SIEMENS

SIMATIC HMI

WinCC flexible 2005 Sm@rtAccess, Sm@rtService

Printout of the Online Help

Printout of the Online Help

Edition 05/2005

Safety Guidelines

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 to property damage only 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

with a safety alert symbol, indicates that minor personal injury can result if proper precautions are not taken.

Caution

without a safety alert symbol, indicates that property damage can result if proper precautions are not taken.

Notice

indicates that an unintended result or situation can occur if the corresponding information is not taken into account.

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 device/system may only be set up and used in conjunction with this documentation. Commissioning and operation of a device/system may only be performed by **qualified personnel**. Within the context of the safety notes in this documentation qualified persons are defined as persons who are authorized to commission, ground and label devices, systems and circuits in accordance with established safety practices and standards.

Prescribed Usage

Note the following:

Warning

This device may only be used for the applications described in the catalog or the technical description and only in connection with devices or components from other manufacturers which have been approved or recommended by Siemens. Correct, reliable operation of the product requires proper transport, storage, positioning and assembly as well as careful operation and maintenance.

Trademarks

All names identified by ® are registered trademarks of the 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
Automation and Drives
Postfach 4848, 90327 Nuremberg, Germany

Siemens AG 2005
Technical data subject to change

Table of contents

Basic principles

1

1.1 What are Sm@rtAccess and Sm@rtService?

Introduction

Sm@rtAccess and Sm@rtService are the options available in WinCC flexible for communicating between HMI systems or to an HMI system by means of TCP/IP connections (for example, LAN).

Note

You can find online information about remote maintenance with WinCC flexible via WAN, Intranet, and Internet at <http://support.automation.siemens.com>. Select one of the available languages, enter the ID "19865167" in the search field, and start your search. The article "WinCC flexible remote maintenance" will open.

Applications

Sm@rtAccess

Sm@rtAccess enables the following communication tasks between HMI systems in production and system control applications:

- Distributed operator stations for controlling large machines or machines that are spread out over a large area
- Operator stations with system-wide access to current process data
- Simple servicing for centralized archiving, analysis, and additional processing of process data
- Provision of current process data for higher-level systems (SCADA, production management systems, office applications)

User benefits:

- Flexible solution for access to HMI systems and process data from any location
- Reduction of load on the field bus: For example, the combination of WinCC flexible Runtime and SIMATIC panels enables a factory control system to have access to process data. No load is placed by the factory level on the sensitive field level with respect to the necessary communication requirements. These requirements are handled by WinCC flexible Runtime along with the SIMATIC panels.
- Simple and fast configuration of communication relationships using the WinCC flexible engineering software.

Sm@rtService

Sm@rtService supports remote maintenance of HMI systems:

- Remote access to HMI systems by means of Internet, Intranet, and LAN.
- Provision of diagnostic information and administrative services using HTML pages of the integrated web server
- E-mail delivery during runtime

User benefits: Global access to machinery and systems by service and maintenance personnel enables malfunctions to be corrected in less time and and expensive on-site service visits to be avoided. Downtime is reduced and productivity is increased.

See also

Integrated web server (Page 4-9)

Elements and Basic Settings

2

2.1 Basic settings for Sm@rtAccess and Sm@rtService

2.1.1 Settings overview

Introduction

To take advantage of the additional options provided by Sm@rtAccess and Sm@rtService, settings must be included in the following:

- Configuration in WinCC flexible ES
- Settings on the HMI devices
- Programming in external applications (according to scenario)

These settings are briefly addressed below. Further information and specific step-by-step instructions can be found in the examples for the application scenarios.

Configuration in WinCC flexible ES

The following aspects must be taken into account when configuring in WinCC flexible ES:

- Device settings

  The requirements for utilizing the Sm@rtAccess and Sm@rtService functions are established for each HMI device in the device settings under "Services in runtime."

- Access to tags via the SIMATIC HMI HTTP protocol

  If access to tags via the SIMATIC HMI HTTP protocol is to be enabled, these tags must be defined for the relevant HMI devices and connected to one another.

- Remote monitoring and remote control via Sm@rtClient display

  If the Sm@rtClient display object is to be utilized for remote monitoring and remote control during runtime, this object must be inserted in a screen and configured.

Settings on the HMI devices

Control panel settings must be made at the HMI devices according to the required configuration. To do so, open the control panel of the HMI device and enter the settings in the "WinCC flexible Internet Settings" dialog.

Programming in external applications

To access tags via web service (SOAP) from an external application, you must have, for example, a VBA macro that reads or writes the tag values.

Specific step-by-step instructions can be found in the application scenario example.

2.1.2 Configuration in WinCC flexible

Introduction

As part of the device settings of a WinCC flexible project, you specify which services should be available on the HMI device during runtime.

Open

Double-click "Device settings" in the "Device settings" area.

Figure 2-1 Device settings

Work area

In the work area, you enter the settings for the selected HMI device under "Services in runtime:"

- Sm@rtAccess or Sm@rtService: Start Sm@rtServer

  The HMI device acts as a Sm@rtServer and permits remote access.

- Sm@rtService: HTML pages

  The HMI device supports access to HTML pages and associated services such as Stop/Start of HMI runtime, remote control, data record/password exchange, access to system information (OP system alarms, call of version releases), and access to the file system of the target device.

- Sm@rtAccess: As SIMATIC HMI HTTP server

  The HMI device allows configured access to the tags during runtime.

  To enable access to the tags, you must define the appropriate tags in the project for each client and connect them to the server tags.

- Sm@rtAccess: Web service (SOAP)

  The HMI device supports data access to tags by means of SOAP. The tag values can be accessed from MS Excel, for example, using a VBA macro.

- Name of the SMTP server

  Here, you can enter the name of the SMTP server that you want to use for sending e-mails. Alternatively, you can enter the name in the system settings WinCC Internet Settings of the HMI device.

- Name of the SMTP sender

  Here, you can enter the name of the SMTP sender. This setting is useful if you want the receiver is to be able to determine the device where the e-mail originated, for example, "MP270 device on Production Line 2." Alternatively, you can enter the name in the system settings WinCC Internet Settings of the HMI device.

- SMTP authentication

  However, if the e-mail is sent via an authentication (in the case of a provider), you must enter a valid e-mail address as "SMTP authentication," for example, "John.Doe@gmx.net". Alternatively, you can enter the name in the system settings WinCC Internet Settings of the HMI device.

2.1.3 Settings on the HMI device

Introduction

Settings on the HMI device for Sm@rtAccess and Sm@rtService are entered in the "WinCC flexible Internet Settings" dialog of the control panel.

Opening the Control Panel

You can open the control panel as follows (example):

- Select the "Settings > Control Panel" menu command in the Windows Start menu.

  In the case of the Windows CE HMI device, this can only be done during startup.
- During runtime, activate the operator control element associated with the "Open Control Panel" system function.

Note

This enables you to modify settings on the HMI device during runtime.

The control panel may appear differently depending on the type of HMI device. The control panel of the MP 270 HMI device is illustrated here as an example:

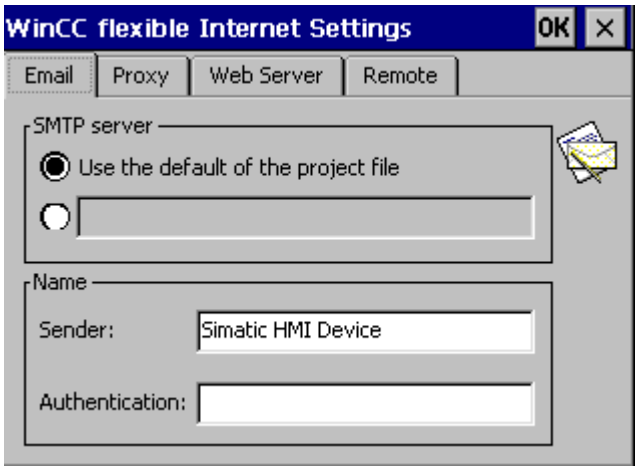


Figure 2-2 Control Panel of MP 270

Note

The number of tabs in the "WinCC flexible Internet Settings" dialog and their names are dependent on the software installed.

Tabs of WinCC flexible Internet Settings

The "WinCC flexible Internet Settings" dialog of the control panel can contain the following tabs:

- "Email" tab

  Entries and settings for utilizing the e-mail service

- "Proxy" tab

  Entries and settings for the proxy server for the HTTP protocol

  This tab exists only on Windows CE devices; on a PC, the corresponding tab is included in the control panel under "Internet Options."

- "Web Server" tab

  Settings for utilizing the web server.

  The "User Administration" button is used to access the dialog for assigning web authorizations.

- "Remote" tab

  Settings for starting and stopping the Sm@rtServer

  The "Change settings" button is used to access the dialogs containing the settings for connection, session management, and security.

2.2 User administration for web server

Introduction

User access to the services associated with Sm@rtAccess and Sm@rtService is controlled with the user administration for the web server.

The web server user administration is based on explicitly assigned web authorizations.

Entries and settings

The web authorizations are assigned on the web server.

To do so, access the "WinCC flexible Settings" in the system settings on the server, and click the "User Administration" button on the "Web Server" tab.

The "UserDatabase-Edit" dialog contains three tabs.

- "User Manager" tab

  Here, you create or delete users.

- "Description" tab

  Here, you can store a description of or comments on the users selected on the "User Manager" tab.

- "Authorizations" tab

  Here, you enter the web authorizations for the user selected on the "User Manager" tab. You use "Add" to activate a web authorization and "Remove" to deactivate one.

  By default, the password is initially preset to "100" and all web authorizations are granted to users with "Administrator" rights.

  For read and write access to the file browser, the user must possess the web authorizations "FileBrowserAdministrator" and "FileBrowserUser".

Note

In principle, every user who has access to the control panel can manage users and web authorizations. If necessary, you can protect the control panel from unwanted access.

List of web authorizations

You can assign web server users the following authorizations:

Web authorization	Authorized for:
UserData	Import and export of recipes
PasswordList	Import and export of password lists
RuntimeAccess	Starting and stopping of runtime
Engineering	HTTP transfer from ES to the target device
FileBrowserUser	Read access to the file browser
FileBrowserAdministrator	Read/write access to the file browser
RTCommunication	Utilization of the SIMATIC HMI HTTP server
SoapUser	Read/write access via web service (SOAP)

2.3 Settings for remote operation

2.3.1 Session management for remote control

Introduction

WinCC flexible enables remote monitoring and remote control of HMI devices over a TCP/IP-ready network such as a LAN or the Internet. Remote monitoring and remote control can be implemented in different ways:

- Remote control by means of Internet Explorer (with Sm@rtService)
- Remote control by means of the Sm@rtClient application (with Sm@rtService)
- Remote control by means of the Sm@rtClient display during runtime (with Sm@rtAccess)

In each of these cases, only one device can ever have control access to the HMI device. Which device is permitted access is determined by the session management.

Session management options

Session management is used to control access. The client-server connection can be in one of two modes:

- Monitoring mode
- Control mode

Monitoring mode

If the client accesses the server in monitoring mode, the operator can see the current screen of the HMI device and track all changes. As a result, he can monitor the server but does not have control access to the server.

In this mode, all of the keys on the client retain their standard functions. If, for example, remote control was started from the Sm@rtClient display, the operator uses the <Tab> key or the cursor keys to go to the next object in the current screen of the client project.

Control mode

If the client accesses the server in operator control mode, he can use the mouse and the keyboard to control the server from the client. If an access attempt is made from another client, the assignment of operating permission depends on the settings at the server and at the clients:

In operator control mode, the client keys act on the server screen. Thus, the operator uses the <Tab> key to go to the next object in the current screen of the project that is running on the server.

If, for example, remote control was started from the Sm@rtClient display, the operator can only go to another object or screen in the project on the client by using an additionally configured function or an additional menu item. The operator accesses this menu item on the touch panel by applying pressure for longer than 1 s; on the keyboard panel, the menu is displayed with <Shift+Ctrl> and controlled with the keyboard plus <Alt>.

In both operating modes, the Sm@rtServer can be set so that the operator of the remotely controlled device, the server, is prevented from performing any activities.

In an emergency, the operator can exact the user rights on a remotely controlled HMI device as well as on an inactive HMI device. If no password is specified, he must click the user interface four times consecutively, touch the screen four times consecutively, or press the <Shift> key four times consecutively. If a password is specified, he must click once or press a key on the client and then enter the specified password.

