SIEMENS

FAQ • 05/2015

What are the requirements for S7 F/FH Systems in virtual environments and for remote access?

S7 F Systems V6.0 and higher and Safety Matrix V6.1 SP1 and higher

https://support.industry.siemens.com/cs/ww/en/view/109475027

This entry originates from the Siemens Industry Online Support. The conditions of use specified there apply (http://www.siemens.com/terms_of_use).

Security Notes

Siemens offers products and solutions with industrial security functions which support the secure operation of plants, solutions, machines, devices and/or networks. They are important components in a comprehensive industrial security concept. The Siemens products and solutions continue to be developed under this aspect. Siemens recommends that you keep yourself regularly informed about product updates.

For the safe operation of Siemens products and solutions it is necessary to take appropriate security measures (cell protection concept, for example) and to integrate each component in an overall industrial security concept which is state of the art. This should also cover the third-party products used. Additional information about industrial security is available at: http://www.siemens.com/industrialsecurity.

In order to keep yourself informed about product updates, we recommend subscribing to our product-specific newsletter. Additional information about this is available at http://support.industry.siemens.com.

Contents

1 Overview

SIMATIC S7 F/FH Systems with S7 F Systems V6.0 and higher and Safety Matrix V6.1 SP1 and higher enable for ESs and OSs the use in virtual environments and the use of remote access under the conditions set out here. The warning "Operation on terminal servers/clients or on a virtual server/system is explicitly prohibited." in the product manuals expires because of the additional requirements to be met in this documentation.

All restrictions and notes in the corresponding releases of S7 F Systems and Safety Matrix, as well as of STEP 7 and PCS 7 continue to be valid for virtual environments and remote access.

Virtual environments

In information technology a virtual machine is designated as the emulation of a real computer system (hardware) on an abstraction layer which can execute multiple virtual machines at the same time. The abstraction layer is known as a hypervisor. Known manufacturers are Microsoft (Microsoft Hyper-V), VMware (VMware vSphere Hypervisor (ESXi)) and Citrix (XenServer).

A virtual environment enables, for example, very convenient test environments, simplifies the transfer of systems and saves space.

Remote access and control

In information technology "remote access" designates the transfer of a graphical user interface and can be employed for different types of access. In this entry "remote access" refers to the unique access to the graphical user interface and the transfer of keyboard actions and mouse movements of an Engineering Station or Operator Station. Known software products include Microsoft Remote Desktop Protocol (RDP) and the RealVNC Open Source Software VNC (RFC 6143).

Software requirements

SIMATIC STEP 7 and PCS 7 are released for virtual environments and remote access and can be integrated in your plant under the environment descriptions linked here.

Table 1-1

Products	Product news	Options packages
PCS 7 V8.0 SP2: • VMware vSphere V5.0 • VMware vSphere V5.1	https://support.industry.siemens.com/cs/ww/en/view/102378876	S7 F Systems V6.1 SP2 SIMATIC Safety Matrix V6.2 SP1
PCS 7 V8.1: • VMware vSphere V5.5	https://support.industry.siemens.com/cs/ww/en/view/93997453	S7 F Systems V6.1 SP2 SIMATIC Safety Matrix V6.2 SP1
Service Pack 4 for STEP 7 V5.5 and STEP 7 Professional Edition 2010*: • VMware vSphere Hypervisor ESX(i) 5.5 • VMware Workstation 10.0 • VMware Player 5.02 • Microsoft Windows Server 2012 Hyper-V	https://support.industry.siemens.com/cs/ww/en/view/9384200	S7 F Systems V6.1 SP2 SIMATIC Safety Matrix V6.2 SP1

* Only configuring, programming and operating in the STEP 7 Engineering

Note Siemens provides preconfigured virtualization solutions with its "SIMATIC Virtualization as a Service".

More information is available in the following entry:
https://support.industry.siemens.com/sc/ww/en/sc/3095

2 Configuration and Operation

2.1 Virtual Environments

WARNING

Use of virtual environments in ES/OS

Note that a HYPERVISOR or the client software of a HYPERVISOR is not permitted to perform functions that reproduce recorded message frame sequences with correct time behavior on a network with connected plants.
Ensure that this is the case when using the following functions:

- Reset of captured states (snapshots) of the virtual machines (VMs)
- Suspending and Resuming of the VMs (Suspend & Resume)
- Replay of recorded sequences in the VMs (Replay)
- Moving of VMs between hosts in productive operation (e.g. Fault Tolerance (FT))
- Digital twins of VMs in the virtual environment

If in doubt, disable these functions in the settings (HYPERVISOR administrator console).

