Library for HTTP Communication (LHTTP)

SIMATIC S7-1500, Open User Communication

https://support.industry.siemens.com/cs/ww/en/view/109763879

Siemens Industry Online Support

Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG (“Siemens”). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.
Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

Disclaimer of liability

Siemens shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness and freedom from defects of the application examples as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Siemens against existing or future claims of third parties in this connection except where Siemens is mandatorily liable.
By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.
The Siemens terms of use (https://support.industry.siemens.com) shall also apply.

Security information

Siemens provides products and solutions with Industrial Security functions that support the secure operation of plants, systems, machines and networks.
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens’ products and solutions constitute one element of such a concept.
Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.
For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.
Siemens’ products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer’s exposure to cyber threats.
To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at: https://www.siemens.com/industrialsecurity.

Table of contents

1 Introduction

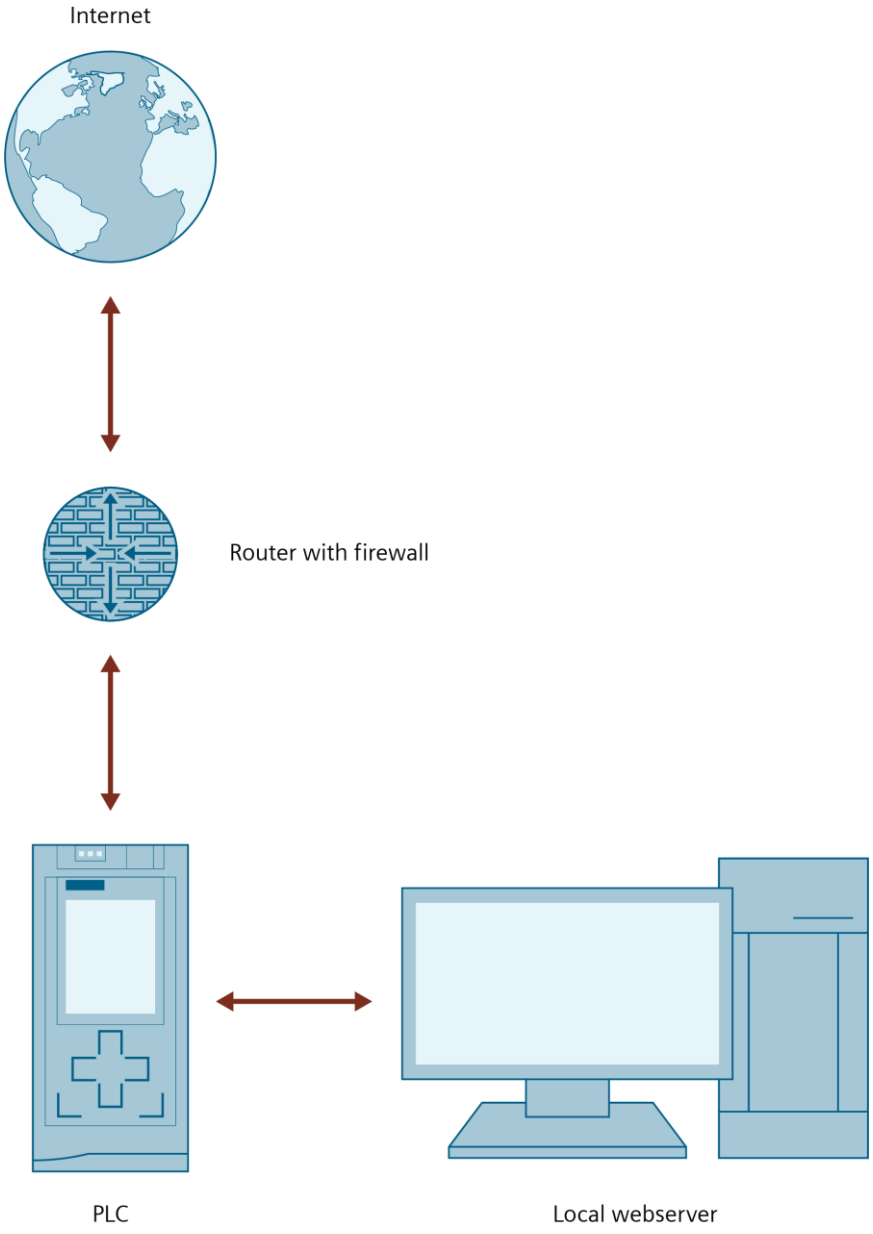
1.1 Overview

The Hypertext Transfer Protocol (HTTP) is a data transfer protocol used primarily to load Web pages from the World Wide Web.