Settings for session management

Settings for session management are made on the server and on the client in the control panel in "WinCC Internet Settings."

2.3.2 Configuring Sm@rtServer for remote control

Introduction

The Sm@rtServer has an internal security concept based on passwords and special settings for session management.

Security concept for the Sm@rtServer

Remote monitoring and remote control of the Sm@rtServer by the Sm@rtClient is protected by two passwords. The second password serves as an additional password, which can be easily changed when required for additional access (for example, for use as a service password). Both passwords are preset to "100".

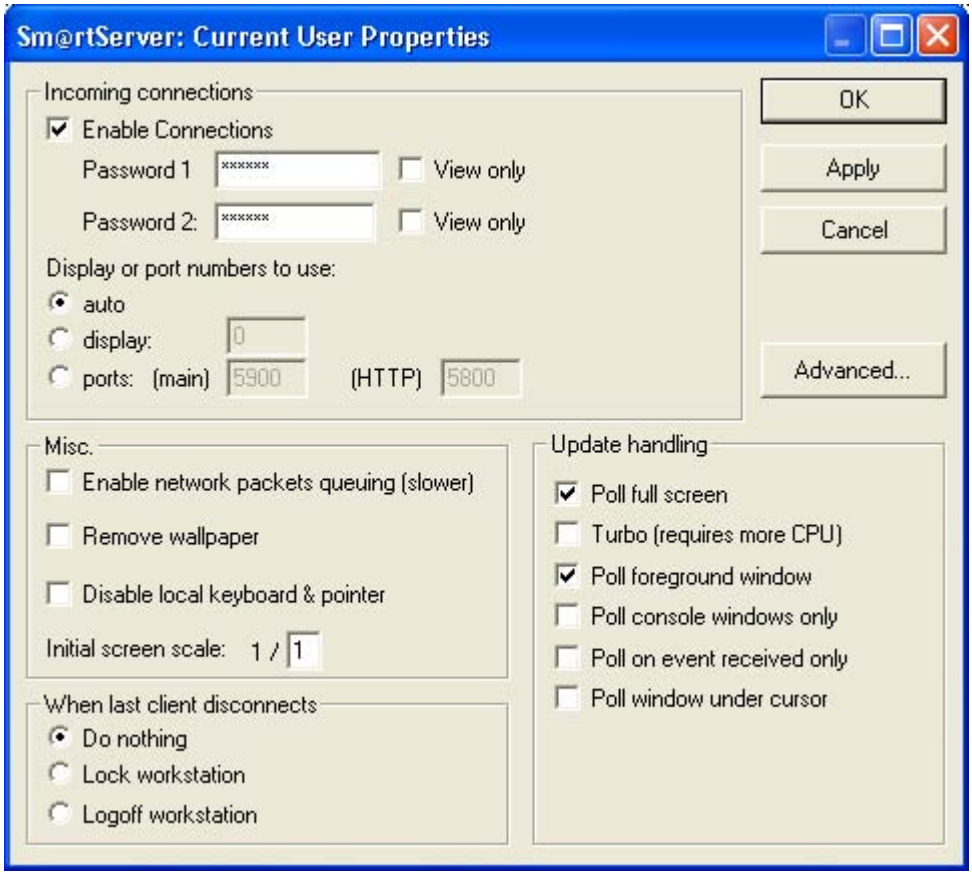
Settings on the Sm@rtServer

The settings on the server govern which remote operators can access the runtime of the server.

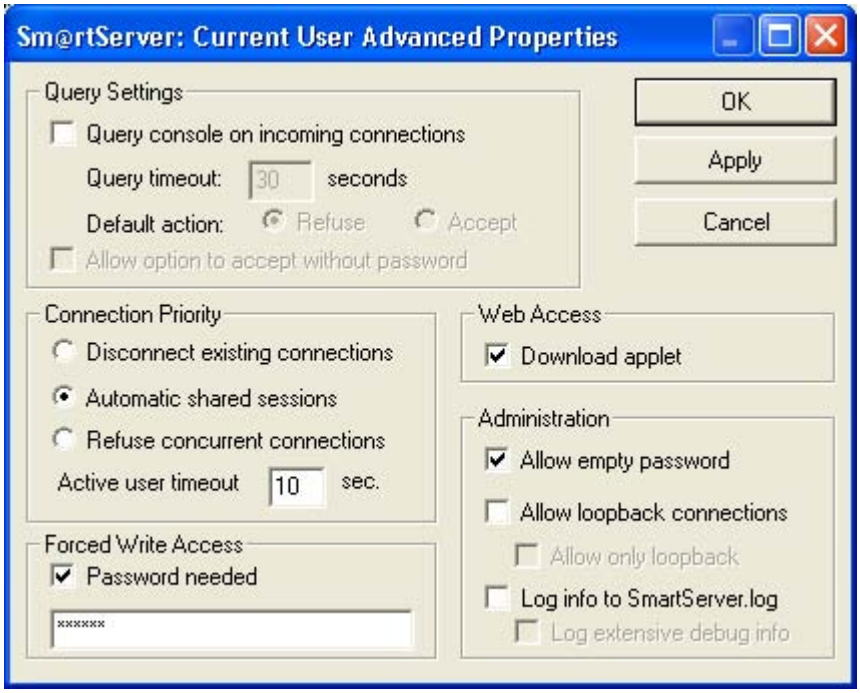
The passwords for access are set on the server. To do this, open "WinCC Internet Settings" in the control panel and click "Change Settings" on the "Remote" tab. The passwords for the Sm@rtClient can be entered in the next dialog box. For both passwords, you can use "View only" to set the monitoring mode and to exclude operator control mode.

Control mode

To enable operator control mode, the "View only" check box must be cleared.



The manner in which the individual remote control station can access the server is set in another dialog box. Click the "Advanced" button and select the following mode under "Connection Priority":



- "Disconnect existing connections"

  When an asset attempt is made by a non-shared client, the previous connection is automatically disconnected and control is transferred to the new client.

  When an access attempt is made by a shared client, the behavior is the same as that described for ""Automatic shared sessions."

- "Automatic shared sessions"

  When an access attempt is made, control is transferred to the new client.

  The condition for transferring control is that no action has been undertaken by the previously active client for a period of time (in seconds) as specified in the "Active user timeout" setting.

- "Refuse concurrent connections"

  When an attempt is made to access by a non-shared client, this access attempt is rejected so long as the operator station that currently has access is still connected to the server.

  When an attempt is made to access by a shared client, the behavior is the same as that described for "Automatic shared sessions."

Disabling local operator control of the server

You can disable local operator control on the server. To do so, click the "Change Settings" button on the "Remote" tab of the control panel "WinCC Internet Settings," and activate the ""Disable Local Keyboard & Pointer" setting in the dialog.

Password for forced access

A password can be specified in "Force Write Access" for forced access in an emergency.

Sm@rtServer as a service

You can let the Sm@rtServer run as a service. The user can then also access the service unit from the client HMI device when, for example, the screen saver is active with a password.

To do so, select the "Start automatically after booting" check box on the "Remote" tab in "WinCC Internet Settings in the control panel."

Settings on the client PC

At the client PC you can yourself limit the connection to observation mode, if desired. This can be useful in order to avoid unwanted control operations.

If you have established the connection via the Sm@rtClient application, click the "Options... " button in the "Connection details" dialog box of the Sm@rtClient application, and select the "View only (inputs ignored) " setting in the "Options" dialog box.

If you have established the connection via Internet Explorer, click the "Options" button and select "View only" in the displayed dialog box.

Configuring the Sm@rtClient display

You can configure the Sm@rtClient display in different ways, thus establishing certain inputs: The server name, the password for accessing Sm@rtServer or the restriction to observation mode.

Using Sm@rtAccess

3

3.1 Communication between HMI systems with Sm@rtAccess

Introduction

Communication between HMI systems can be achieved using the Sm@rtAccess option of WinCC flexible. The following are suitable for this purpose: 270- and 370-series Panels and MultiPanels, xP 177B, Mobile Panel 177 PN, and PCs with WinCC flexible Runtime.

Application scenarios

Communication between HMI systems is implemented in three different ways, or a combination of these.

- Sm@rtServer and Sm@rtClient

  An HMI device configured as a Sm@rtServer can be remotely monitored or remotely controlled from another PC or HMI device.

- SIMATIC HMI HTTP Protocol

  Tags of an HMI device configured as a SIMATIC HMI HTTP server can be accessed via the SIMATIC HMI HTTP protocol.

- Web service (SOAP)

  Tags of an HMI device can be accessed from an external application such as MS Excel via web service (SOAP) using a VBA macro.

Communication between HMI systems permits the following scenarios to be implemented:

Coordinated operator control stations (Sm@rtServer and Sm@rtClient)

For operator control of large machines/systems or machines/systems that are spread out over a large area, coordinated operator stations can be employed. The operator can thus control and monitor the system from various locations, although only one operator station can access the device containing the configuration. The operator sees the same screen on every operator station and on the device containing the configuration.

Because only a single master configuration is involved, changes to this configuration only have to be made once.

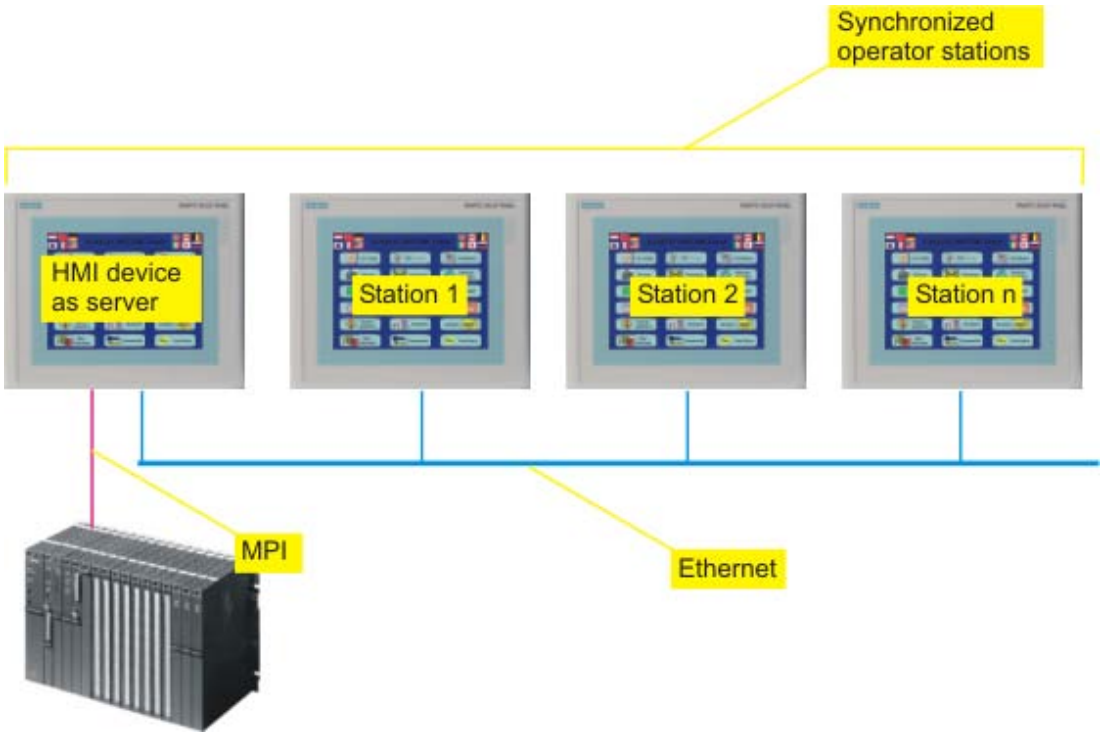


Figure 3-1 Coordinated operator stations

Communication between HMIs via SIMATIC HMI HTTP protocol

Use of the SIMATIC HMI HTTP protocol enables you to provide tags of an operation device (server) to another device (client).

HMI devices used locally or centrally can thus access tags of other stations. As a result, cell concepts or line concepts can be easily implemented. Information obtained decentrally can be made available centrally.

