SIEMENS

Fundamental safety instructions 1

System requirements 2

Product information/technical update 3

SINUMERIK

MindSphere
Manage MyMachines /Remote

Readme

Valid for control:
SINUMERIK 840D sl, 840DE sl
SINUMERIK 828D
Software
Manage MyMachines /Remote Version 1.2

05/2019

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 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.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

℗ 06/2019 Subject to change

Table of contents

1 Fundamental safety instructions 5

1.1 General safety instructions 5

1.2 Warranty and liability for application examples 6

1.3 Industrial security 7

2 System requirements 9

3 Product information/technical update 15

3.1 Supplementary conditions 15

Fundamental safety instructions 1

1.1 General safety instructions

⚠ WARNING

Danger to life if the safety instructions and residual risks are not observed

If the safety instructions and residual risks in the associated hardware documentation are not observed, accidents involving severe injuries or death can occur.

- Observe the safety instructions given in the hardware documentation.
- Consider the residual risks for the risk evaluation.

⚠ 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 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.

1.3 Industrial security

Note

Industrial security

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. Products and solutions from Siemens 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. using firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that can be implemented, please visit:

Industrial security (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 become available, and that only 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 at:

Industrial security (https://www.siemens.com/industrialsecurity)

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.
- Protect the drive against unauthorized changes by activating the "Know-how protection" converter function.

System requirements

2

Prerequisite

"Manage MyMachines" is a prerequisite for using "Manage MyMachines /Remote".

References

Notes on how to connect remote control systems are provided in the following manual:

"Manage MyMachines /Remote - installation in existing control environments" and "SIMATIC IoT2040".

Hardware and operating software

The connection is established via the "Manage MyMachines /Remote Service Client".

SINUMERIK 840D sl

SINUMERIK Integrate client software version	Operating software SINUMERIK Operate version	Hardware version	Operating system
2.0.13	4.5 SP4, HF1, 2, 3, 4	NCU 730.3 PN	Linux
	4.5 SP5, HF1, 3, 5 4.5 SP6, HF3, 5, 7, 8, 10, 11, 13	PCU 50.5	Windows 7
	4.5 SP6, HF1, 12	NCU 730.3 PN	Linux
	4.5 SP6 HF2	PCU 50.5	Windows 7
3.0.13	4.7 SP2 HF1, 3, 4	NCU 730.3 PN	Linux
	4.7 SP3, HF1, 2, 3, 4 4.7 SP4, HF1, 4, 6 4.7 SP5, HF1 4.7 SP6, HF1, 3, 4, 5 4.8 SP1, HF1, 2, 3 4.8 SP2, HF1, 3 4.8 SP3, HF1	PCU 50.5	Windows 7
	4.7 SP4, HF3, 5	NCU 730.3 PN	Linux

SINUMERIK 828D

SINUMERIK Integrate client software version	Operating software SINUMERIK Operate version	Hardware version	Operating system
2.0.13	4.5 SP4 4.5 SP5, HF1, 2 4.5 SP6, HF1, 2, 3, 4	PPU 281.3 PPU 261.3	Linux
3.0.13	4.7 SP2, HF1 4.7 SP3, HF2 4.7 SP4, HF1, 2 4.7 SP5 4.7 SP6, HF1	PPU 241.3	
3.0.13	4.8 SP4, HF1	PPU 271.4	

Note

"Remote STEP 7"

"Remote STEP 7" is available on SINUMERIK Operate under Linux.

"Remote STEP 7" is **not** supported by SINUMERIK 828D.

SIMATIC Manager

The following versions of SIMATIC Manager are supported: 5.4 and 5.5

SINUMERIK control system

Screen resolution	1600 x 1200 1680 x 1050 1920 x 1200

Operator PC

Processor	1 GHz processor
RAM (GB)	4
Free hard disk capacity (GB)	1

Operating systems	Windows 7 SP1 (x64) Professional/Enterprise/Ultimate Windows 10 (x64) Pro/Enterprise
Screen resolution	800 x 600 1280 x 1024 1366 x 768 1440 x 900 1600 x 1200 1680 x 1050 1920 x 1200 1920 x 1080

Industrial PC

Processor	1 GHz processor
RAM (GB)	4
Free hard disk capacity (GB)	1
Operating systems	Windows 7 SP1 (x64) Professional/Enterprise/Ultimate Windows 7 Standard Embedded Windows 10 (x64) Pro/Enterprise
Screen resolution	At least 1980 x 1080

Note

SINUMERIK Integrate applications

Parallel operation with SINUMERIK Integrate applications is not possible.

