.2 Documentation on the internet

### Siemens Industry Online Support (SIOS)

The complete documentation from version 6.13 on can be found under SINUMERIK ONE (<https://support.industry.siemens.com/cs/document/109768483>) documentation overview



### Feedback on the technical documentation

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

### 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. The "Configuration" link is available for Siemens content that supports the mySupport documentation application.

Start the application via "My documentation" on the mySupport homepage (<https://support.industry.siemens.com/cs/ww/en/my>).

## 2.3 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 for on the go





With the award-winning "Siemens 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 "Siemens Industry Online Support" app is available for Apple iOS and Android.

### **Data matrix code on the nameplate**

The data matrix code on the nameplate contains the specific device data. This code can be read with any smartphone and technical information about the device displayed via the "Industry Online Support" mobile app.

## 2.4 Important product information

### 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>)

### Compliance with the General Data Protection Regulation

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

For this product, this means:

The product does not process or store any personal data, only technical function data (e.g. time stamps). If the user links this data with other data (e.g. shift plans) or if he/she stores person-related data on the same data medium (e.g. hard disk), thus personalizing this data, he/she must ensure compliance with the applicable data protection stipulations.

## Delivery condition of the system

### Area of validity

This document applies to SINUMERIK ONE NCU 17x0 and PPU 1740.

### Directories SSD (16 GB)

The following directories are available:

Directory	Content
/addon	Software expansions
/siemens	CNC software
/system	Open source parts of the CNC software
/var/log/messages	Log file (same as event.log under Windows)

### Directories SD card (8 GB)

The SD card contains both a Linux partition (EXT4) and an FAT partition:

- The **24 MB** FAT partition is reserved for data that is exchanged with PC systems, e.g. for backing up license information or for initial network configuration.
- The Linux partition is mainly provided for storing the data in the **/oem** and **/user** directories.

At runtime, the following directories are present on the Linux partition of the SD card:

Directory	Content
/install/siemens	Restore point of the CNC software
/install/addon	Restore point of the software add-ons
/keys	Licensing
/oem	Additional software and configurations of the machine manufacturer
/user	End user data
/user/system/etc	Configuration file basesys.ini (template)
/user/common/tcu	TCU configuration files

Files in the directory under **/user** always have priority over files with the same name in the directory **/oem** → **/addon** → **/siemens**.

## References

The following states are described in these chapters:

①	New installation (Page 21)	NCU without CNC software + brand-new SD card
②	Procedure for replacing an NCU/PPU (Page 33)	NCU without CNC software + SD card with OEM data
③	Procedure for replacing an SD Card (Page 34)	NCU with CNC software + brand-new SD card
④	Upgrade (Page 29)	NCU with CNC software + SD card with OEM data

## More information

The meaning of the LED and 7-segment status displays can be found in the respective hardware description (<https://support.industry.siemens.com/cs/document/109768483>).

# New installation

## 4.1 Procedure for new installation

### Installing CNC software

Requirement:

- The NCU or PPU is connected.
- The NCU or PPU and the SD Card with the CNC software are in delivery condition.
- The original licensed SINUMERIK ONE SD Card is inserted.

Procedure:

- Switch on the system:  
During run-up, the Linux partition of the SD Card is adapted for operation and the CNC software V6.x supplied on the SD Card is automatically installed on the SSD memory. This procedure is indicated on the 7-segment display by a rotating circle.
- The NCU or PPU is then automatically restarted.
- Startup of the CNC software with SINUMERIK Operate.
- Commissioning of the NCU or PPU via TIA Portal and Operate or, if available, read in the series commissioning archive (\*.dsf).

Alternative:

- If the current or required CNC software (Page 29) has not been installed from the SD Card, perform a software update (Page 30).

## 4.2 This is how you create a SINUMERIK service system

### Application

The "SINUMERIK service system (eboot)" starts up the NCU from the USB storage medium. The SINUMERIK service system supports you in the following tasks:

- New installation
- Upgrade (Page 29)
- Device replacement (Page 33)
- Service tasks (Page 37)

---

#### Note

##### Designation

The SINUMERIK service system is also known as the Emergency Boot System for NCU and is available via the usual sales channels.

---

### Requirements

The following requirements are necessary to create a SINUMERIK service system:

- The use of the following USB flash drive is preferred: Article number 6AV6881-0AS42-0AA1.
- Administrator rights on PG/PC: All data on the USB storage medium will be deleted.
- A program for writing the image file: for example, Access MyMachine /P2P or Win32 Disk Imager (OSS (Page 46)).
- Image file linuxbase.img for SINUMERIK ONE.