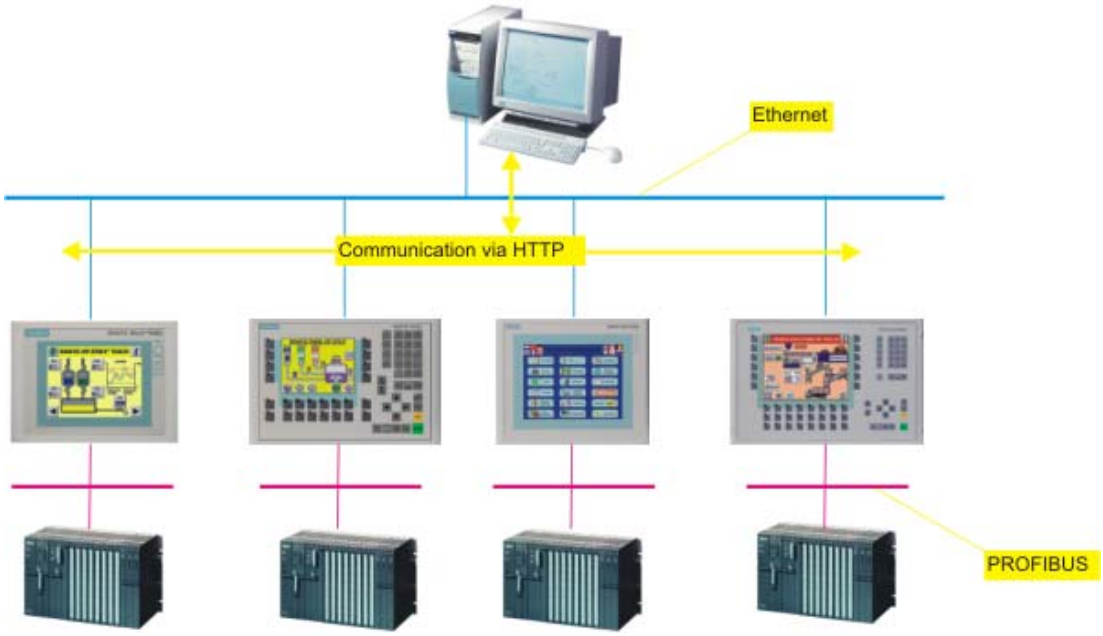


Figure 3-2 Communication between HMIs

This concept also allows for more cost-effective equipment and less central maintenance. If a PC is used for this purpose, options are also available for archiving, analysis, and further processing of acquired process data.

Remote monitoring and remote control - maintenance solution

By combining use of the SIMATIC HMI HTTP protocol and the Sm@rtServer, you can implement a complex maintenance solution.

This involves displaying the HMI device tags of interest on the maintenance PC and, when necessary, using the PC for remote operation and remote control of a certain HMI device.

Locally used HMI devices are combined in this way, and the overall process can be controlled universally.

The remote maintenance concept is possible through the use of the Sm@rtClient display in the HMI application of the control room. Flexible configuration of the Sm@rtClient display enables the user to access any local HMI device he chooses.

Data access from other applications via web service (SOAP)

The opportunity for data exchange also exists between an HMI device and office applications, such as MS Excel, using a VBA macro.

For this purpose, the HMI device must support web service (SOAP). The Simple Object Access Protocol (SOAP) is used for the data exchange. A customized script or macro that has read or write access to the tags involved based on a specified syntax is called in the external application.

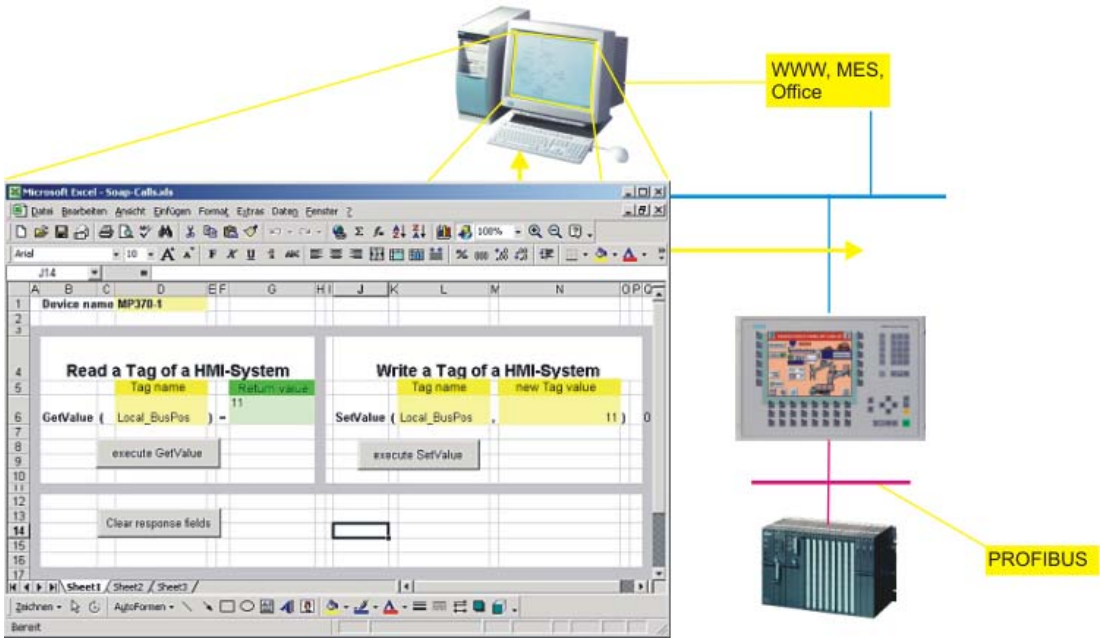


Figure 3-3 Communication with other applications

3.2 Use of Sm@rtAccess

3.2.1 Conditions for using the Sm@rtAccess option

HMI devices suitable for use

Sm@rtAccess can be used in connection with the following operator control systems.

- TP, OP, MP (270 series)
- MP 370
- OP 177B, TP 177B
- Mobile Panel 177 PN
- PC with WinCC flexible Runtime and the Windows 2000 or Windows XP operating system

Use restrictions

Observe the following notes on data quantities and system utilization when using the Sm@rtAccess and Sm@rtService options.

- Sm@rtServer and Sm@rtClient

  If a PC is used as a Sm@rtServer, select the highest-performance platform available. The server and client must have the same screen resolution.

  Use only simple projects. Avoid photographs and color gradients in screens.

  Avoid heavy background loading during operation, for example, due to scripts or archives.

  The maximum number of clients that can be interconnected with the server depends on the HMI device type of the server:

Sm@rtServer	Mobile Panel 177 PN	xP 177B	xP 270 6"	xP 270 10"	MP 370 12"	MP 370 15"	WinCC flexible Runtime
Number of Sm@rtClients	2	2	3	2	3	2	5

The count for each device includes one service client for remote monitoring and remote control using Microsoft Internet Explorer.

- SIMATIC HMI HTTP Protocol

  Tag exchange via the SIMATIC HMI HTTP protocol is not suitable for exchanging bulk data.

  The maximum number of connections depends on the HMI device type:

SIMATIC HMI HTTP Protocol	xP 177B Mobile Panel 177 PN	xP 270 / Multi Panel	WinCC flexible Runtime
Number of client connections	4	8	16
Number of active connections of a SIMATIC HMI HTTP server	4	8	16

Combining options on panels

Observe the following notes regarding the ability to combine various functions on panels when using the Sm@rtAccess and Sm@rtService options.

	SIMATIC HMI HTTP Protocol	Sm@rtServer	HTML browser	WinAC/ MP	ProAgent
SIMATIC HMI HTTP Protocol	--	Yes	Yes	Yes	Yes
Sm@rtServer	Yes	--	No	No	No
HTML browser	Yes	No	--	No	No
WinAC/ MP	Yes	No	No	--	Yes
ProAgent	Yes	No	No	Yes	--

3.2.2 Remote control via the Sm@rtClient display during runtime

Introduction

The Sm@rtAccess option of WinCC flexible enables access from the HMI device or PC to a remote HMI device via Ethernet.

Requirement

The license key for the Sm@rtAccess option is available on the HMI device.

Both devices are linked via a TCP/IP-ready network, that is, via a LAN or the Internet.

A project created using WinCC flexible ES with the Sm@rtAccess option is running on the remote device (server). The "Support Sm@rtAccess or Sm@rtService: Start Sm@rtServer" setting is selected in the project in the device settings under "Services in Runtime."

In order to use the Sm@rtClient display for remote control and remote monitoring, insert the Sm@rtClient display screen object in a screen in the project running on the client HMI device. Configure the server address either as a fixed value or as a tag in an input/output field.

Implementing remote access

The Sm@rtServer supports remote monitoring or remote control on the remote device (server).

On the client HMI device, the connection to the Sm@rtServer is made during runtime by means of the Sm@rtClient display.

On the HMI device only the screen of the server, and not the function keys, is displayed.

All mouse and keyboard actions are transmitted to the server and take effect there. The form of the cursor is not a part of the screen and is therefore not transmitted. Only the coordinates of the cursor are transmitted.

Notice

If a function key is activated on the client HMI device, this signal is transmitted to the server HMI device and goes into effect there only if no function has been configured for the function key on the client.

Otherwise, the function configured on the client is executed.

3.3 Scenario: Coordinated operator stations (distributed HMI)

3.3.1 Coordinated operator stations: Distributed HMI

Introduction

Distributed HMI enables operator control of a process from several coordinated operator stations. This system can be used by multiple operators as well as by a single operator.

Requirement

The "Sm@rtAccess" option is required for implementation.

Structure

In distributed HMI, multiple HMI devices are used as decentralized, coordinated operator stations that enable access to a centralized HMI device connected to the controller. The devices are linked via a TCP/IP-ready network, that is, via a LAN or the Internet.

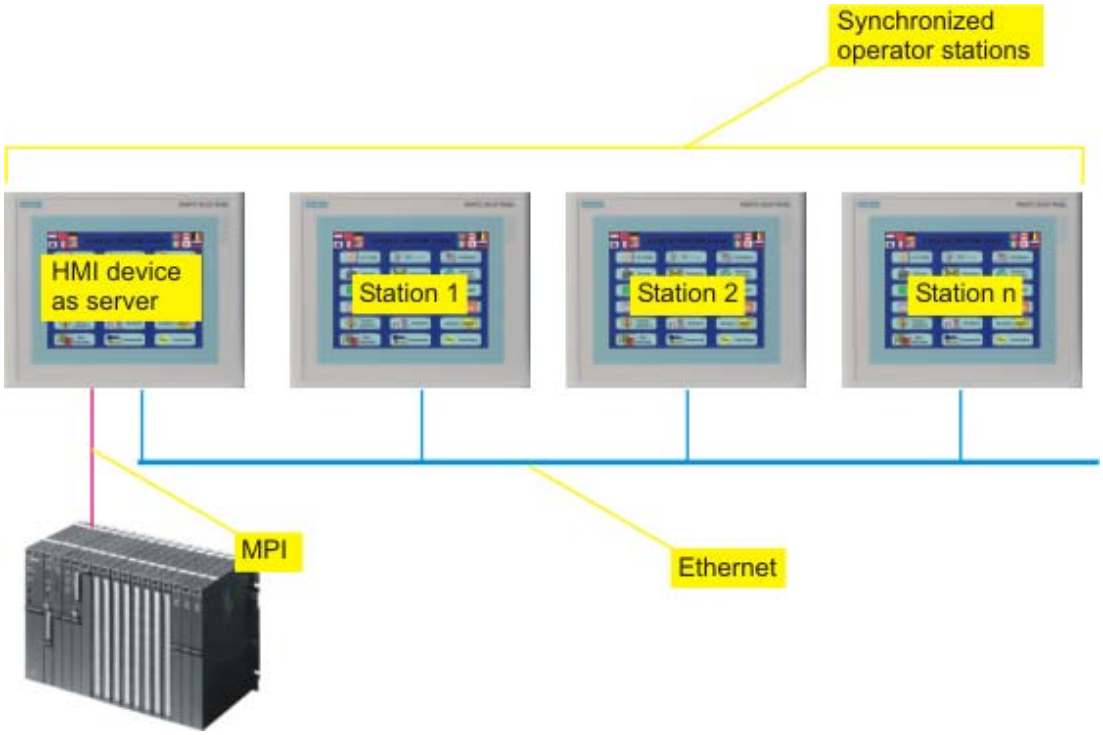


Figure 3-4 Distributed HMI

Only one HMI device (the server) contains configuration data. The server can be controlled from the other HMI devices.

The other decentralized operator stations are clients, all of which display the same process screen of the server.