Due to the increasing networking of plants and the advancement of the Internet of Things (IoT), HTTP and HTTPS also play an increasingly important role in automation technology.

The library for HTTP communication (LHTTP) enables the data exchange of a SIMATIC S7-1500 PLC via the integrated Ethernet interface with another device in the local network or a web server in the Internet via HTTP or HTTPS.

Figure 1-1: Overview



1.2 Mode of operation

The LHTTP library provides function modules with which the most conventional HTTP request methods can be implemented in the user program:

- GET
- POST

Due to the integrated certificate management in the TIA portal, it is also possible to transfer data securely with HTTPS using the same components.

1.3 Components used

This library was created with these hardware and software components:

Table 1-1: Components used

Component	Quantity	Article number	Note
SIMATIC S7-1500 CPU 1516-3 PN/DP	1	6ES7516-3AN01-0AB0	From FW 2.5
STEP 7 Professional V15.1	1	6ES7822-1AE05-0YA5	--

This library consists of the following components:

Table 1-2: Components of the application example

Component	File name	Note
Documentation	109763879_LHTTP_DOC_V10_de.pdf	This document
Building block library for TIA portal V15.1	109763879_LHTTP_LIB_V10.zip	--

2 Engineering

2.1 Components of the library

Function blocks and functions

Table 2-1: Function blocks and functions of the Library

Name	Version	Description
LHTTP_Get	V1.0.0	Realizes the HTTP method GET
LHTTP_Post	V1.0.0	Realizes the HTTP method POST
LHTTP_FindStringInArray	V1.0.0	Searches an array of chars for a given string
LHTTP_ExtractString FromArray	V1.0.0	Extracts a string between two specified text parts from an array of chars
LHTTP_ExtractString FromArrayExt	V1.0.0	Same function as "LHTTP_ExtractStringFromArray" with extended options

PLC data types

Table 2-2: PLC library data types

Name	Version	Description
LHTTP_typeTLS	V1.0.0	Data type for transferring certificates for secure communication via HTTPS

2.2 Interface description

2.2.1 LHTTP_Get

Description

The block implements the HTTP method GET to retrieve data from a web server.