### Procedure

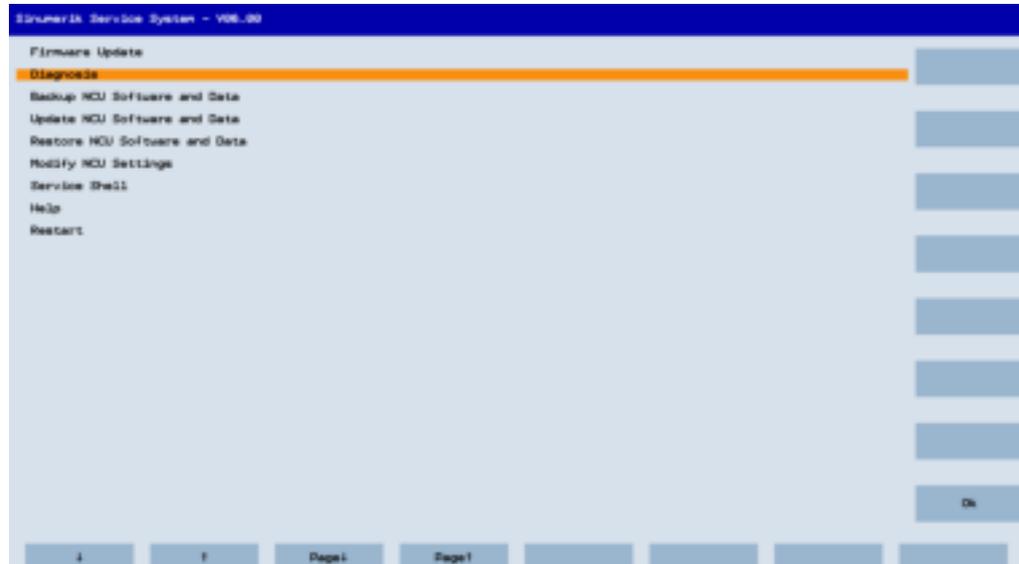
To create a SINUMERIK service system on a USB storage medium:

1. Copy the image file to a local drive of the PG/PC.
2. Connect the USB storage medium to a PG/PC. Determine in Windows Explorer which drive letter has been assigned to the USB storage medium.
3. Copy the image file to the USB storage medium using the respective tool. The transfer is optimized for USB 3.0.
4. Switch off the control system. Connect the SINUMERIK service system to the USB interface X125 or X135 of the NCU.
5. Set the NCK rotary switch to a position other than zero. Switch the control system back on again:  
The image file is unzipped the first time the NCU is started up with the USB storage medium: This process is indicated by "P" in the 7-segment display. Only then can the USB storage medium be used as SINUMERIK service system and the complete storage capacity is available.

2 partitions are created on the SINUMERIK service system:

- A Linux partition that is not available under Windows.
- A FAT partition to save backup files or software updates.  
The FAT partition is available under both Linux and Windows for reading and writing. The FAT partition can be addressed under the path `/data` in a Service Shell under Linux.

## Run up with the SINUMERIK service system



## Operating the SINUMERIK service system

The SINUMERIK service system is prepared for operation both with keys and a Touch Panel. An onboard keyboard (Page 37) is displayed in the respective menus for this purpose.

## 4.3 How to create a backup of the SSD memory

### Procedure

To create a backup of the SSD memory (CNC software and software extensions):

1. Run-up of the control system with SINUMERIK service system.
2. In the main menu, select the menu command "Backup NCU and Data".
3. Select the menu command "Backup SSD system (/siemens, /addon) partition to USB stick" to back up the data on the SINUMERIK service system.



4. Enter a name for the backup file and confirm with OK.

**Result:** The data backup is stored in the following directory: /data/<name>.tgz

Alternatively, you can create a data backup on a network drive:

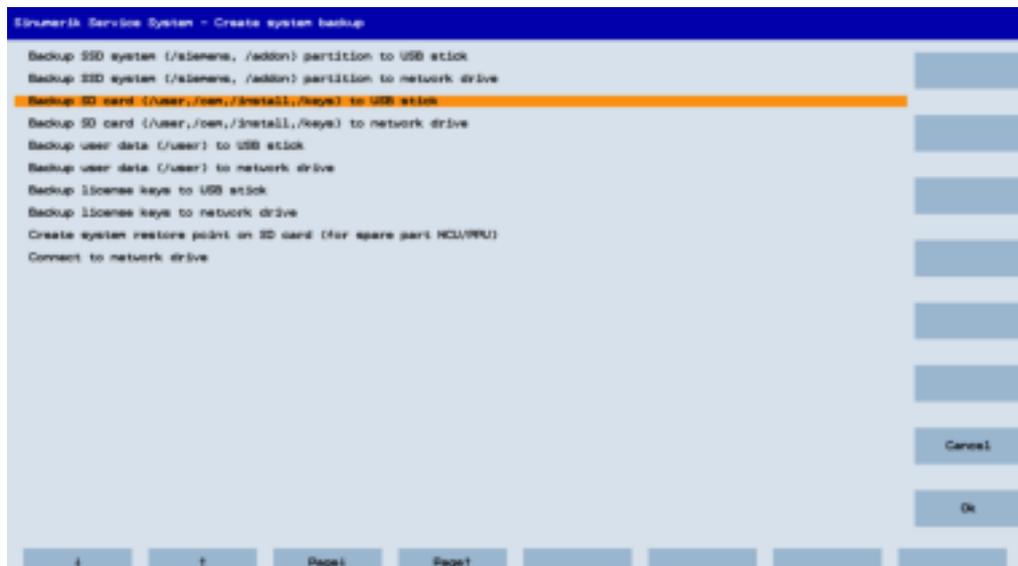
1. Select the bottom-most menu command "Connect to network drive" to connect a network drive.
2. Select the menu command "Backup SSD system (/siemens, /addon) partition to network drive" to back up the data on the network drive.
3. Enter a name for the backup file and confirm with OK.

## 4.4 How to create a backup of the SD Card

### Procedure

To create a complete data backup (including licensing) of the SD Card:

1. Run-up of the control system with SINUMERIK service system.
2. In the main menu, select the menu command "Backup NCU and Data".
3. Select the menu command "Backup SD card (/user, /oem, /install, /keys) to USB stick" to back up the data on the SINUMERIK service system.