Web browser

You can use the following web browsers:

- Chrome
  Version from 65.0.3325.18 (64 bit) up to the current version
- Firefox
  Version 59.0.2 (64 bit) up to the current version

Security notes

NOTICE

Security standards for SINUMERIK controls connected to MindSphere

The connection of SINUMERIK controls to MindSphere via TLS 1.2 /https meets the highest security standards.

SINUMERIK versions that do not meet these standards are not part of the product. For these versions, additional security measures must be taken.

You are solely responsible for preventing unauthorized access to your plants, systems, machines and network. Systems, machines and components should only be connected to the company's network or the Internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

NOTICE

Data misuse due to an unprotected Internet connection

An unrestricted Internet connection can lead to data misuse, e.g. when transferring the asset data.

Before establishing a network connection, ensure your PC is exclusively connected to the Internet via a secure connection. Pay attention to the security-relevant notes.

Further information about communications security can be found in the Configuration Manual: Industrial Security (https://support.industry.siemens.com/cs/ww/en/view/108862708).

Note

Backing up the operator PC (service engineering side)

The necessary security measures (e.g. virus scanner, firewalls, OS patching, etc.) must be implemented on the PCs that are used for visualization and configuration of "Manage MyMachines /Remote" with the machine operator or end customer.

Further information about PCs in the industrial environment can be found in the Configuration Manual: Industrial Security (https://support.industry.siemens.com/cs/ww/en/view/108862708).

Note

Backing up the SINUMERIK control (machine operator side)

The necessary security measures (e.g. virus scanner, firewalls, operating system patching, etc.) must be implemented on the SINUMERIK controls.

Further information about communications security can be found in the Configuration Manual: Industrial Security (https://support.industry.siemens.com/cs/ww/en/view/108862708).

NOTICE

Misuse of data

It is essential to use secure data storage when saving your data - particularly your confidential data. Store this data, encrypted locally or encrypted on the network. Make sure that this data cannot be accessed by unauthorized personnel.

This applies to the following data:

- Archive files
- Image files
- Project files
- Trace files
- Safety-relevant data

Further information about secure data storage can be found in the Configuration Manual: Industrial Security (https://support.industry.siemens.com/cs/ww/en/view/108862708).

NOTICE

Data manipulation possible

There is a risk that an attacker could gain access to the operating PC within the network. There, the hacker can read or manipulate various system components (e.g. the content of databases). In this way, the attacker can change tool data, NC programs, machine archives, or the system structure itself, for example. "Manage MyMachines /Remote" cannot prevent this type of attack.

- As the person responsible for the machine network, it is therefore imperative that you take the appropriate industrial security measures for the production/machine network.

Siemens AG accepts no liability for this!

Note

Saving the data that has been captured

The "Manage MyMachines Remote" product was developed by Siemens, also taking into account the "Privacy By Design" principle. This means that the service provider (OEM) makes the decision as to how long the captured data, such as information about the time period and participation in remote sessions, is saved.

NOTICE

Allowing remote access to the SINUMERIK controller

Only allow a remote access session if you know the following:

- Have you been notified of a remote access session?
- Do you know and trust the person who is conducting the session?

Delivery form

The "Manage MyMachines /Remote Service Client" is available via the "Manage MyMachines / Remote" application.

The updates and further information on the applications and products are stored on PridaNet and can be downloaded directly from there.

- OR -

You can contact your machine manufacturer.

- OR -

You can contact the Siemens Service & Support.

Product information/technical update 3

3.1 Supplementary conditions

In some cases, a service engineer cannot delete a file

Error description:

It is sometimes possible that a file cannot be deleted. In this case, an error message is not displayed – the operation status is "Unknown".

Remedy:

Close the session and start a new session to delete files.

Participation of a second service engineer in a session

Error description:

A second service engineer cannot join a session conducted by a service engineer.

Remedy:

Wait until the machine operator has joined the session.

"Access denied" message when transferring files

Error description:

If you would like to transfer an already deleted file from the remote system into the local file system or vice versa, then the "Access denied" message is output.