Parameters

Figure 2-1: LHTTP_Get

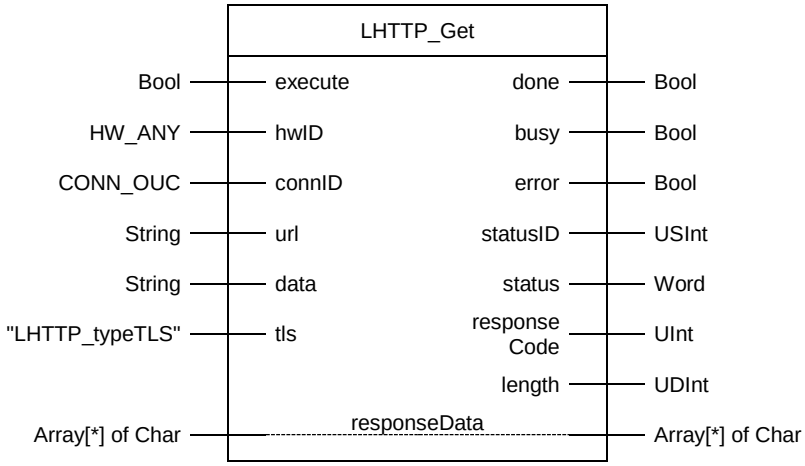


Table 2-3: Parameters of LHTTP_Get

Name	Declaration	Data type	Description
execute	Input	Bool	Send HTTP request
hwID	Input	HW_ANY	Hardware identification of the Ethernet interface
connID	Input	CONN_OUC	Unique connection ID
url	Input	String	URL, e.g. "http://httpbin.org/get"
data	Input	String	Optional parameters to append to the URL, e.g. "lang=en&country=de"
tls	Input	"LHTTP_typeTLS"	TLS certificates for secure data transmission (HTTPS), see section 2.2.6. For unsafe data transfer (HTTP) leave unconnected.
done	Output	Bool	Job finished
busy	Output	Bool	Job is being processed.
error	Output	Bool	An error has occurred in the processing of the FB.
statusID	Output	USInt	Specifies the source of the internal error, see section 2.4.
status	Output	Word	Internal status/error code of the FB, see section 2.4
responseCode	Output	UInt	Received HTTP status code
length	Output	UDInt	Length of the received user data
responseData	InOut	Array[*] of Char	received user data The array must start at "0".

Principle of operation

The user specifies the requested resource in the form of a URL, e.g. "http://httpbin.org/get" or "https://192.168.0.1:80/index.html", at the "url" parameter.

Optional parameters can be passed with two variants:

- Appended to the URL at the parameter "url" with a "?" in front, e.g. " URL, e.g. "http://httpbin.org/get?lang=en&country=de".
- At the separate parameter "data", e.g. "lang=en&country=de"

With a rising edge at the "execute" parameter, the block queries the IP address associated with the host at the configured DNS server if necessary and establishes a connection to the Web server.

If the specified URL starts with "https", a secure connection is established. In this case, the certificate of the requested web server must be referenced by the parameter "tls" (see section 2.2.6). If the web server requires client authentication, the certificate of the PLC must also be referenced.

The module creates the HTTP request from the specified URL and sends it to the server.

The server responds with the requested data or an error message. After all telegrams have been received successfully, the block closes the connection to the server again.

Note The block outputs the HTTP status code received from the server with the first received telegram and writes the user data of each received telegram directly into the memory area connected to the parameter "responseData". Evaluate the user data only after the output "done" has been set.

Note The block doesn't support redirects. If the server responds with a redirect (HTTP response code 3xx) the block outputs an error (see chapter 2.4).

Check the URL and correct it if necessary.

2.2.2 LHTTP_Post

Description

The block implements the HTTP method POST to transfer data to a web server.

Parameters

Figure 2-2: LHTTP_Post

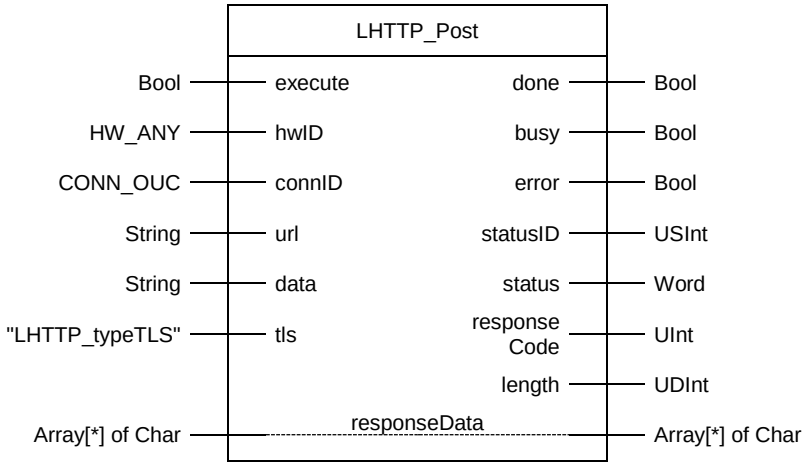


Table 2-4: Parameters of LHTTP_Post

Name	Declaration	Data type	Description
execute	Input	Bool	Send HTTP request
hwID	Input	HW_ANY	Hardware identification of the Ethernet interface
connID	Input	CONN_OUC	Unique connection ID
url	Input	String	URL, e.g. "http://httpbin.org/post"
data	Input	String	Message body
tls	Input	"LHTTP_typeTLS"	TLS certificates for secure data transmission (HTTPS), see section 2.2.6. For unsafe data transfer (HTTP) leave unconnected.
done	Output	Bool	Job finished
busy	Output	Bool	Job is being processed.
error	Output	Bool	An error has occurred in the processing of the FB.
statusID	Output	USInt	Specifies the source of the internal error, see section 2.4.
status	Output	Word	Internal status/error code of the FB, see section 2.4
responseCode	Output	UInt	Received HTTP status code
length	Output	UDInt	Length of the received user data
data	InOut	Array[*] of Char	received user data The array must start at "0".