4. Enter a name for the backup file and confirm with OK.

**Result:** The data backup is created on the following path: /data/<name>.tgz

Alternatively, you can create a data backup on a network drive:

1. Select the bottom-most menu command "Connect to network drive" to connect a network drive.
2. Select the menu command "Backup SD card (/user, /oem, /install, /keys) to network drive" to back up the data on the network drive.
3. Enter a name for the backup file and confirm with OK.

## 4.5 How to create a system restore point

### Objective

A restore point writes a compressed copy of the CNC software and software add-ons installed on the SSD memory to the SD Card so that in case of a spare part replacement only the SD Card has to be inserted into the spare part NCU or PPU.

To restore the SSD memory after replacing a part (Page 33), you need one of the following installation files (\*.tgz):

- Restore point: /install/siemens/snapshot-siemens\_<xxx>.tgz

or:

- Original CNC software: /install/siemens/current.tgz

---

### Note

#### Creating a restore point

When creating a restore point, an existing "current.tgz" is overwritten, i.e. the CNC software supplied with the SD Card is replaced by the software currently installed on the NCU/PPU.

---

## Procedure

To create a restore point on the SD Card:

1. Run-up of the control system with SINUMERIK service system.
2. In the main menu, select the menu command "Backup NCU Software and Data".  
Alternative: In the main menu, select the menu command "Update NCU Software and Data".
3. Select the menu command "Create system restore point on SD card (for spare part NCU/PPU)":



Creating a restore point can take a few minutes:



## 4.6 How to deactivate the internal SINUMERIK Operate

### Proceed as follows

The "internal" SINUMERIK Operate is part of the CNC software. When a SINUMERIK Operate is used on an IPC instead of a TCU, the internal SINUMERIK Operate must be deactivated:

1. Startup of the control system with SINUMERIK service system.
2. In the main menu, select the menu item "Modify NCU Settings".
3. Select the menu item "Disable internal HMI (currently enabled)":



After this, you can install and use SINUMERIK Operate on an IPC under Windows.

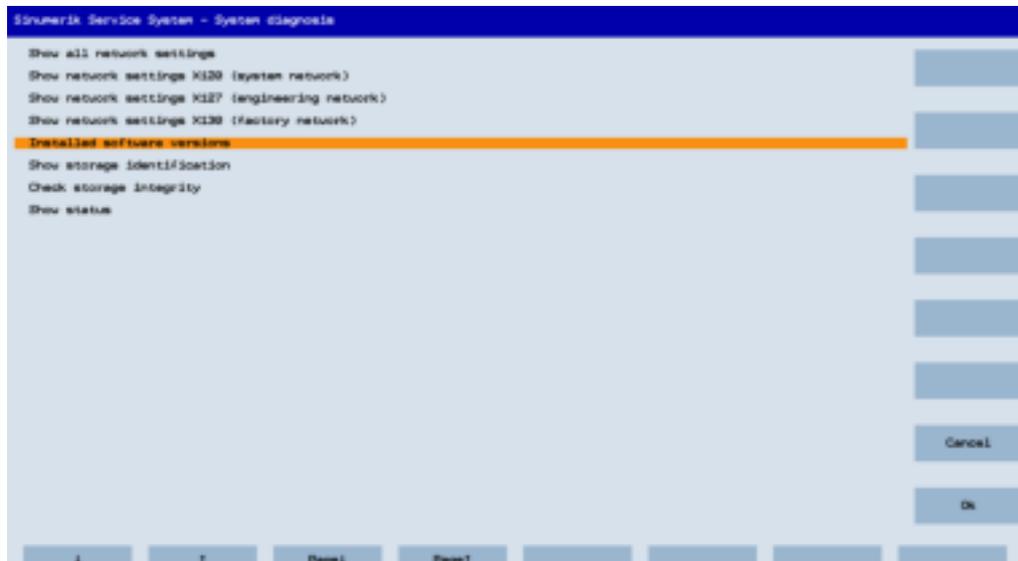
# Upgrade

## 5.1 How to check the installed software version

### Procedure

To display the installed software version:

1. Run-up of the control system with SINUMERIK service system.
2. In the main menu, select the menu command "Diagnosis".
3. Select the menu command "Installed software versions":



### Example:



## 5.2 How install a software update

### Procedure

To install a software update:

1. Copy the new CNC software package (\*.tgz) to the FAT partition of the SINUMERIK service system.
2. Run-up of the control system with SINUMERIK service system.
3. In the main menu, select the menu command "Update NCU Software and Data".
4. Select the menu command "Update system software from USB stick and create system restore point" or "Update system software from USB stick without new system restore point":



This operation can take several minutes.

---

### Note

#### Restore point

A software update can be installed with or without creating a restore point.

A restore point writes a compressed copy of the CNC software and software add-ons installed on the SSD memory to the SD Card so that in case of a spare part replacement (Page 33) only the SD Card has to be inserted into the new NCU or PPU.

---

## 5.3 How to create a defined initial state

### Procedure

In order to establish a defined initial state, all data on the SD Card is first deleted and then the CNC software is reinstalled:

1. Run-up of the control system with SINUMERIK service system.
2. In the main menu, select the menu command "Update NCU and Data".
3. Select the menu command "Clear all + reinstall system SW from USB stick and create system restore point":



This operation can take several minutes.