Note How do you use VMware vSphere Client to assign operator permissions for a virtual machine?
https://support.industry.siemens.com/cs/ww/en/view/90142228

Note How do you use a controller to load from a VM (VMware Player/Workstation) via a PROFIBUS/MPI CP connected via PCI or PCIe?
https://support.industry.siemens.com/cs/ww/en/view/100450795

Note Configure Hyper-V for Role-based Access Control
https://technet.microsoft.com/en-us/library/dd283076(v=ws.10).aspx

2.2 Remote Access and Control

WARNING

Remote access from higher-level control room and Engineering Center

Make sure that the plants are clearly distinguished from other accessible plants connected on the network before you start making changes or start operation.
Examples:

- Specify optical distinguishing marks (plant designation) for the operator station.
- The pair of numbers for SAFE_ID1 and SAFE_ID2 with SDW must be unique for all the plants accessible in the network.
- Specify distinct descriptions for title and project in the properties of the Safety Matrix for all the plants connected on the network and check this before starting operations.
- Specify Active Directory access limitations in the corporate directory service and use SIMATIC Logon for accessing projects and for logging on to operator stations.

WARNING

The "S7 F Systems HMI" and "Safety Matrix Viewer" functionality makes changes in the safety program during RUN mode.

As a result, the following safety measures are required:

- Make sure that operations that could compromise plant safety cannot be carried out. You can use the EN_SWC and EN_CHG input for this purpose, for example, by controlling it with a key-operated switch or on a process-specific basis via the safety program.
- Make sure that only authorized persons can carry out operations.
  Examples:
  - Control the EN_SWC or EN_CHG input with a key-operated switch.
  - Control the EN_SWC or EN_CHG input with separate key-operated switches.
  - Set up access protection at operator stations where process operation can be performed.

Carefully choose the persons who may have remote access to the plant and authorize them accordingly:

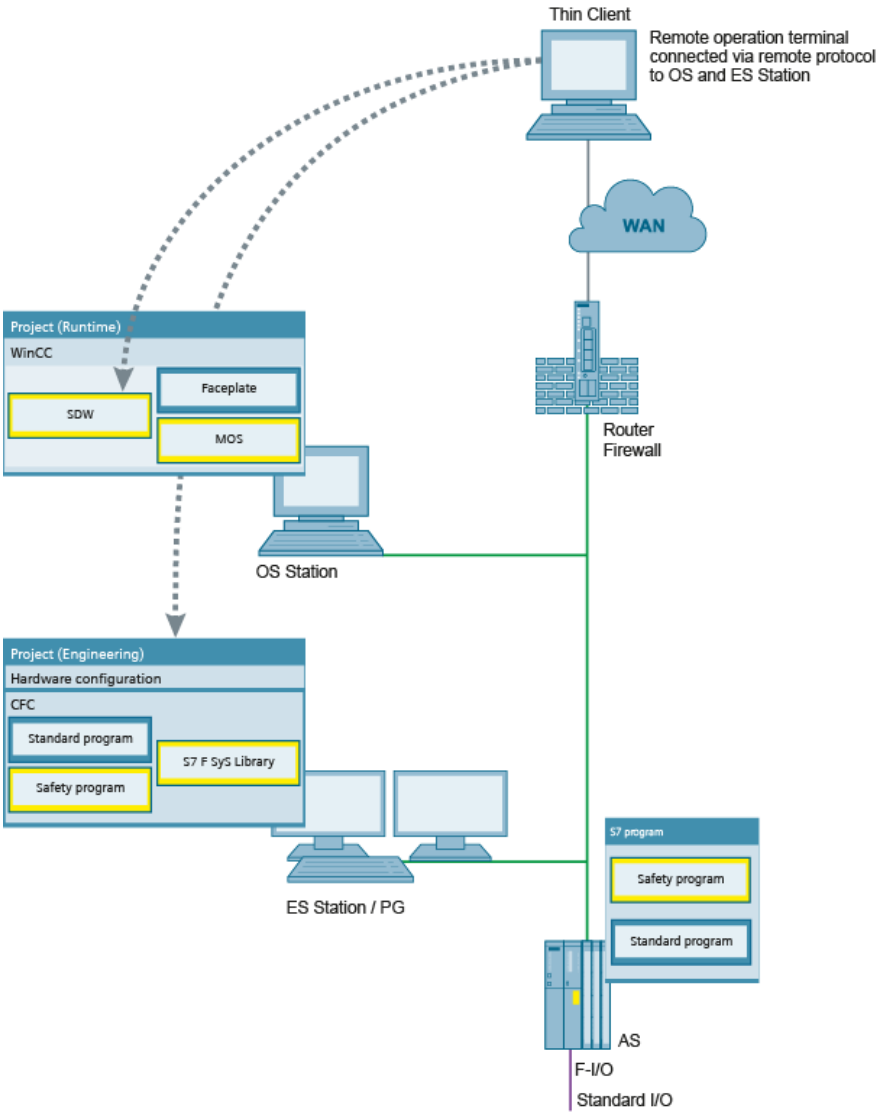
- Locally on the target computer "Remote Desktop User" (Workgroups)