All devices have the same screen resolution.

The operator stations are in shared mode. As soon as a defined period of time elapses without any action on an operator station, another operator station can become active. If Sm@rtClient display is configured accordingly, the user can also log off directly.

Advantages

This model has multiple advantages:

- Operator control and monitoring can be performed from various locations without significant effort.

  The project only has to run on one HMI device configured as a server. The same client project runs on all other HMI devices; the Sm@rtClient display object is contained in a screen on these devices. The screen of the server is displayed via the Sm@rtClient display.
- The server can be situated remotely from the machine and is thus not exposed to the environmental conditions of the machinery room.
- Coordinated operation is provided by the Sm@rtServer. Additional controller investments are not required. For example, the load on the field bus is also reduced – the communication load on the bus is removed due to the interlocking mechanisms on the controller side.

3.3.2 Example: Configuring coordinated operator stations

Task

Operator control of an extensive printing machine requires the option to exercise control, when necessary, at multiple locations along the machinery. Depending on his current location, the operator must be able to access the process from an operator station in the vicinity.

Procedure

Connect the HMI device containing the configuration data to the controller via PROFIBUS and to the other operator stations situated according to need via Ethernet.

Procedure on server

Proceed as follows:

1. Configure the project for machine control.

   Select the "Sm@rtAccess or Service: Start Sm@rtServer" check box in device settings under "Services for Runtime."

   This causes the HMI device to be configured as a Sm@rtServer.
2. Transfer the compiled project to the HMI device.
3. On the HMI device, select the "Start automatically after booting" check box on the "Remote" tab of WinCC Internet Settings" in the control panel, and click "Change settings."
4. In the "Sm@rtServer: Current User Properties" dialog, select the "Enable connections" check box, enter "Password 1" and "Password 2," and click "Advanced".
5. In the "Sm@rtServer: Current User Advanced Properties" dialog under "Connection priority," select the "Automatic shared sessions" option and enter the "Active user timeout" (for example, 10 seconds).
6. Clear the "Password needed" check box under "Forced write access" for forced access to the HMI device.
7. Transfer the license key for Sm@rtAccess to the HMI device.

Procedure on client

Proceed as follows on the operator stations:

1. Configure a small project for the HMI device type you want as an operator station.
2. Insert the Sm@rtClient display in the start screen.
3. Define the IP address of the central HMI device in the properties and set up "Password 1" configured on the server.
4. Select the "Allow Menu" setting.

   This provides the operator the option to log off using the menu.
5. Download the compiled project to all operator stations.
6. Transfer the license key for Sm@rtAccess to all operator stations.

Note

The 14-day license is not supported by Windows CE devices.

Result

After the server and operator stations are started, the operator sees the current process screen of the central HMI device at each operator station.

In order to control the server from an operator station, the operator must wait a specified amount of time following the last action on another HMI device.

If he uses the menu of the Sm@rtClient display to log off at the previously used HMI device, he can immediately control the server at the next HMI device.

3.4 Scenario: Communication between HMIs

3.4.1 Communication between HMI systems

Introduction

The Sm@rtAccess option in WinCC flexible enables communication between HMI devices via Ethernet.

Requirement

The license key for the "Sm@rtAccess" option is available in the HMI system.

Configuration

When communication between HMI devices takes place via the SIMATIC HMI HTTP protocol, an HMI device can have "read only" or "read/write" access to tags of another HMI device, depending on the configuration of the respective HMI device.

The HMI device providing the tags is the server; the other HMI device is the client. However, access to tags functions in both directions.

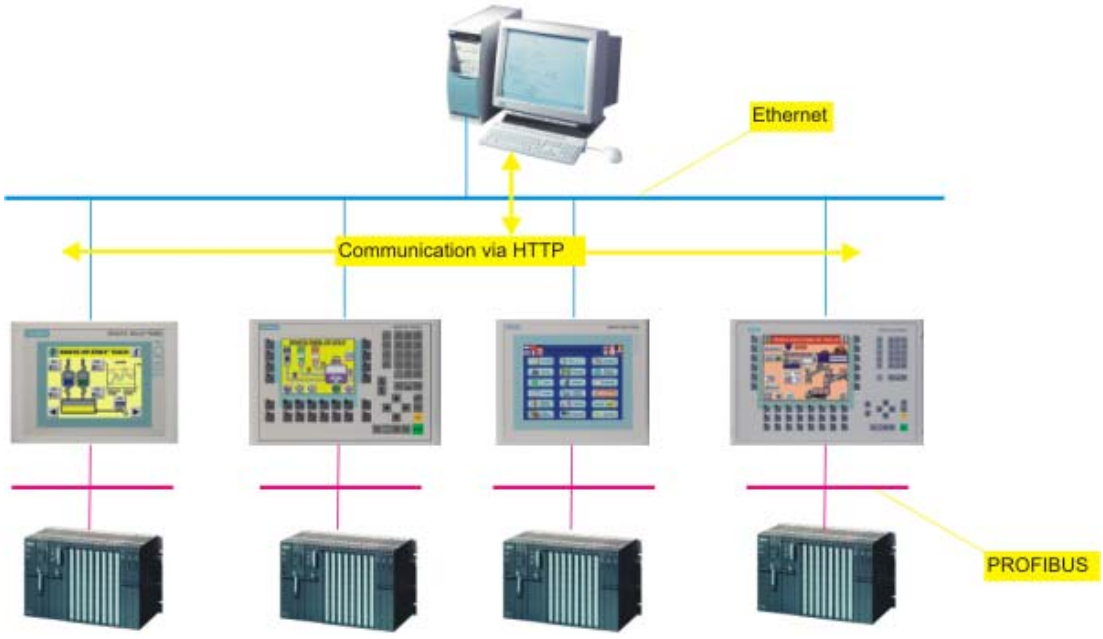


Figure 3-5 Communication between HMIs

Configuring the server

Multiple HMI devices are linked to their respective controller via PROFIBUS and to each other via Ethernet. In order for the tags of an HMI device to be made available to other HMI devices, the "Support Sm@rtAccess: Operate SIMATIC HMI HTTP Server" check box must be selected in the device settings under "Services in Runtime."

Configuring the client

In the project for the client HMI device that is to access the tags, create and link these tags to the tags of the server.

In "Communication," configure a connection based on the SIMATIC HMI HTTP protocol.

Settings

Settings for authentication, users, and user web authorizations must have been entered on the operator server device under the "Web Server" tab of "WinCC Internet Settings" in the control panel.

3.4.2 Example: Configuring an HMI system with common tags

Task

For a configuration with multiple HMI devices, tags are to be displayed in an overview screen in a maintenance application.

The panels are used as a tag server in the machine level. The maintenance application, which displays the essential machine tags in an overview screen, runs on a PC.

Procedure on server

The HMI devices of the HMI system are connected as an HTTP server to a central computer via Ethernet.

1. In the project for the individual HMI devices, select the "Support Sm@rtAccess: Operate as SIMATIC HMI HTTP Server."
2. Transfer the compiled projects to the HMI devices.
3. Establish the network connection between the devices.

Procedure on client

The central computer is used as a maintenance PC. It accesses all servers as a client.

1. In the project, configure in the maintenance PC the HTTP connection to each HMI device (server).
2. Create the necessary tags in the project for the maintenance PC and connect the tag addresses to the tags of the individual HMI devices.
3. Transfer the compiled projects to the HMI devices.
4. Establish the network connection between the devices.

For more detailed information, refer to the "Communication" configuration manual and "SIMATIC HMI HTTP Protocol."

Result

Once runtime is started and the connection between the HMI devices is established, the tags are continuously updated at the central maintenance PC.

3.4.3 Configuring the SIMATIC HMI HTTP communication driver

3.4.3.1 Installing the communication driver

Installing the communication driver

Installing HTTP components

The following HTTP components are supplied with WinCC flexible and installed when you transfer the configuration to the HMI devices:

- HTTP server
- HTTP client

For a standard PC or Panel PC, the following must also be installed:

- WinCC flexible Runtime

No special blocks are required on the HMI device for communication.

3.4.3.2 Configuring HTTP server

Configuring HTTP server functions

Procedure

In addition to the HTTP communication channels (in the control panel), it must also be ensured that the HTTP server is supported by WinCC flexible Runtime . These settings are defined in the project from WinCC flexible ES.

1. Double-click "Device settings" in the project window, and open the "Device settings" editor.

2. Select the "Sm@rtAccess: SIMATIC HMI HTTP Server" check box in the "Services in Runtime" area.

Before the HMI device can be used as an HTTP server, the project must be transferred to the HMI device.

See also

Communication between HMI systems (Page 3-10)

Configuring tags in HTTP servers

Tags used

The client can use the HTTP Protocol for read and write access to tags configured on the server in runtime. This means that it is not necessary to configure additional tags for an HTTP communication.

However, the following aspects must be taken into account to ensure correct data exchange:

1. The data type of the server tags must match the data type in the client,
2. The tag name configured in the HTTP server must be identical to the name of the address tag of the HTTP client.

3.4.3.3 Configuring HTTP clients

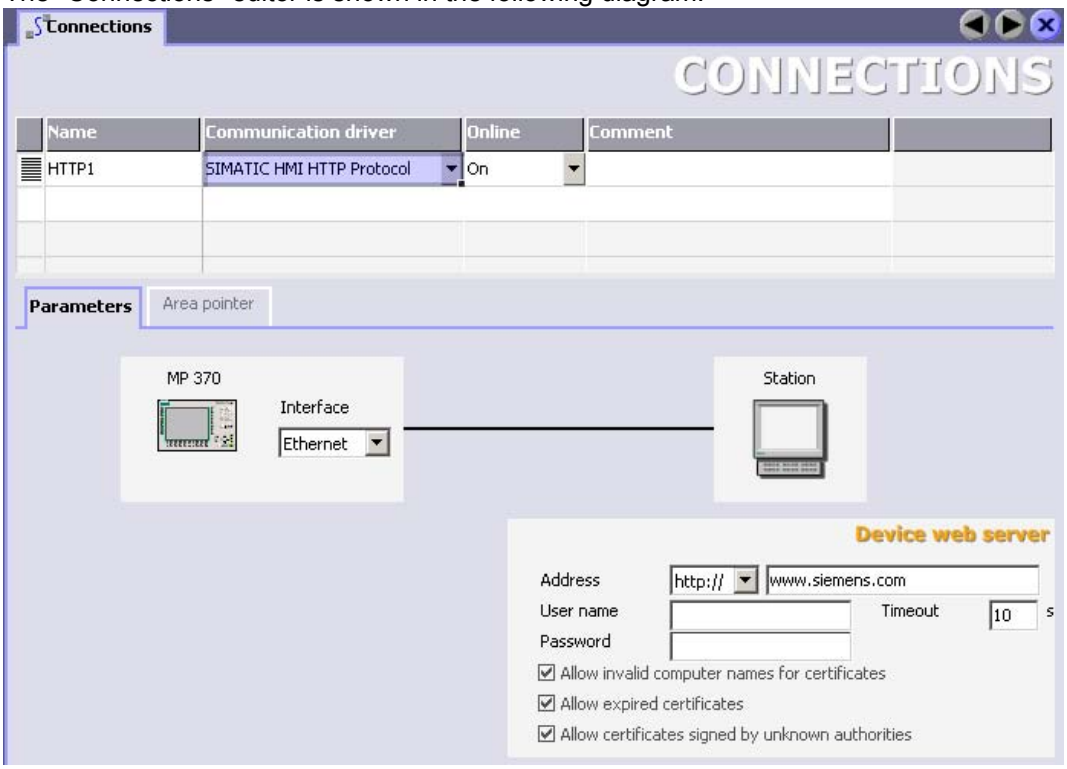
Configuring HTTP connections in the client

Procedure

To be able to access the tags on the HTTP server, a SIMATIC HMI HTTP protocol communication connection must be created.

1. Create a new connection using "Communication > Connections and assign it to the "SIMATIC HMI HTTP Protocol" communication driver.

   The "Connections" editor is shown in the following diagram.