4. After this, a system restart is necessary.

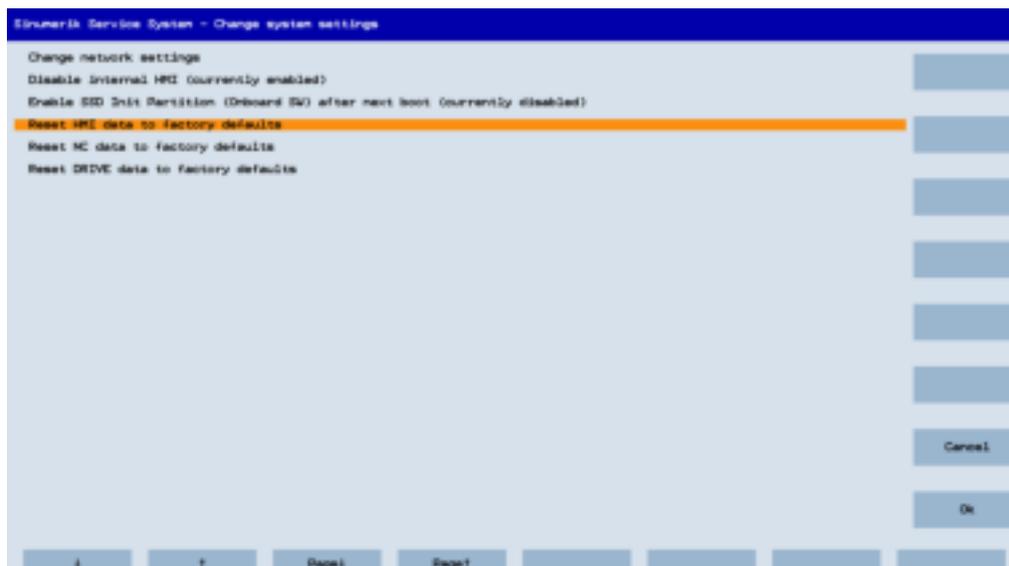
## 5.4 This is how you load factory settings

### Procedure

DSF archives stored on the SD Card are not affected by this.

To load factory settings:

1. Run-up of the control system with SINUMERIK service system.
2. In the main menu, select the menu command "Modify NCU Settings".
3. Select the menu command "Reset HMI data to factory settings" to delete all of the data in the oem/sinumerik/hmi directory:



4. Select the menu command "Reset NC data to factory settings" to delete all of the data in the /oem/sinumerik/nck directory.
5. Select the menu command "Reset DRIVE data to factory settings" to delete all of the data in the /oem/sinamics/data directory.

---

### Note

#### Factory settings of the PLC

No PLC data is processed with the SINUMERIK service system.

To reset the PLC to factory settings, you have the following options:

- Toggle switch in position MRES
- SIMATIC STEP 7 Professional (TIA Portal)

Further information can be found at: SINUMERIK ONE (<https://support.industry.siemens.com/cs/document/109768483>)

---

## Device replacement

### 6.1 Procedure for replacing an NCU/PPU

#### Replacing the NCU or PPU

Requirement:

- The defective NCU or PPU has been replaced with a replacement device. All of the plug-in connections have been reconnected
- The SD Card contains a restore point (Page 26) or a CNC software package (current.tgz) in the `/install/siemens` directory.
- Before the defect, a DSF archive was created as a backup using SINUMERIK Operate and saved on the SD Card in one of the following directories:  
`oem/sinumerik/data/archive` or `/user/sinumerik/data/archive`

Procedure:

- Insert the SD Card into the replacement NCU or PPU.
- Switch on the system and wait until SINUMERIK Operate is started. The restoration of the CNC software is indicated by a rotating circle in the 7-segment display.
- Read in the DSF archive with NC, PLC and drive data: The DSF archives are located on the SD Card under `/oem/sinumerik/data/archive` or `/user/sinumerik/data/archive`.

---

#### Note

##### Restore point

You create a restore point either directly after installing the CNC software or after installing several software packages.

---

## 6.2 Procedure for replacing an SD Card

### Replacing the SD Card

Requirements:

- The NCU/PPU is functional. The system data is present on the SSD memory.
- A backup (Page 25) was created before the defect occurred.
- A new replacement SD Card is available and ready to use.

Procedure:

- Insert the new spare part SD Card in the NCU/PPU and connect the SINUMERIK service system.
- Power up the control system with rotary switch not equal to 0 and SINUMERIK service system: after switching on, run-up with the installed CNC software (SSD). Already loaded NC and PLC data are initialized.
- In the main menu, select the menu command "Restore NCU Software and Data".
- Select the menu command "Restore backup from USB stick".