  or
- In the Active Directory and inheritable permissions to the target computer "Remote Desktop User" (Domain).

As required, make a distinction in the WinCC authorizations between

- Process control
- Higher process control
- Safety application control (SIF)

Figure 2-1: Diagram of Engineering Station and Operator Station in projects with safety applications



ES Station

Table 2-1: Explanation of Figure 2-1

Physical location	Installed software
At the same location as the AS station and connected to the plant/terminal bus.	SIMATIC PCS 7 (package: PCS 7 Engineering) or STEP 7

OS Station

Table 2-2: Explanation of Figure 2-1

Physical location	Installed software
At the same location as the AS station and connected to the plant/terminal bus.	SIMATIC PCS 7 (package: OS Client or OS Single Station)

Thin Client

Table 2-3: Explanation of Figure 2-1

Physical location	Installed software
Not at the same location as the AS station and not connected to the plant bus.	No SIMATIC software installed

Note SIMATIC Process Control System PCS 7 - PC Configuration (V8.1) - section 4.8.2
https://support.industry.siemens.com/cs/ww/en/view/109476180

Note White paper; Security concept PCS 7 and WinCC - Basic document
https://support.industry.siemens.com/cs/ww/en/view/26462131

Note How do you access WinCC and PCS 7 plants with "RealVNC"?
https://support.industry.siemens.com/cs/ww/en/view/55422236

Note What should you watch out for with a remote access to a SIMATIC S7 with STEP 7 via the Internet?
https://support.industry.siemens.com/cs/ww/en/view/38571711