2. Assign a name to this connection that indicates its function.

3. Define the parameters in the Properties view:

Interface	Select "Ethernet."
Address	Select the protocol http:// or https:// and enter the name of the HTTP server or its address to which communication is required. Ask your network administrator for the specific name or parameters of your network. If the server has already been commissioned, you can read out the IP address on the server as well: • Panel Click "Start > Programs > Command Prompt" on the server and enter the "ipconfig" command using the screen keyboard. The IP address is displayed after pressing <Ret>. • PC/Panel PC Click "Start > Run", enter "Cmd", and press <Ret>: The command interpreter is displayed. Enter the "ipconfig" command. The IP address is displayed after pressing <Ret>.
User name and password	If the "Authentication required" check box was selected in the HTTP server in the "Control Panel > WinCC Internet Settings > Web Server" dialog, a user name and password must be entered here in the client.
Timeout	The period after which a connection break is recognized.

4. If you have selected the HTTPS protocol, you can use the settings "Allow invalid computer names for certificates", "Allow expired certificates", and "Allow certificates signed by unknown authorities" to specify how the HTTPS client checks the properties of the server certificate and how it reacts to errors.

See also

Communication between HMI systems (Page 3-10)

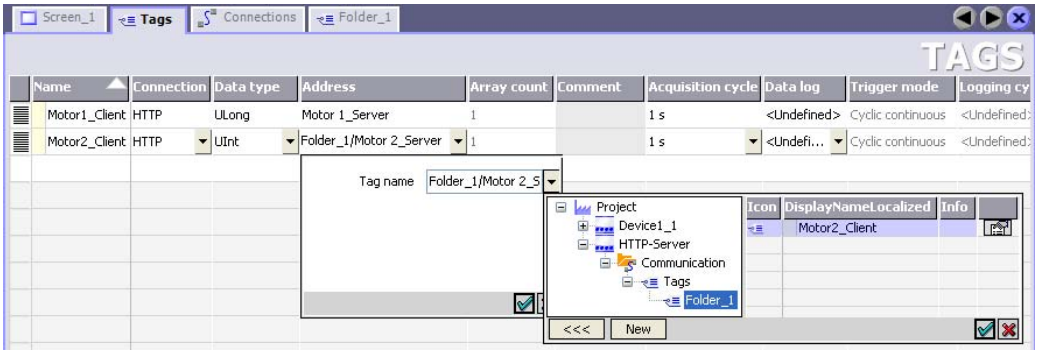
Configuring tags in HTTP clients

Procedure

In order to be able to access tags on the HTTP server, they must be configured in the client as tag addresses.

1. Create tags in the client project under "Communication > Tags" for all server tags you wish to access.

   The following figure illustrates the "Tags" editor with the browser open.



2. Define the parameters in the working area:

Name	Enter the tag names on the HTTP client
Connection	Select the HTTP connection
Data type	Select the data type of the tags: Note The client does not check the data type. Therefore, pay attention that the data type selected here matches the data type of the tags on the server. Note Array tags are not permissible.
Address	Enter the name of the tag to be used to communicate on the HTTP server exactly as it is written. If the tag to be addressed is located in a subfolder, the full path including tag name must be specified as the address, e.g. [folder name]\[tag name]. This is a particular advantage when the devices for server and client are in the same WinCC flexible Project. In this case, the names of the server tags can be selected in the editor browser and thus accepted.

3.4.3.4 Permitted data types

Permitted data types

When configuring tags, the data types listed below can be used.

Data types in the HTTP Protocol	Length	Signs	Range of values
Bool	0	No	true (-1) or false (0)
Char	1 bytes	yes	-128 to 127
Byte	1 bytes	No	0 to 255
Int	2 bytes	yes	-32768 to 32767
UInt	2 bytes	No	0 to 65535
Long	4 bytes	yes	-2,147,483,648 to 2,147,483,647
ULong	4 bytes	No	0 to 4,294,967,295
Float	4 bytes	yes	-3.402823E38 to -1.401298E-45 for negative values and 1.401298E-45 to 3.402823E38 for positive values
Double	8 bytes	yes	-1.79769313486231E308 to -4.94065645841247E-324 for negative values and 4.94065645841247E-324 to 1.79769313486232E308 for positive values
String	1 to 255 byte	——	
DateTime	8 bytes	——	1.1.1970 00:00:00 up to 31.12.2037 23:59:59

Please note that data types can be defined in external controllers which have different names in WinCC flexible. To ensure correct assignment, please observe the tag definition in the external controllers.

Note

It is not possible to access array tags from an HTTP client.

3.5 Scenario: Data access over a network

3.5.1 Web service (SOAP) - data access over a network

Introduction

WinCC flexible provides options for utilization of web service (SOAP). Web service (SOAP) is based on the Simple Object Access Protocol. Use of this protocol enables an external application to access tags of an HMI device via Ethernet.

Requirement

The license key for the "Sm@rtAccess" option is available on the HMI devices.

When the HMI device projects were configured, the "Sm@rtAccess support: Web service (SOAP)" was selected in the device settings under "Services in Runtime". Web Service (SOAP)" check box was selected in the device settings under "Services in Runtime" when the HMI device projects were configured.

Data access via web service (SOAP)

Data access via web service (SOAP) is mainly used for display of tags and setting of new values for tags in an external application.

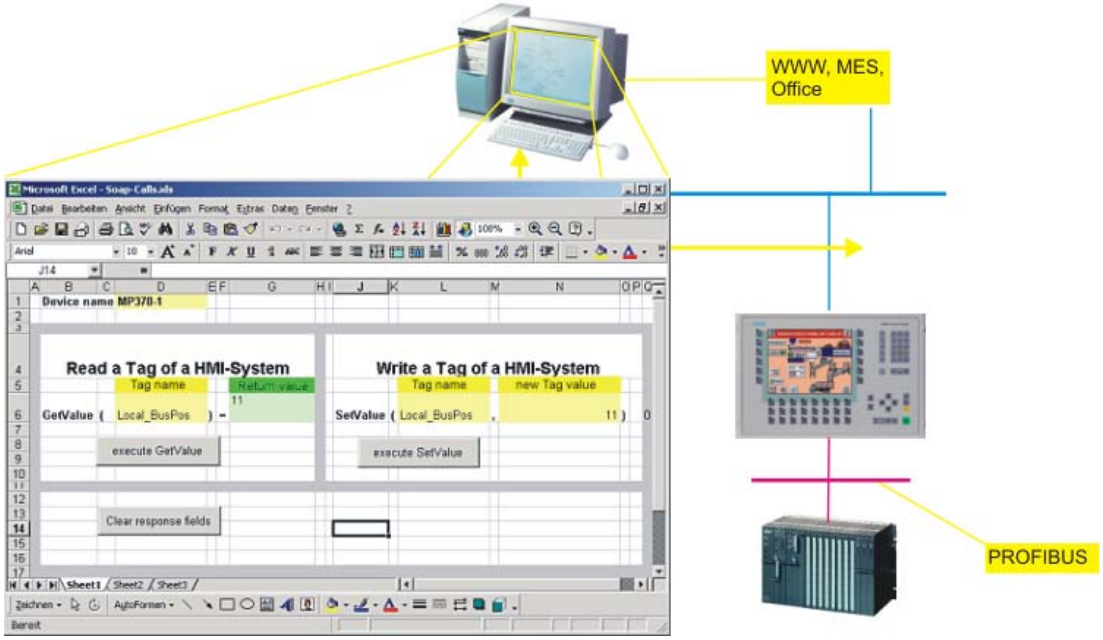


Figure 3-6 Communication with other applications

For example, a device is accessing two HMI devices. The operator sees the values of certain tags and can modify them.

3.5.2 Example: Editing tag values in MS Excel

Introduction

Data access over the network via web service (SOAP) is to be used to permit certain tags of an HMI device to be displayed and reset.

For this purpose, macros are written in Excel, which: 1) obtain the relevant tags on the PC over the network and display them, and 2) transfer reset values back to the HMI device.

Requirement

The license key for the "Sm@rtAccess" option is available on the HMI devices.

The SOAP toolkit is installed.

The "Support Sm@rtAccess: Web Service (SOAP)" check box was selected in the device settings under "Services in Runtime" when the projects were configured.

Procedure

The task can be solved using VBA macros "ReadTagValue" and "Write TagValue," which obtain and display the relevant tags in Excel over an appropriate interface and return them to the HMI device over the network.

1. Insert the "Control element toolbox" toolbar in your workbook in Microsoft Excel.
2. Create a new command button.

   The button is named "CommandButton1".
3. Double-click this command button.

   The macro editor is displayed. The "Click" event is already preset.
4. Write the "ReadTagValue" macro ("intVarTag_1" designates the actual tag value):

```
'--------------------------------------------------------------
Private Sub WriteTagValue()

Dim objRuntime
Dim intVarTag_1
Dim objWorksheetSet

objWorksheet = Excel.Worksheets("Sheet1")

Set objRuntime = CreateObject("MSSOAP.SoapClient")

objRuntime.mssoapinit "HTTP://servername/soap/RuntimeAccess?wsdl"
objRuntime.ConnectorProperty("AuthUser") = "Administrator"
objRuntime.ConnectorProperty("AuthPassword") = "100"
Var = objWorksheet.Cells(2, 3)
Value = objWorksheet.Cells(2, 5)
intVarTag_1 = objRuntime.SetValue(Var, Value)
objWorksheet.Cells(2, 8) = intVarTag_1

End Sub
'--------------------------------------------------------------
```

5. Label the button "Read value."
6. Insert another command button and double-click it.

7. Write the "WriteTagValue" macro ("intVarTag_1" designates the return value of the operation):

```
'---------------------------------------------------------------
Private Sub WriteTagValue()


Dim objRuntime
Dim intVarTag_1
Dim objWorksheetSet

objWorksheet = Excel.Worksheets("Sheet1")

Set objRuntime = CreateObject("MSSOAP.SoapClient")
objRuntime.mssoapinit "HTTP://servername/soap/RuntimeAccess?wsdl"
objRuntime.ConnectorProperty("AuthUser") = "Administrator"
objRuntime.ConnectorProperty("AuthPassword") = "100"
Var = objWorksheet.Cells(2,3)
Value = objWorksheet.Cells(2,5)
intVarTag_1 = objRuntime.SetValue(Var,Value)
objWorksheet.Cells(2,8) = intVarTag_1

End Sub
'---------------------------------------------------------------
```

8. Label the button "Write value."

Result

As soon as Macro 1 is called by double-clicking the "Read value" button, the specified intVarTag_1 tag is obtained from the HMI device using the specified IP address and displayed in the cell (1,1).

As soon as you call Macro2 by clicking the "Write value" button, the tag name is read from the cell (2,3), and the tag value is transferred from cell (2,5) to the HMI device.

Using Sm@rtService

4

4.1 Remote diagnostics and remote maintenance with Sm@rtService

Introduction

The Sm@rtService option can be used for remote control, remote diagnostics, and remote maintenance of operator stations via the Internet or company network. Panels of the 270 series, xP 177B, Mobile Panel 177 PN as well as Multi Panels and PCs with WinCC flexible Runtime are suitable for this purpose.

Technical implementation

Remote control and remote monitoring of stations with WinCC flexible using MS Internet Explorer requires TCP/IP communication (LAN, Intranet/Internet).

- Remote control of an HMI device via Internet Explorer

  An HMI device configured as a Sm@rtServer can be remotely monitored or remotely controlled from a Sm@rtClient.

- Providing of service and maintenance functions via HTML pages

  An integrated web server provides the following functions to standard HTML pages:

  - Remote control
  - Starting and stopping of HMI runtime for maintenance purposes
  - Remote access to recipe data records, password lists, and system-specific information
  - Access to files of the station via the integrated file browser
  - Downloading of configuration data

  The standard HTML pages can be supplemented with your own HTML pages.

- E-mail delivery

  During runtime, e-mails can be sent automatically to maintenance personnel via an SMTP (Simple Mail Transfer Protocol) server. The following events can trigger an e-mail to be sent:

  - Alarm of a certain alarm class
  - Event in which the SendEMail function is configured, such as a tag value change, etc.

4.2 Application scenario with Sm@rtService

Introduction

An example of a scenario that can be implemented with the Sm@rtService option is as follows:

Remote maintenance following e-mail notification

A factory has a service contract with an external service company. The HMI device and the service technician's PC are linked together over a TCP/IP-ready network. E-mail delivery of certain alarms to the service technician was configured in the project.

The service technician receives an e-mail that was triggered by an alarm during runtime. The service technician then establishes a connection to the HMI device using MS Internet Explorer.

The service technician initially sees the start page of the HMI device. The following topics are offered on the start page:

The service technician first sees the system alarms and then calls the device information (for example, the version release of the image).