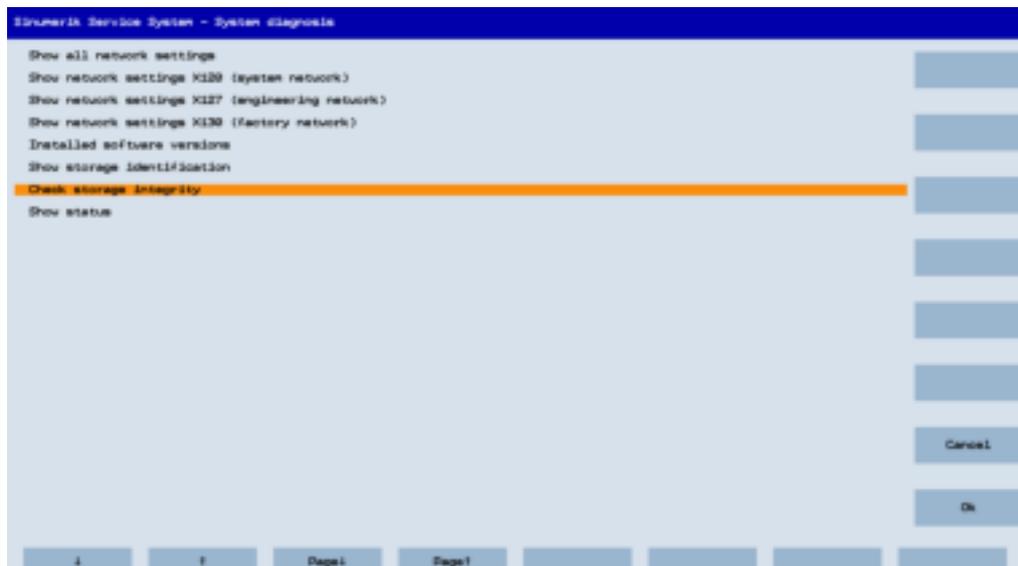
- In the main menu, select the menu command "Diagnosis" and then the menu command "Check storage integrity" to adapt the Linux partition to the brand-new SD Card (see following chapter).
- Switch off the control and disconnect the SINUMERIK service system.
- Set the rotary switch to position 0 for normal run-up and switch on the control.

## 6.3 How to check the SD Card

### Procedure

To expand the memory of the Linux partition on a brand-new SD Card:

1. Run-up of the control system with SINUMERIK service system.
2. In the main menu, select the menu command "Diagnosis".
3. Select the menu command "Check storage integrity" to start a fault check and to activate the journal:



With a brand-new SD Card, the Linux partition is adapted during this process. After checking with "Check storage integrity", this partition will be expanded to about 8 GB.



## 6.4 How to restore the SSD memory

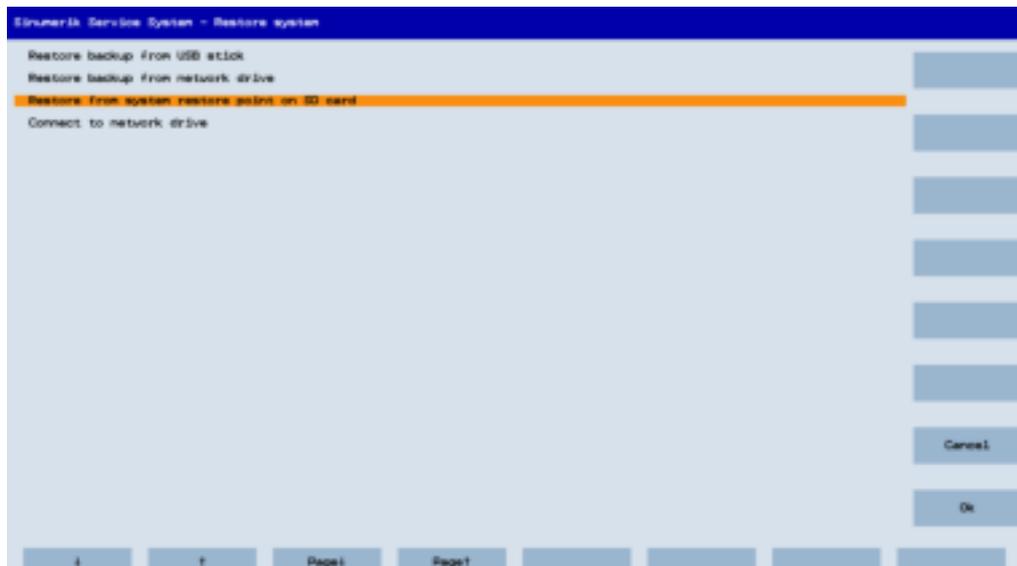
### Precondition

The SD Card contains a backup snapshot-siemens\_<xxx>.tgz with restore point (Page 26).

### Procedure

To restore the SSD memory data:

1. Run-up of the control system with SINUMERIK service system.
2. In the main menu, select the menu command "Restore NCU Software and Data".
3. Select the menu command "Restore from system restore point on SD card".