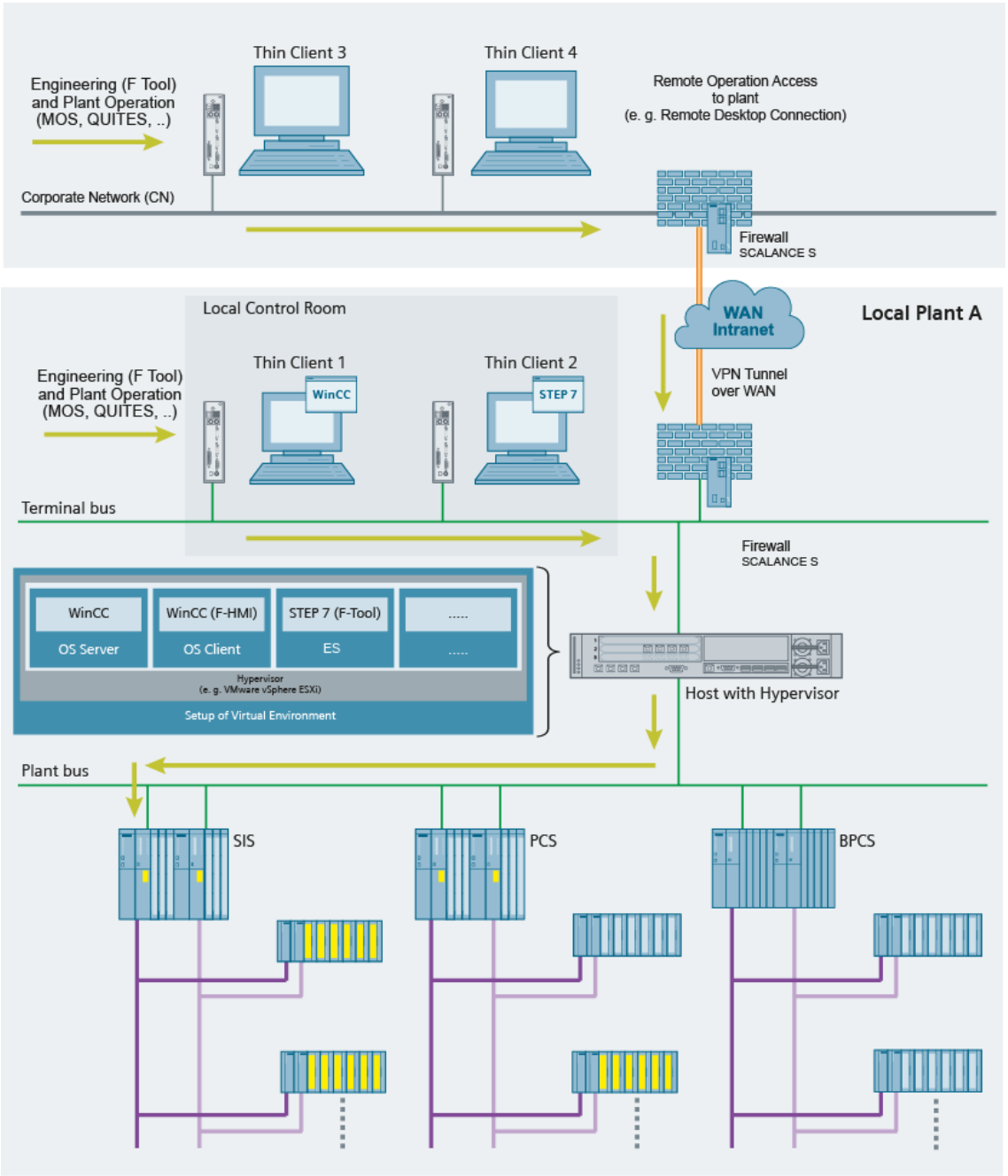
Note IP-based Remote Networks
https://support.industry.siemens.com/cs/ww/en/view/26662448

3 Examples of Valid Configurations in PCS 7

3.1 Example 1

The following figure shows a virtual environment for engineering and plant operation of safety applications including remote control.