Next, the service technician will want to remotely control the device in order to make any necessary changes in the control panel or to place the machine back to its initial state by accessing the process.

The service technician can connect to the HMI device from his work station using the remote control feature. He can display the user interface directly on his work station in Microsoft Internet Explorer.

Note

With Microsoft Internet Explorer, the service technician sees only the screen contents of the HMI device. This is sufficient for touch devices, but not for keyboard devices.

For this purpose, the Sm@rtClient application is offered on the HTML pages; this application can be started on the service PC. This application simulates the target device including the keys, thereby enabling the keys on the target device to be operated as well.

In this way, the technician can control the HMI device from his work station and monitor the ongoing process. He can undertake the necessary steps immediately and assess the urgency in which actions on the machine must be taken.

Advantage: An alarm that reaches the service technician in a timely manner helps to minimize unplanned downtime.

4.3 Conditions for using the Sm@rtService option

HMI devices suitable for use

Sm@rtService can be used in connection with the following operator control systems.

- TP, OP, MP (270 series)
- MP 370
- OP 177B, TP 177B
- Mobile Panel 177 PN
- PC with WinCC flexible Runtime and the Windows 2000 or Windows XP operating system

Use restrictions

Observe the following notes on data quantities and system utilization when using the Sm@rtAccess and Sm@rtService options.

- Remote control of an HMI device

  If a PC is used as a Sm@rtServer, select the highest-performance platform available. The server and client must have the same screen resolution.

  Use only simple projects. Avoid photographs and color gradients in screens.

  Avoid heavy background loading during operation, for example, due to scripts or archives.

  The maximum number of clients depends on the HMI device type:

- Integrated HTML pages

  The size of the HTML pages must not exceed 100 Kbytes in the case of Windows CE. When this number is exceeded, these pages can also be swapped out to external memory media.

- E-mail delivery

  The e-mail delivery function is not suitable for mass mailing of e-mails. It is intended for sending important messages.

Requirements for use in the company network

Access to the company network must be possible in order to implement this scenario. If the company network is protected by a firewall, the system administrator must isolate the relevant ports for this purpose.

- Access to integrated HTML pages

  The connection to the web server is established using Port 80.

- Access to Sm@rtServer for downloading the Java applet with Internet Explorer

  The connection to the Sm@rtServer for downloading the Java applet is established using Port 5800.

- Access to Sm@rtServer with Internet Explorer for remote monitoring and remote control

  The connection to the Sm@rtServer is established using Port 5900.

4.4 Remote control and remote monitoring by means of Sm@rtServer

Introduction

The Sm@rtService option of WinCC flexible enables access from the HMI device or PC to a remote HMI device via Ethernet.

Requirement

The license key for the "Sm@rtService" option is available on the HMI device.

Note

The 14-day license is not supported by Windows CE devices.

Both devices are linked via a TCP/IP-ready network, that is, via a LAN or the Internet.

A project created using WinCC flexible ES with the Sm@rtService option is running on the remote device (server). The "Support Sm@rtAccess or Sm@rtService: Start Sm@rtServer" setting is selected in the project in the device settings under "Services in Runtime."

Additional requirements must be satisfied according to the type of implementation.

Implementing remote access

The Sm@rtServer supports remote monitoring or remote control on the remote device (server).

Remote monitoring or remote control can be implemented on the local device (client) in various ways:

- By means of Internet Explorer
- By means of the Sm@rtClient application

Access via HTML pages

The Sm@rtService option enables access for remote control with Microsoft Internet Explorer and by means of integrated HTML pages of the server.

4.5 Types of remote control

4.5.1 Remote control by means of Internet Explorer

Introduction

On the client HMI device, the connection to the remote HMI device is established by means of Internet Explorer.

The window of the Internet Explorer displays only the screen of the remote HMI device, the server HMI device. If task switching is not disabled at the server HMI device, you can access the complete desktop.

Requirement

Note

Only one PC is involved as a client HMI device.

Internet Explorer V6.0 SP1 and higher is suitable.

Remote monitoring and remote control requires a Java applet that is automatically downloaded when the connection is first established and is then ready for use in subsequent sessions. For this purpose, the "Download applet" setting must be selected on the server in the "WinCC flexible Internet Settings."

The Java applet accesses the Java runtime environment that is installed on the client.

Note

The best results are obtained using Internet Explorer when the current Java Runtime Environment (JRETM) of Sun Microsystems has been installed. Go to www.java.com to download this program.

Sequence

The address of the remote device is first entered in Internet Explorer. The address consists of the server name and the HTTP port number that is set on the server. The default setting is: 5800.

Examples of addressing: "http://MyPanel:5800" or "http://192.168.168.1:5800".

Restrictions

The "Force write access with password" function cannot be implemented using the Java applet.

4.5.2 Remote control by means of the Sm@rtClient application

Introduction

The Sm@rtClient application provides the connection to the remote HMI device on the service PC.

In the Sm@rtClient application window, the entire layout of the remote HMI device is shown. You can use the mouse to operate all keys, including the function keys. In addition, the entire desktop can be accessed in the case of a PC.

Requirement

You have the Sm@rtService option.

Note

Only one PC is involved as a client HMI device.

Sequence

You can access the Sm@rtClient application, the program "SmartClient.exe", in various ways:

- If WinCC flexible Runtime is installed on the client device, the Sm@rtClient application is automatically installed as well.
- If WinCC flexible Runtime is not installed on the client device, several options are available:
  - You copy the Sm@rtClient application from the \Support\SmartClient directory on the WinCC flexible CD.
  - You copy the Sm@rtClient application via diskette or Intranet from the \Programs\Siemens\WinCC flexible\WinCC flexible RT directory from another PC.

In order to establish the connection to the remote HMI device, call the Sm@rtClient application and enter the IP address of the server.

Example: "192.168.0.1"

Note

If the Sm@rtServer at the server HMI device does not runs as a service, the connection established with the Sm@rtClient application is interrupted automatically as soon as the key combination CTRL+ALT+DEL is pressed at the server HMI device or the screen saver is active. In order for the Sm@rtServer to run as a service, the "Start automatically after booting" check box must be selected on the "Remote" tab in "WinCC flexible Internet Settings" in the control panel.

4.5.3 Installing the client and server certificates for SSL

Introduction

To ensure data security, data are encoded for transmission over the Internet. Encoding and decoding is performed by appropriate software – the certificates for SSL (Secure Sockets Layer).

- The client certificate for SSL must be installed on devices that are to be used to control a remote device.
- The server certificate for SSL must be installed on HMI devices that are to allow remote control.

4.6 Scenario: Remote maintenance for service

4.6.1 Remote maintenance for service

Introduction

The Sm@rtService option in WinCC flexible provides the option for remote maintenance by a service technician.

Application example

Flow rate is one of the properties measured for process control of a cooling unit. Contamination in a feed line reduces the flow of coolant. When the flow rate drops below the configured limit value, the HMI device displays a warning. This warning is also dispatched as an e-mail to the assigned service technician.

The service technician then establishes a connection with the remote device and takes the appropriate actions.

Advantage: An alarm that reaches the service technician in a timely manner helps to minimize unplanned downtime.

Remote control for service

By using remote control, the service technician can connect to an HMI device from a workstation over a network (Internet, LAN).

Example: A manufacturing facility has a service contract with an external service company. When service is needed, the service technician can connect to the HMI device.

He can retrieve the operator system and boot loader versions as well as the system alarms via the HTML pages provided by each panel. He can have the user interface displayed directly at his work station.

In this way, the technician can control the HMI device from his work station and monitor the ongoing process.

He can undertake the necessary steps immediately and assess the urgency in which actions on the machine must be taken.

4.6.2 Example: Remote maintenance for service

Introduction

A service technician receives an e-mail that was triggered by an alarm during runtime. The service technician then establishes a connection with the remote device and takes the necessary actions.

Procedure

In order to implement this scenario, the HMI device must be configured for remote control.

Configuring HMI device for remote control

The description below shows how to configure the HMI device so that it can be controlled remotely from the service technician's computer.

1. Configure the HMI device in such a way that other HMI devices or PCs can be connected to it.

   Select the "Support Sm@rtAccess or Service: Start Sm@rtServer" check box in device settings under "Services for Runtime."

2. Transfer the project to the HMI device.
3. Configure the remote control settings on the HMI device.

   To do so, call up access "WinCC Internet Settings" on the control panel and select the "Start automatically after booting" check box on the "Remote" tab. Click "Change settings" and select "Enable connections".

4. In order for the HMI device to be remotely controlled by the service technician, enter "Remote01" as "Password 2".

Result

As soon as the service technician starts the Sm@rtClient application on his computer, connects to the HMI device, and enters the password "Remote01", he can control the HMI device from his computer.

4.7 Scenario: Displaying integrated service pages

4.7.1 Integrated web server

Introduction

The operator can display and navigate between web pages during runtime using the web server integrated in the HMI device.

The web server can display local standard pages and – depending on the configuration – other configured HTML pages or HTML pages of a server accessible over Ethernet.

Requirement

The license key for the "Sm@rtService" option is available on the HMI device.

The "Support Sm@rtAccess: HTML pages" check box is selected in the device settings under "Services in Runtime" in the project on the server.

Purpose of the web server

The integrated web server permits HTML pages to be displayed during runtime over one of the following routes:

- Internet Explorer
- HTML browser screen object during runtime (not on Windows CE devices)

The following are displayed:

- Internal standard pages available by default on the HMI device
- Other pages that you configure
- Other Internet pages

An operator or service technician whose computer is connected to the HMI device over Ethernet can access service-critical information via the HTML pages. The standard HTML pages provide the following options:

- Remote control (if the HMI device is configured as a Sm@rtServer)
- Remote control using Microsoft Internet Explorer
- Starting and stopping of runtime
- Remote access to recipe data records and password lists
- Display of system information
- File management using a file browser
- Downloading of configuration data

HTML browser for HTML pages

HTML pages can also be displayed using the configured "HTML browser" screen object (not on Windows CE devices).

You can can also arrange for input or activation of an Internet address. As soon as the operator enters or activates an address, the HTML browser opens the relevant page.

The appearance and functionality of the HTML browser screen object depends on the HMI device type. On PCs, the HTML browser corresponds to the Internet Explorer installed.

Notice

Note that the HTML browser options during runtime are restricted due to operating device capacities and options.

See also

What are Sm@rtAccess and Sm@rtService? (Page 1-1)

4.7.2 Standard pages of the web server

Introduction

The operator can use Internet Explorer or the HTML browser screen object during runtime to display HTML standard pages without any additional configuration.

As a prerequisite, the "Support Sm@rtService: HTML pages" check box must be selected in the device settings on the HMI device for which HTML pages are to be displayed.

Standard pages

WinCC flexible Runtime and Panel Runtime has the following standard pages:

- start.html: Home page
- RemoteControl.html: Remote control (only for Internet Explorer)
- Control.html: Control functions
- StatusDetails.html: System diagnostics
- Browse.html: File browser (only for Internet Explorer)

Home page: Start.html

The start page contains the links to all other pages and displays current information about the project: Mode, software versions, device data, etc.

"Remote control": RemoteControl.html:

The "Remote control" page enables operator control of the HMI device for which a page is to be displayed. This page can only be displayed by using the Internet Explorer.

"Control functions": Control.html

The "Control functions" page enables the following options on the HMI device for which a page is to be displayed:

- Starting and stopping of HMI runtime

  Note

  The transfer mode has to be set in the loader menu at the HMI device.

- Exporting and importing of recipes
- Exporting and importing of password lists

  Note

  The password list must be named "pdata.pwl." It is exported to the following directory:

  On Windows CE devices: In the "\Flash\simatic\" target directory

  On PCs: In the directory that was set in the "HMILoader.exe" file

  The password list is exported and becomes active the next time Runtime is started.

"System diagnostics": StatusDetails.html

The System diagnostics" page contains system alarms from the alarm buffer.

"File Browser" – Browse.html

The "File Browser" page is used to administer directories and files on the remote device. This page can only be displayed by using the Internet Explorer.

See also

Application scenario with Sm@rtService (Page 4-2)

4.7.3 Example: Configuring an integrated web server

Task

In addition to the standard pages of the web server, you create your own HTML pages and download them to the respective HMI device. When creating your own HTML pages, you must observe certain guidelines so that pages will appear correctly and in their entirety on a Windows CE device.