4. Select the backup snapshot-siemens\_<xxx>.tgz and confirm with OK.

## Service tasks

### 7.1 Service shell

#### Service shell

---

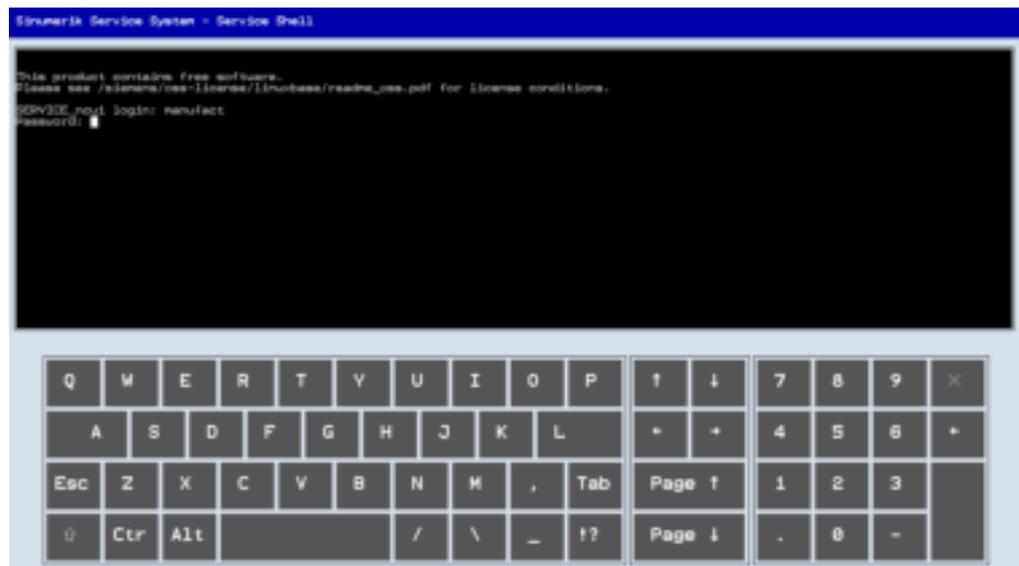
##### Note

##### Calling a service command

The service commands are only available in the "Service Shell" on the SINUMERIK service system.

---

The service command "sc" is a tool used for performing service tasks in the Service Shell. An onboard keyboard is available for making entries:



To get a list of all of the actions with a brief description, enter "sc help". After an action, further parameters or options can follow.

The access level (privilege) that the execution requires is noted for each individual action.

#### Default users

The following users are already set up:

User	Access level	Target group
user	Password: CUSTOMER	Operator
service	Password: EVENING	Service personnel
manufact	Password: SUNRISE	Machine manufacturer

**NOTICE****Change password**

To increase system security, you should change the passwords in the Linux system for users "manufact", "service" and "user" analogous to the passwords for the NC access levels: Security information (Page 11)

**Example:**

An action marked with the "user" authorization can also always be executed by members of the groups "service" and "manufact". Actions with the authorization "none" can be called by any users. If a user does not have the required privileges, the following error message is output:

```
Action "ACTION" needs at least GROUP privilege level.
```

**Syntax**

"sc" in the command line is essentially not case-sensitive. The following entries are therefore interpreted as identical:

**sc help show**

**SC help SHOW**

**sc HeLp sHoW**

**Examples:**

- Names completely in upper case represent objects to be used depending on the situation.  
Example: `sc help ACTION`  
In this case, ACTION is to be replaced by the action for which you want a description. If written in lower case, however, the entry should be entered as specified.
- Square brackets indicate optional entries.  
Example: `sc help [ACTION]`  
In this case the specification of an action is optional, which means that you can enter an action, but do not have to. Square brackets may also be nested:  
... `[USERNAME[/DOMAIN]] ...`  
In this case, USERNAME and DOMAIN are both optional, but you can only enter a DOMAIN if you have also entered the USERNAME.
- Alternatives are separated with "|".  
Example: `sc start all|system|SUBSYSTEM`  
This means that any of the following commands applies:  
`sc start all`  
`sc start system`  
`sc start SUBSYSTEM`  
In the latter case, SUBSYSTEM in upper case can be replaced by an actual subsystem name.

- As a shortened form, alternatives can also be written in square brackets:  
`sc save [-full|-user] ...`  
 Here you can use the option "-full" or "-user", or none at all.
- Options that begin with "-" can always be entered in any order.  
 For example, the notation could be interpreted to mean that "-force" must come after "-full" or "-user", but this is not necessarily the case:  
`sc save [-full|-user] [-force] FILENAME`

## 7.1.1 Help

### Description

Syntax: `sc help [Action]`  
 Alternative names: `-h, --help`  
 Authorization level: `None`

Calling "sc help" without any additional action outputs a list of all possible actions with a brief description. If you enter an additional action, you receive a more detailed description for this action.

#### Examples:

```
sc help
All actions:
help [ACTION]
Print help about a specific or list all actions
restart
Reboot the machine
enable hmi|nck|SUBSYSTEM...
enable DHCPSvr -INTERFACE
Enable HMI, NCK, or any other subsystem
[...]
sc help enable
enable hmi|nck|SUBSYSTEM...
DHCPSvr -INTERFACE
```

## 7.1.2 Clear sdcard

### Description

The partitions of an SD card are restored with the sdcard.img image using command "sc clear sdcard".

---

#### Note

##### SD card image

Use the SD card image and a data backup to restore the SD card after partition damage. The SD card image is available on PridaNet.

---

### sc clear sdcard

Syntax: `sc clear scard /data/sdcard.img`

Alternative names: ---

Authorization level: `service`

#### Procedure:

1. Copy the SD card image to the root directory of the SINUMERIK service system.
2. Run-up of the control system with SINUMERIK service system.
3. In the main menu, select menu item "Service Shell" and log on.
4. Enter the following command: `sc clear sdcard /data/sdcard.img`
5. Close the service shell using "exit".
6. In the main menu, select the menu command "Restore NCU Software and Data".
7. Select menu command "Restore backup ..." to restore the data on the SD card.

## 7.1.3 Disable

### Description

Syntax: `sc disable hmi|nck|SUBSYSTEM ...`  
`sc disable DHCPsvr -INTERFACE`  
`sc disable DHCPsync [-X120]`  
`sc disable IPAlias [-X120]`  
`sc disable usb [-MINUTES] all | HOSTS`

Alternative names: ---

Authorization level: `service`

The "sc disable" command switches the specified subsystems off. These subsystems are then not loaded again at the next cold restart. You can also switch several subsystems off with a single "disable" command. "hmi", "nck" or any other subsystem names can be used for the subsystems.