Remedy:

Ensure that the file is available in the local file system.

Canceling the delete operation

Error description:

The machine operator cannot cancel the deletion of files once the deletion process has been initiated.

Remedy:

The service engineer can delete the machine operator's files and any other files if the machine operator has granted the service engineer permissions for all activities in the session.

Data transfer of more than 300 files

Error description:

Data transfer of more than 300 files can lead to application problems.

Remedy:

Note that the maximum amount of data is 300 files.

Join the meeting as an observing engineer

Error description:

As an observing engineer, you cannot join a session when screen sharing is active.
- OR -

You cannot join a session while a data transfer is running.

Remedy:

Wait until screen sharing is stopped.
- OR -

Wait until the data transfer is complete.

Session information incomplete when transferring multiple files

Error description:

When multiple files are transferred in parallel, session information may contain incomplete information, for example, the duration and end time may be missing.

Remedy:

Transfer data one after the other.

Logs are sporadically incomplete

Error description:

It is possible that logs contain incomplete data.

Sender and receiver are not correctly displayed

Error description:

It is possible that senders and receivers are not correctly displayed in the logs.

Missing memory space

Error description:

If the storage space on the target system is limited, the files will not be transferred correctly.

Remedy:

Check whether there is sufficient storage space.

Termination of the session when the leading service engineer leaves the session

Error description:

When the leading service engineer leaves the session, the session is closed.

Remedy:

Transfer the role of the leading service engineer for the session to another service engineer before you leave the session.

Delete files on D:\

Error description:

The service engineer cannot delete files in the D:\ directory. The system refuses access.

Cancel data transfer

Error description:

The machine operator cannot cancel the data transfer of multiple files with small file size if he selected the option "Do this automatically for all files like this from now on".

Remedy:

Check whether the "Do this automatically for all files like this from now on" option is deselected.

Renaming a file

Error description:

If the service engineer cancels the "Rename files" action, then the machine operator receives a query as to whether he really wishes to cancel the data transfer.

Remedy:

Use the dialog to confirm or cancel the request.

Interrupted connection during a session

Error description:

If the connection to the client is interrupted for longer than 1 minute, then when the connection is restored, a dialog informs you that the connection cannot be established to the particular IP address.

Remedy:

Click the "OK" button to confirm the dialog.

In the prompt asking whether you want to leave the session, click the "No" button.

You remain in the session.

The system behavior can vary depending on the duration of the interrupted connection.

Connection interruption of more than 1 minute

Error description:

After a connection interruption of more than 1 minute and subsequent restoration of the connection, the ongoing session is displayed as terminated.

Remedy:

No remedy possible, because no further participants can join this session due to lacking buttons.

Uninstalling Manage MyMachines /Remote Service Client

Error description:

When uninstalling the "Manage MyMachines /Remote Service Client", you receive a message that uninstallation of the certificate has failed.

Remedy:

Click "OK".

Joining the session with the "client.mmmr" file

Error description:

It is not possible to start or join a session using a valid "client.mmmr" file.

Remedy:

In Windows, select "Manage MyMachines /Remote Service Client" as the default program for opening the "*.mmmr" file.

Mozilla Firefox

Error description:

It is not possible to select the default application "MMM /Remote Service Client" in Mozilla Firefox.

Remedy:

In Windows, select "Manage MyMachines /Remote Service Client" as the default program for opening the "*.mmmr" file.

Subtenant user starts Manage MyMachines /Remote

Error description:

It is not possible to start a "Manage MyMachines /Remote" session with a subtenant user.

Remedy:

Assign administrator rights.

The "Manage MyMachines /Remote" softkey is not displayed after updating the SINUMERIK Integrate client.

The "Manage MyMachines /Remote" softkey is not displayed after updating the SINUMERIK Integrate Client if the Base Setup has already been installed on the SINUMERIK Integrate client.

Procedure 1: The update of the SINUMERIK Integrate client has not yet been performed.

1. Uninstall Base Setup.
2. Restart the HMI.
3. Update the SINUMERIK Integrate client.
4. Install Base Setup.
5. Restart the HMI.

Procedure 2: The update of the SINUMERIK Integrate Client has already been performed.

1. Uninstall Base Setup.
2. Restart the HMI.
3. Install Base Setup.
4. Restart the HMI.

The "Manage MyMachines /Remote" softkey is displayed again.