Restrictions

Note that only a small amount of memory space is typically available depending on the HMI device type.

- Therefore, you should limit the size of your pages or, if necessary, use an external storage medium, such as a CF card.
- Configure only simple HTML pages, that is, without use of Java, scripts, and ActiveX.

Procedure

Create the HTML pages using a conventional text editor. For example, "Notepad" is a suitable editor, which can also be used to create the special tags described below.

As soon as a user connects to an HMI device using "http://<device name>", he is automatically forwarded to the start page http://<Device name>/www/start.html. This page represents the starting point for the HTML pages of the web server. Every standard page is accessible from the start page via a link.

For this reason, you insert a link for each of your HTML pages in the start page.

Note

When inserting links in the HTML page, you must differentiate between relative and absolute links. Make sure that absolute links start with "/www" to ensure that the document will be searched for in the correct directory. Example: "/www/MyDocument.HTML".

Location of prepared HTML pages

Standard pages are located as follows:

- On the PC: "<Runtime directory>\WebContent"
- On XP 177B: "<ES-Installationspfad>\Transfer\1.1\XP177B\WebContent.zip"
- on Mobile Panel 177 PN: "<ES-Installationspfad>\Transfer\1.1\XP177B\WebContent.zip"
- On MP 370: "<ES-Installationspfad>\Transfer\1.1\MP370\WebContent.zip"
- On XP 270: "<ES-Installationspfad>\Transfer\1.1\XP270\WebContent.zip"

Variable parameters in HTML pages

You can specify variable parameters in HTML documents. As soon as a page with variable parameters is opened, the parameters are replaced by specific values.

In the example below, the "HostName" parameter is replaced by the network name of the device.

<HTML> <HEAD> <TITLE> MiniWeb </TITLE> </HEAD> <BODY > Welcome on

<MWSL><!-- write(GetVar("HostName")); --></MWSL></BODY></HTML>

List of parameters that can be applied

Tag	Meaning
ProgramMemoryComplete	CE only: Total program memory
ProgramMemoryFree	CE only: Program memory available
ProgramMemoryUsed	CE only: Program memory utilized
FlashComplete	CE only: Total flash memory
ObjStrComplete	CE only: Total available flash memory
ObjStrFree	CE only: Volatile memory available
ObjStrUsed	CE only: Volatile memory utilized
DeviceType	Type of target device (as specified in the control panel)
BtLdVer	CE only: Bootloader version (as specified in the control panel)
BtLdRelDate	CE only: Bootloader release date
ImageVersion	CE only: Image version as it appears on the loader
DramSize	CE only: Size of DRAM
HostName	The name by which the device is logged on/identified in the network
RtState	Indicates whether Runtime is running on the target device
SystemMessageTable	Outputs a table containing the current system alarms

Display of process tags

Process tag values can also be displayed in HTML pages. The syntax is the same as for device tags: Use the tag name as a placeholder for the tag value.

Example: The project includes a tag named "Tag_1." The value of this tag is to be output on an HTML page.

In the example below, the value of "Tag_1" is displayed on the HTML page after the text "Value of Tag_1:"

<HTML> <HEAD> <TITLE> MiniWeb </TITLE> </HEAD> <BODY > Value of Tag_1: <MWSL><!-- write(GetVar("Tag_1")); --></MWSL></BODY></HTML>

Downloading HTML pages to the HMI device

In order to be able to access a newly created HTML page, it must be downloaded to the HMI device. The following options are available:

- Standard route (active Sync/CF card)

  Copy the files (HTML pages and pictures) following "\Flash\Simatic\WebContent". Access then takes place with "http://<device>/www/<HTML page>".

- Project transfer using WinCC flexible ES - this method also brings the standard HTML pages onto the HMI device.

  Create a file named "WebContent.zip". This file must contain all HTML pages and associated pictures. It is transferred to the Windows CE device where it is unpacked.

  Make sure to provide the correct path information because the files are unpacked in the directories specified in the zip file. Incorrect path information results in errors in direct addressing or due to links.

In order for the file to be located during a transfer operation, it must be in a particular directory:

A file that is to be transferred to an MP 370 must be located under \Transfer\1.1\MP370 in the WinCC flexible installation directory.

A file that is to be transferred to an xP 270 must be located under \Transfer\1.1\xP270 in the WinCC flexible installation directory.

A file that is to be transferred to an xP 177B or Mobile Panel 177 PN must be located under \Transfer\1.1\XP177B in the WinCC flexible installation directory.

Deleting HTML pages

The HTML pages transferred to a Windows CE device using WinCC flexible ES remain on the device.

If necessary, you can delete these pages using Explorer or the file browser accessible during runtime via the HTML browser object.

4.8 Scenario: E-mail notification from runtime

4.8.1 E-mail notification from runtime

Introduction

The Sm@rtService option of WinCC flexible provides the option to send messages automatically via e-mail.

The automatic e-mail delivery feature ensures that all people affected by the machine status (for example, shift engineer and sales manager) are informed in a timely manner.

Application example

Flow rate is one of the properties measured for process control of a cooling unit. Contamination in a feed line reduces the flow of coolant. When the flow rate drops below the configured limit value, the HMI device displays a warning. This warning is also dispatched as an e-mail to the assigned service technician.

The service technician then establishes a connection with the remote device and takes the appropriate actions.

Advantage: An alarm that reaches the service technician in a timely manner helps to minimize unplanned downtime.

Contents and triggers for e-mail delivery

The following events can trigger an e-mail to be sent:

- Alarm of a certain alarm class
- Event in which a standard function has been configured, such as a tag value change, etc.

Such an e-mail can have the following contents:

- Alarm text with process tags (maximum of 256 characters)
- Date/time
- E-mail address for replies

If you use e-mail gateways or SMS gateways, you receive access to standard networks, which requires external service providers. If configured accordingly, in critical situations the operator station sends an SMS to your mobile phone.

Enabling e-mail delivery and SMS

The HMI device can send e-mails to an SMTP server only. The server sends the e-mails to the addresses configured in the server.

Nothing else is required to send e-mails to addresses in the company network. However, an external service provider is required to access standard networks.

If an SMS communication is to be sent to service personnel, an SMS gateway is required as well.

Settings on the HMI device

The settings for e-mail delivery on the HMI device are carried out on the "E-mail" tab under "WinCC Internet Settings" on the control panel.

The "Sender" entry field is assigned the default value "Automation HMI device." This setting is useful if you want the receiver is to be able to determine the device where the e-mail originated, for example, "MP270 device on Production Line 2."

However, if the e-mail is sent via an authentication (in the case of a provider), you must enter a valid e-mail address for the "SMTP authentication," for example, "John.Doe@gmx.net".

4.8.2 Example: E-mail notification from runtime

Introduction

A service technician receives an e-mail that was triggered by an alarm during runtime. The service technician then establishes a connection with the remote device and takes the necessary actions.

Procedure

In order to implement this scenario, enable e-mail delivery in the project.

Enabling e-mail delivery

The following shows how to send alarms (alarm class "Error") to the relevant service technicians within the company network.

Settings in the project:

1. In the project, enter the e-mail address of the service technician for the "Error" alarm class.
2. In the project, enter the name of the SMTP server that will transmit the e-mails in the company network.

Settings on the HMI device:

1. On the HMI device, select the "Use the default of the project file" option under "SMTP server" on the "E-mail" tab in "WinCC Internet Settings" on the control panel.

   Alternatively, you can clear the "Use the default of the project file" option and enter the name of the SMTP server in the input field. This means that you can easily change the server name.

Result

If a tag (for example, a mixer rotational speed) violates the configured limit values, the corresponding alarm is both displayed on the HMI device and sent as an e-mail to the service technician.

Once the service technician has received the alarm by e-mail, he establishes a connection directly from his work station to the HMI device.

Reference

5

5.1 Settings in the project

5.1.1 Basic settings for Sm@rtAccess and Sm@rtService

Introduction

The settings required in the project in order to use the services of Sm@rtAccess and Sm@rtService are effected in the device settings under "Services in Runtime".

Purpose of the dialog box

The project allows the use of the services in Runtime.

Sm@rtAccess or Sm@rtService: Start Sm@rtServer

The HMI device acts as a Sm@rtServer and permits remote access.

Sm@rtService: HTML pages

The HMI device allows access to the existing HTML pages via the Internet Explorer or the HTML Browser screen item in Runtime .

Sm@rtAccess: Web service (SOAP)

The HMI device supports the data access to Runtime tags by means of SOAP (Simple Object Access Protocol).

Sm@rtAccess: SIMATIC HMI HTTP Server

The HMI device supports the SIMATIC HMI HTTP protocol and allows access to tags in Runtime in case of corresponding configuration.

Function as OPC server

The HMI device acts as an OPC server

Name of the SMTP server

The name of the SMTP server in the network that is used for e-mail dispatch.

If a corresponding setting is used in the control panel of the HMI device, the name set in the control panel is used and not the name set here.

Name of the SMTP sender

The name of the sender to be specified in the e-mail.

If a corresponding setting is used in the control panel of the HMI device, the name set in the control panel is used and not the name set here.

SMTP authentication

The e-mail address required for SMTP authentication.

If a corresponding setting is used in the control panel of the HMI device, the name set in the control panel is used and not the name set here.

5.2 Settings on the HMI device

5.2.1 "WinCC flexible Internet Settings" dialog, "E-mail" tab

Introduction

This dialog opens when you click "WinCC Internet Settings" in the control panel.

Purpose of the dialog box

Settings for utilizing e-mail delivery from runtime

SMTP server

When the ""Use the default of the project file"" option is selected, the name of the SMTP server for e-mail delivery is taken from the project (Device Settings, Services in Runtime).

If you select the second option, the server entered in the input field is applied as the SMTP server for e-mail delivery.

Sender

The name of the sender to be specified in the e-mail.

Authentication

The e-mail address required for authentication.

5.2.2 "WinCC flexible Internet Settings" dialog, "Proxy" tab

Introduction

This dialog opens when you click "WinCC Internet Settings" in the control panel.

Purpose of the dialog box

Settings for using a proxy server

Note

On a PC, this tab is located under "Internet Options," not in the "WinCC flexible Internet Settings" dialog.

Use proxy server

Activate this check box when an HTTP proxy server is used in the network. Otherwise the device cannot be used as a server because it cannot be found.

Proxy

Enter the name of the proxy server here.

Port

Enter the name of the port via which the device is to be addressed by the proxy server.

5.2.3 "WinCC flexible Internet Settings" dialog, "Web Server" tab

Introduction

This dialog opens when you click "WinCC Internet Settings" in the control panel.

Purpose of the dialog box

Settings for utilization of the integrated web server and the HTTP server and access to web authorization settings.

Tag access (Group)

Regulates access to tags via the SIMATIC HMI HTTP log:

- "Read/write": Tags can be read and rewritten
- "Read only": Tags can only be read

Tag authenticate (Group)

Regulates authentication to tags via the SIMATIC HMI HTTP log:

- "No authentication": No authentication (password) is required for access.
- "Authentication required": Authentication (password) is required for access. The password is specified while configuring the connection via the SIMATIC HMI HTTP log in the "Connections" editor.

Enable Remote-Transfer for Projects

(on panel only)

This setting enables remote transfer of project files.

Start automatically after booting

(on panel only)

The web server is automatically started immediately after the HMI device boots.

As a result, the web server can be utilized independent of runtime.

Note

If you are utilizing the web server on the PC and also want the web server to start automatically when the PC starts, insert a link to the "Miniweb.exe" program (located in the installation directory of Runtime) into the autostart folder.

Close with Runtime

The web server is closed along with Runtime.

User Administration

This opens the "UserDatabase-Edit" dialog for setting web authorizations for the web server, HTTP server, web service (SOAP), and Sm@rtServer.

Start Web-Server

Starts the web server explicitly.

Close Web-Server

Closes the web server explicitly.

See also

Communication between HMI systems (Page 3-10)

5.2.4 "UserDatabase-Edit" dialog

Introduction

This dialog opens when you click the "User Administration" button on the "Web Server" tab of "WinCC flexible Internet Settings".

Purpose of the dialog box

This dialog is used to set web authorizations for the web server, HTTP server, web service (SOAP) and Sm@rtServer.

The dialog box has three tabs.

- "User Manager" tab

  This tab is used to select and create/delete users.

  To create a new user, click "New" and enter the password twice. To delete a user, click "Remove." To apply the new and deleted user settings, click "Apply."