"sc disable IPAlias" deactivates the second alias IP address on the X120 network interface. This is only supported for X120. The IP address itself has the usual notation with four numbers separated by decimal points. If not specified, the subnet mask is determined from the class (A/B/C) of the IP address or specified explicitly. The CIDR notation (number of bits of the network section) is also possible.

---

#### Note

The "sc disable" command acts on the parameters in the basesys.ini file located in the user/system/etc/basesys.ini directory.

---

Parameters in the file "basesys.ini": "InternalIP\_Alias", "InternalNetMask\_Alias".

## 7.1.4 Enable

### Description

Syntax: `sc enable hmi|nck|SUBSYSTEM ...`  
`sc enable DHCPsvr -INTERFACE`  
`sc enable DHCPsync [-X120] [-PRIORITY]`  
`sc enable IPAlias [-X120] IPADDR[/NETMASK]`  
`sc enable usb [-MINUTES] all | HOSTS`

Alternative names: ---

Authorization level: service

The "sc enable" command switches on the specified subsystems such that these are also activated when a subsystem is started. Multiple subsystems can also be activated with a single "enable" command. "hmi", "nck" or any other subsystem names can be used for the subsystems.

"sc enable IPAlias" defines a second alias IP address for a network interface. This is only supported for X120. The IP address itself has the usual notation with four numbers separated by decimal points. If not specified, the subnet mask can be determined from the class (A/B/C) of the IP or determined explicitly. The CIDR notation (number of bits of the network section) is also possible.

With "sc enable usb" USB storage devices on permanently disabled USB interfaces or on certain host names or IP addresses are enabled again.

---

#### Note

The "sc enable" command acts on the parameters in the basesys.ini file located in the user/system/etc/basesys.ini directory.

---

Parameters in the file "basesys.ini": "InternalIP\_Alias", "InternalNetMask\_Alias", "SyncModeDHCPD\_SysNet".

## 7.1.5 Distribute

### Description

Syntax: `sc distribute [parameter]`

Alternative names: `dist`

Authorization level: `service`

This command distributes TCU data to other machines in the system network. Only the "tcudata" parameter is relevant here.

#### **distribute tcudata**

Syntax: `sc distribute tcudata`

Alternative names: `---`

Authorization level: `service`

This command informs the active DHCP server that TCU data in `/user/common/tcu` has been manually changed. The server can then distribute this data to the standby servers.

It is recommended that the version file in `/user/common/tcu` be changed manually as this is only read-in once by the DHCP server at the start. An incrementing of the version would then only take effect at a cold restart.

---

#### **Note**

This command can be performed on any machine in the system network, not only on the active server. A message is always sent to the active server.

---

## 7.1.6 Vncpwd

### Description

The following actions are executed using command "sc vncpwd":

- `sc vncpwd set` to assign a password.
- `sc vncpwd reset` to delete a password.

Syntax: `sc vncpwd set companynetwork|systemnetwork`

`sc vncpwd reset companynetwork|systemnetwork`

Alternative names: `---`

Authorization level: `None`

Using command "sc vncpwd set", on the server (NCU) a password is set up for the VNC connection via the company network or the factory network. As soon as a password has been assigned, a connection can only be established from a VNC client (TCU, Ultr@VNC, etc.) by specifying the correct password.

Command `sc vncpwd set` always asks for a password to be entered.

Example: `sc vncpwd set systemnetwork secreT7+`

Command `sc vncpwd reset` deletes the password for the specified network. A connection in the network is therefore possible without authentication.

---

**Note****Password in the network**

In the network (factory network or company network), in order to access any server (NCU) in the network from a TCU (client) via a VNC connection, all servers should use the same password.

---

## 7.2 Configuration file "basesys.ini"

### Storage path

For a Linux system, a file template is available under the following path:

`siemens/system/etc/template-basesys.ini`

Copy this template with the name `basesys.ini` into one of the following directories:

`oem/system/etc/basesys.ini`

`user/system/etc/basesys.ini`

### Use

Settings are made in the `basesys.ini` file that specify the behavior of the system in the network. The file contains the descriptions for all of the settings.

To edit the `basesys.ini` file:

- Comments are introduced by ';' or '#' at the beginning of the line, and span the width of the line. Empty lines are also handled as comments.
- The sections that start with a "[NAME]" line are ignored by the basic system itself, but are sometimes used by the HMI.
- Variable definitions are written in the form "NAME=VALUE". Blanks are permitted around the '=' character. The value may also be enclosed in double quotation marks, but this is optional.

---

#### Note

##### **SINUMERIK Operate**

To make settings in the file `basesys.ini`, dialogs are available in the SINUMERIK Operate in the "Commissioning" operating area for adapting the individual parameters.

---

### Example: Defining the IP address range during run-up

The controller does not have the preset IP address (X120 interface), but uses a different IP address range.