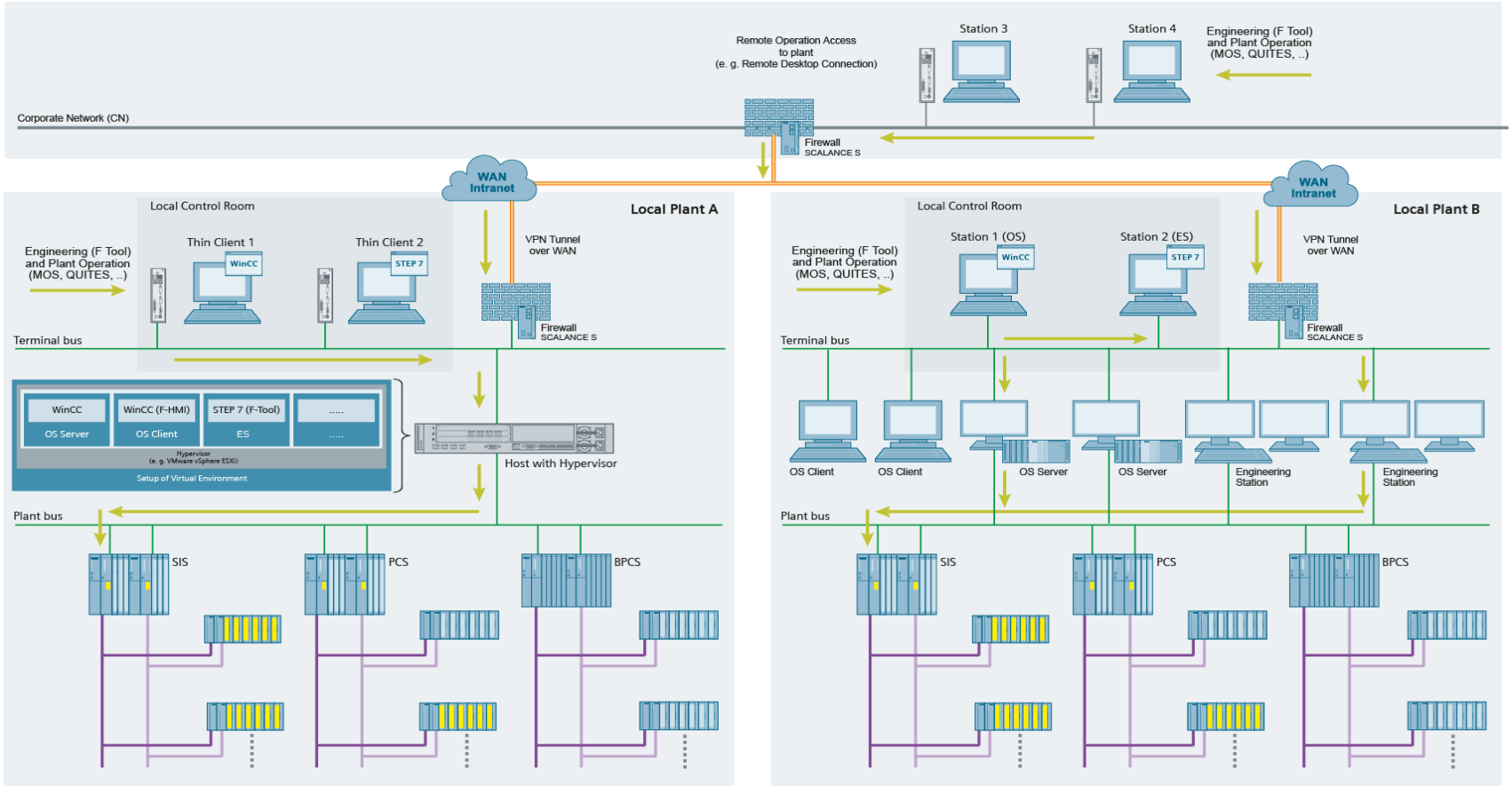
Figure 3-1



3.2 Example 2

The following figure shows a configuration for remote access for configuration and maintenance operations as well as plant operation from higher-level control room in real and virtual environments.

Figure 3-2



4 Abbreviations and Explanations

Table 4-1

Abbreviation	Explanation
AD	Active Directory
BPCS	Basic Process Control System
CN	Corporate Network (company network/intranet)
ES	Engineering Station
LCR	Local Control Room
LER	Local Engineering Room
MOS	Maintenance Override Switch
OS	Operator Station
PCS	Process Control System
QUITES	Acknowledgment via ES/OS
ROC	Remote Operation Center (higher-level control than LCR)
SDW	Safety Data Write
SIF	Safety Instrumented Function
SIS	Safety Instrumented System
VM	Virtual Machine (guest operating system)
WAN	Wide Area Network

5 Literature

Table 5-1

	Subject area	Link
\1\	SIMATIC Industry Software Safety Engineering in SIMATIC S7	https://support.industry.siemens.com/cs/ww/en/view/12490443
\2\	SIMATIC Industry Software S7 F/FH Systems – Configuring and Programming	https://support.industry.siemens.com/cs/ww/en/view/101509838
\3\	SIMATIC Industry Software Safety Matrix	https://support.industry.siemens.com/cs/ww/en/view/100675874
\4\	Technical documentation SIMATIC PCS 7	http://w3.siemens.com/mcms/industrial-automation-systems-simatic/en/manual-overview/tech-doc-pcs7/Pages/Default.aspx
\5\	SIMATIC PCS 7 OS Software Client V7.1 + SP2 and higher released for implementation in virtual operation environments	https://support.industry.siemens.com/cs/ww/en/view/51401737
\6\	SIMATIC Virtualization as a Service	https://support.industry.siemens.com/cs/ww/en/view/107586660
\7\	What are the options for upgrading the software of a virtualization system?	https://support.industry.siemens.com/cs/ww/en/view/103496884
\8\	VMware vSphere Documentation V5.5	https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html
\9\	Microsoft Hyper-V	https://technet.microsoft.com/en-us/windowsserver/dd448604.aspx
\10\	XenServer Documentation Index	http://docs.vmd.citrix.com/XenServer/6.5.0/1.0/en_gb/

6 History

Table 6-1

Version	Date	Change
V1.0	05/2015	First edition