- "Description" tab

  Provides a description of the user selected on the "User Manager" tab for more precise identification (optional).

- "Authorizations" tab

  Enables web authorizations to be awarded and revoked.

  The list contains the web authorizations.

  To add each of the selected web authorizations to the list for the user selected on the "User Manager" tab, click "Add" or double-click.

  To remove each of the selected web authorizations from the list for the user selected on the "User Manager" tab, click "Remove" or double-click.

5.2.5 "WinCC flexible Internet Settings" dialog, "Remote" tab

Introduction

This dialog opens when you click "WinCC Internet Settings" in the control panel.

Purpose of the dialog box

Settings for utilizing the Sm@rtServer

"Start automatically after booting

The Sm@rtServer is automatically started immediately after the HMI device boots.

Otherwise, the Sm@rtServer starts together with the Runtime.

"Close with runtime

The Sm@rtServer is closed together with the Runtime.

"Change settings

This opens the "Sm@rtServer: Current User Properties" dialog for specifying passwords, authorizations, the screen update mechanism, and the behavior when connections are disconnected.

"Start Remoting

Starts the Sm@rtServer explicitly.

"Stop Remoting

Stops the Sm@rtServer explicitly.

5.2.6 "Sm@rtServer: Current User Properties" dialog

Introduction

This dialog opens when you click the "Change settings" button on the "Remote" tab of "WinCC flexible Internet Settings."

Purpose of the dialog box

This dialog enables specification of passwords, authorizations, the screen update mechanism, and the behavior when connections are disconnected.

Note

On the panel, this dialog is called "Sm@rtServer: Default Local System Properties" and contains fewer dialog elements than the dialog on the PC.

Incoming connections (Group)

Settings for handling an attempt to establish a connection

Enable connections

This setting enables the connection to the HMI device. It is a basic requirement for utilizing the Sm@rtServer from the outside.

If this check box is cleared, remote monitoring and remote control is not possible.

Password

(On the panel: "Password 1")

First password for remote access. "View only" is enabled by default.

Password 2

Second password for remote access. "View only" is enabled by default.

This password can be provided as a reserve password for third-party users (such as service technicians); it can be modified when necessary without significant effort within the organization.

View only

If this check box is selected, read access (monitoring mode) is the only access available when the corresponding password is entered.

Default: selected

Display or port numbers to use

Here, you select the TCP/IP port in the network where the Sm@rtServer waits for attempts to establish a connection.

- "auto": The Sm@rtServer itself automatically searches for the appropriate port.
- "display": The server utilizes Port 5900 plus display number. For HTTP, the server utilizes Port 5800 plus display number.
- "ports": You enter the port numbers for "main" and "HTTP" yourself.

Misc. (Group)

Other settings for various functions.

Enable network packets queuing (slower)

(On the panel: "Enable network packets queuing")

This setting enables splitting of data into multiple data packets, which are sent separately over the network.

It is useful when multiple clients are connected.

Remove Wallpaper

(On PC only)

This setting removes the screen background on the PC, thus saving transmission effort.

Default: selected

Disable local keyboard & pointer

The keyboard and mouse on the HMI device (on the server) are disabled as long as connections are active.

For example, this setting is useful when an HMI device is being administered from outside.

Initial screen scale

(On PC only)

This setting scales the height and width of the transferred screen according to the factor indicated:

- 1 = No reduction (default)
- 2 = 50% reduction in height and width
- 3 = 33% reduction in height and width, etc.

This reduces the amount of data transferred but also reduces the resolution and resulting quality of the screen.

Note

The reduced screen can be enlarged again on the client. However, the quality loss remains.

Update handling (Group)

(available on PC only)

The settings in this group govern how the image on the server screen is updated.

Usually, most changes are recognized automatically by the server. In case of problems, you can enter additional settings here.

The update method cannot be set on the panel. The "Poll Full Screen" setting always applies.

Poll full screen

(On PC only)

This setting specifies an update each time the screen changes. This setting provides you the lowest display error but places a maximum load on the server.

Turbo (requires more CPU)

This setting increases the scan frequency, thus recognizing changes faster.

You must determine the setting that is suitable for your configuration.

Poll foreground window

(On PC only)

This setting specifies an additional update when the active application window changes. It increases the load on the server.

Poll console windows Only

(On PC only)

This setting specifies an additional update when changes occur in a console window (MS input requirement).

Poll on event received only

(On PC only)

This setting specifies an additional update each time an entry is made.

Default: selected

Poll window under cursor

(On PC only)

This setting specifies an additional update when a change occurs in the operator control element under the mouse cursor.

Default: selected

When last client disconnects

(On PC only)

This setting governs the behavior after disconnection of the last client connection:

- "Do nothing": No response.
- "Lock workstation": Server is disabled.
- ""Logoff workstation": Server is shutdown.

The latter two settings are only useful if the Sm@rtServer is running as a service.

Advanced

This setting opens the "Current User Advanced Properties" dialog (on the panel: "Default Local System Advanced) containing the specifications for session management.

5.2.7 "Sm@rtServer: Current User Advanced Properties" dialog box

Introduction

This dialog opens when you click the "Advanced" button in "WinCC flexible Internet Settings," "Remote" tab, "Sm@rtServer: Current User Advanced Properties" dialog.

Purpose of the dialog box

This dialog enables specifications for session management.

Note

On the panel, this dialog is called "Default Local System Advanced" and contains fewer dialog elements than the dialog on the PC.

Query settings (group)

These settings govern acceptance of incoming attempts to establish a connection.

Query console on incoming connections

The Sm@rtServer registers the incoming attempts to establish a connection and displays a dialog on the screen in which the connection attempt can be accepted or rejected.

Query timeout

Here, you enter the waiting time after which the system decides on a response if the operator fails to act.

Default action

Here, you select the automatic response to an attempt to establish a connection once the waiting time expires:

- "Refuse": Reject attempt (operator control mode - single mode)
- "Accept": Accept attempt (operator control mode – shared mode)

Allow option to accept without password

The dialog for handling attempts to establish connections also contains the button "Accept without password." This gives you the option to accept an attempt to establish connection without a password.

Connection priority (group)

These settings govern handling of attempts to establish a connection by non-shared clients.

Disconnect existing connections

When an attempt is made to establish a connection by a non-shared client, the attempt is accepted; the existing connections are disconnected (single mode).

Automatic shared sessions

When an attempt is made to establish a connection by a non-shared client, the attempt is accepted; the prior existing connections are retained. Access is controlled using session management in shared mode.

Default: selected

Active user timeout

For shared mode, enter the time that must elapse without any actions on the active HMI device before access can be changed.

Default setting: 10 seconds

Refuse concurrent connections

If a non-shared client is already connected to the server, attempts to establish a connection by other non-shared clients are rejected.

Forced write access (group)

This setting governs forced access in an emergency contrary to normal session management.

Password needed

If this check box is not selected, any operator can force access in an emergency by pressing the <Shift> key four times, clicking four times, or touching the screen four times.

If this check box is selected, to force access an attempt must be made to gain access and a password must also be entered.

In this case, enter the applicable password in the input field underneath. If a password is not entered, it is not possible to force access in an emergency.

Note

On the server, access can only be forced by pressing the <Shift> key four times, clicking four times, or touching the screen four times.

Default: selected

Web access (group)

This setting governs downloading of the Java applet for utilizing Internet Explorer on the client device.

Download applet

Select this check box in order to enable automatic downloading of the Java applet on the PC the first time the connection is established.

The Java applet accesses the Java VM that is installed on the client and enables remote monitoring and remote control using Internet Explorer.

Default: selected

Administration (group)

These settings are additional settings for security.

Allow empty password

Select this check box in order to allow an "empty" password (on the panel: empty "Password 1").

Default: selected

Allow loopback connections

(On PC only)

This setting allows connections using your own PC. It is useful and necessary when security software is used for secure (encoded) connections.

Allow only loopback

(On PC only)

This setting allows only those connections to your own PC.

Log info to SmartServer.log

(On PC only)

This setting writes information to the server logbook.

Log extensive debug info

(On PC only)

This setting writes expanded information to the server logbook (for locating errors).

5.3 Dialogs of the Sm@rtClient application

5.3.1 "Connection details" dialog

Introduction

To display this dialog, click the icon for the Sm@rtClient application in the system tray of the task bar.

Purpose of the dialog box

This dialog is used for selecting the server and the connection method.

Server:

Here, you enter the address of the server to which the connection is to be established. The various options for for entering addresses are listed below.

Quick options (group)

Select the type of connection to the server according to the network you are using.

View only

This setting activates monitoring mode for this client. The server can only be monitored, and not controlled, from the current PC irrespective of the "WinCC Internet Settings" in the control panel of the server. Thus, inadvertent operator control actions are ruled out.

You can disable this setting during operation using the system menu.

Options

The "Options" dialog containing the technical settings for the Sm@rtClient application is displayed.

5.3.2 "Options" dialog box

Introduction

To display this dialog box, click the icon for the Sm@rtClient application in the system tray of the task bar as well as "Options" in the "Connection Details" dialog box.

Purpose of the dialog box

Technical settings for the Sm@rtClient application are carried out in this dialog box. The settings are assigned automatically with the selection under "Quick Options".

Only carry out modifications here in special cases.

Note

You can also carry out these settings in the Java Applet. Note that some of the dialog elements have other designations there.

Preferred encoding (group)

Settings for compressing (encoding) the screen data of the server. The selection under "Quick Options" is preassigned.

Select the desired compression or "Raw" (no compression).

Use CopyRect encoding

(in the Java Applet: Use CopyRect. Encoding)

Allows compression while using "similar rectangles".

Custom Compression level

Allows individual customizing of the compression level in the "Level" input field:

1 = fastest compression (less compression); 9 = highest compression (slowest).

Allow JPEG compression

Allows the use of JPEG compression (involves losses).

Enter the "Screen quality" in the input field underneath:
0 = maximum compression, 9 = least compression hardly any loss.

Misc (group)

Various different settings

Allow Cache Management

Allows the use of a cache memory for the transfer of screen sections which have already been transferred and which occur several times.

Optimizes the transfer for slow connections (for example per modem).

Request shared session

(in the Java Applet: Share desktop)

Declares this client to be a non-exclusive client.

Deiconify on Bell

Restores the minimized program window when, for example, a dialog box has to be confirmed at the server.

Default: selected

Disable clipboard transfer

Disables the actions from being transferred as well with the clipboard from PC to PC. Applies only to the copying and pasting of texts.

This functionality is not available at a Windows CE server.

Mouse (group)

(in the Java Applet: Mouse buttons 2 and 3)

Settings for the evaluation of mouse actions

Emulate 3 Buttons (with 2-button click)

Emulation of a three-button mouse by a two-button mouse.

Swap mouse buttons 2 and 3

(in the Java Applet: reversed/normal)

Mouse buttons 2 and 3 are swapped.

Cursor shape updates (group)

(in the Java Applet: Cursor shape updates)

Settings for the display of the cursor

Select the type of transfer of the mouse actions:

- Track remote cursor locally": The information on the location of the cursor is transferred separately from the screen information. This speeds up the transfer of the cursor. (JavaApplet: Enabled)

  "Let remote server deal with mouse cursor": The cursor is transferred as an integrated part of the screen information. This allows more accurate cursor positioning. (YES: Ignore)
- "Don't show remote cursor": The cursor at the server is not included in the transfer. (YES: Disable)

Display (group)

Settings for the screen display

Use CTRL + Cursor Key for Scrolling

The key combinations <CTRL> + cursor key are used to scroll within the local screen. They are thus not transferred to the server.

View only (inputs ignored)

Sets the view mode for this client irrespective of the settings on the server.

Fullscreen Mode

Displays the transferred screen on the full screen of the PC.

If the server screen is larger than the screen of the client, it is scrolled automatically by the mouse movement.

Scale Viewer Window by

Scales the display of the transferred screen in accordance with your entries. You can scale the screen up or down. The scaling is calculated by the client.

Scale Server Screen by

Scales the screen to be transferred at the server for this client in accordance with your entries. Servers with Windows CE ignore this setting.

You can only scale down the screen to be transferred, not scale it up.

"1/1" means: The setting at the server is effective.

Restricted Colors

(only in the Java Applet): Reduces the color depth at the client to 8 bits (256 colors). The data are then transferred faster. However, incorrect colors may result..

Index

U

W