## Procedure:

1. On the FAT partition of the SINUMERIK service system, store the file basesys.ini in the following directory: /data/system/etc/
2. In the basesys.ini file the default IP addresses are adjusted in the following section:

```
[ExternalInterface]
ExternalIP=210.210.210.210
ExternalNetMask=255.255.255.0
InternalIP=192.168.214.1
InternalNetMask=255.255.255.0
Gateway=210.210.210.1
Nameservers=210.210.210.1 210.210.210.2
Hostname=somename
Domain=example.com
InternalIP_Alias=192.168.216.1
InternalNetMask_Alias=255.255.255.0
DHCPClientID=@MAC
InternalDynRangeStart=192.168.214.10
InternalDynRangeEnd=192.168.214.239
```

Result: After restarting with the SINUMERIK service system, only the entries from the [ExternalInterface] section are transferred. The changes in the IP address range are effective once for this boot process.

## 7.3 Open source software

### Service programs

The following service programs support you during commissioning and service tasks:

- **WinSCP** is a graphical, open-source SFTP and FTP client for Windows, which also supports the old SCP protocol. It offers protected data and file transfer between different computers, effectively providing the user with a protected "tunnel".  
Download: WinSCP (<https://winscp.net>)
- **PuTTY** is free software for establishing connections via Secure Shell, Telnet, remote login or serial interfaces. PuTTY serves as a client and establishes the connection to a server. During connection setup, the identity of the user is checked using one of the authentication methods provided.  
Download: PuTTY (<https://www.putty.org>)
- **Win32 Disk Imager** for Windows systems writes images to a mobile storage medium (USB flash drive or SD Card). The compact open-source software allows Linux images to be written to a storage medium so that they can be booted from there. Admin rights on the computer are necessary for installing software.  
Download: Win 32 Disk Imager (<https://sourceforge.net/projects/win32diskimager/>)

# Abbreviations

## A.1 Abbreviations

CFS	Compressed File System
CIFS	Common Internet File System
DCK	Direct Control Keys: direct keys
DCP	Discovery and Basic Configuration Protocol
DHCP	Dynamic Host Configuration Protocol: dynamic assignment of an IP address and other configuration parameters to a computer in a network
DNS	Domain Name System: conversion of domain names to IP addresses
EUNA	End User Notification Administration
IRT	Isochronous Real Time (Ethernet)
LLDP	Link Layer Discovery Protocol: manufacturer-independent Layer 2 protocol, defined according to the IEEE-802.1AB standard and offering the possibility to exchange information between devices
MAC	Media Access Control: In Ethernet networks, the MAC address is comprised of 48 bits in hexadecimal format.
MCP	Machine Control Panel:
MPI	Multi Point Interface: multiple-point interface
MUI	Multilingual User Interface
NAT	Network Address Translation
NCU	Numerical Control Unit: SINUMERIK control
NFS	Network File System is a network protocol. Synonym: Network File Service
NRT	Non-Realtime (Ethernet)
NTFS	New Technology File System
NTLMSSP	NT LAN Manager (NTLM) Security Support Provider
NTP	Network Time Protocol: standard for synchronizing clocks in the entire network
NTPD	NTP Daemon: Utility program that works in the background and does not have to be started by the user.
PridaNet	Product Information and Data Net
PG	Programming device
PLC	Programmable Logic Control: programmable logic controller
RAM	Random Access Memory: program memory that can be read and written to
RDY	Ready: The system is ready for operation.
RPC	Remote Procedure Call Synonym: Remote Function Call (RFC)
SMB	Server Message Block
SNMP	Simple Network Management Protocol (network protocol for monitoring and controlling network elements such as routers, servers, switches, printers, etc. from a central station).
SSD	Solid-state drive
SSH	Secure Shell: protocol for an encrypted network connection to a remote device
TCU	Thin Client Unit

## Abbreviations

---

### A.1 Abbreviations

TFTP	Trivial File Transfer Protocol: very simple data transmission protocol
UDP	User Datagram Protocol: NTP is mostly processed via UDP.
USB	Universal Serial Bus
UPS	Uninterruptible power supply
UTC	Universal Time, Coordinated: (formerly: Greenwich Mean Time)
VNC	Virtual Network Computing

# Index

## B

basesys.ini, 44

## C

Command

- Clear sdcard, 40
- Disable, 40
- Distribute, 42
- Enable, 41
- Help, 39
- Vncpwd, 42

## D

- Data matrix code, 17
- Define IP address, 44
- Device replacement
  - NCU/PPU, 33
  - SD Card, 34
- Documentation
  - mySupport, 15
  - Send feedback, 15
  - Standard scope, 13
  - Target group, 13
  - Websites of third-party companies, 13

## E

Emergency Boot System NCU, 22

## G

General Data Protection Regulation, 18

## N

New installation, 21

## O

OpenSSL, 18

## P

Product Support, 16  
PuTTY, 46

## S

- SD card
  - data management, 19
  - Image, 40
- SD Card
  - Linux partition, 35
- Service case, 22
- Service command
  - Syntax, 38
- SINUMERIK service system
  - Back up licenses, 25
  - Backup, 25
  - Backup SSD data, 24
  - Check storage integrity, 35
  - Create, 22
  - Creating a restore point, 27
  - Deactivating Operate, 28
  - defined initial state, 31
  - Diagnostics, 29
  - Factory settings, 32
  - Installed software version, 29
  - operating, 23
  - Restore, 36
  - Restoring the system, 36
  - Service shell, 37
  - Update, 30
- SINUMERIK service system (eboot), 22
- SSD
  - data management, 19

## T

Technical support, 16  
Training, 16

## U

Upgrade, 30  
Users (default setting), 37

**W**

Win32 Disk Imager, 46

WinSCP, 46