Principle of operation

The user specifies the requested resource in the form of a URL, e.g. "http://httpbin.org/post" or "https://192.168.0.1:80/index.html", at the parameter "url".

The format of the user data to be transferred at the parameter "data" depends on the web server. For web form elements data is usually described in key-value pairs, e.g. "usr=admin&pwd=12345".

With a rising edge at the "execute" parameter, the block queries the IP address associated with the host at the configured DNS server if necessary and establishes a connection to the web server.

If the specified URL starts with "https", a secure connection is established. In this case, the certificate of the requested web server must be referenced by the parameter "tls" (see section 2.2.6). If the web server requires client authentication, the certificate of the PLC must also be referenced.

The module creates the HTTP request from the specified URL and sends it to the server.

The server responds with the requested data or an error message. After all telegrams have been received successfully, the block closes the connection to the server again.

Note The block outputs the HTTP status code received from the server with the first received telegram and writes the user data of each received telegram directly into the memory area connected to the parameter "responseData". Evaluate the user data only after the output "done" has been set.

Note The block doesn't support redirects. If the server responds with a redirect (HTTP response code 3xx) the block outputs an error (see chapter 2.4).

Check the URL and correct it if necessary.

2.2.3 LHTTP_FindStringInArray

Description

The function "LHTTP_FindStringInArray" searches an Array of Char for a string and returns its position as return value.

Parameters

Figure 2-3: LHTTP_FindStringInArray

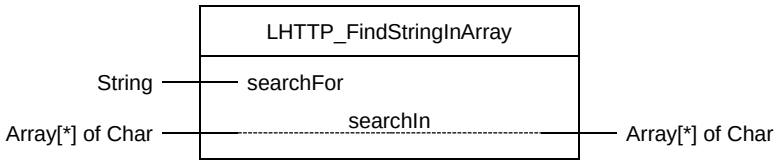


Table 2-5: Parameters of LHTTP_FindStringInArray

Name	Declaration	Data type	Description
searchFor	Input	String	Text to search for.
searchIn	InOut	Array[*] of Char	Array of Char to be searched.
Ret_Val	Return	DInt	Position (index) of the searched string in the array. -1: String was not found.

2.2.4 LHTTP_ExtractStringFromArray

Description

The LHTTP_ExtractStringFromArray function extracts a string between two specified text parts from an array of chars.

Parameters

Figure 2-4: LHTTP_ExtractStringFromArray

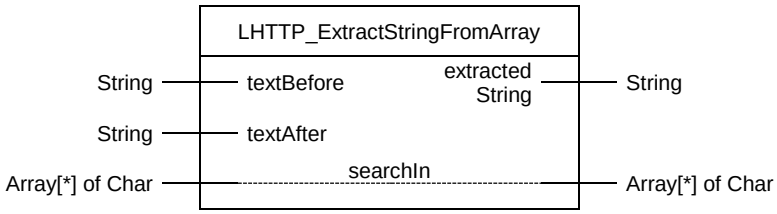


Table 2-6: Parameters of LHTTP_ExtractStringFromArray

Name	Declaration	Data type	Description
textBefore	Input	String	Text part before the text that is to be extracted.
textAfter	Input	String	Text part after the text that is to be extracted.
extractedString	Output	String	Extracted Text
searchIn	InOut	Array[*] of Char	Array of Char to be searched
Ret_Val	Return	Word	Return value: 16#0000: Successful, Text was found 16#9001: Only text before was found. String is output with max. length 16#9002: Neither text before nor after was found

2.2.5 LHTTP_ExtractStringFromArrayExt

Description

The function "LHTTP_ExtractStringFromArrayExt" extracts a string between two specified text parts from an array of char with extended options.

NOTE This function is part of the library to enable the user to parse the received data although it is not used by the blocks of the library.

Parameters

Figure 2-5: LHTTP_ExtractStringFromArrayExt

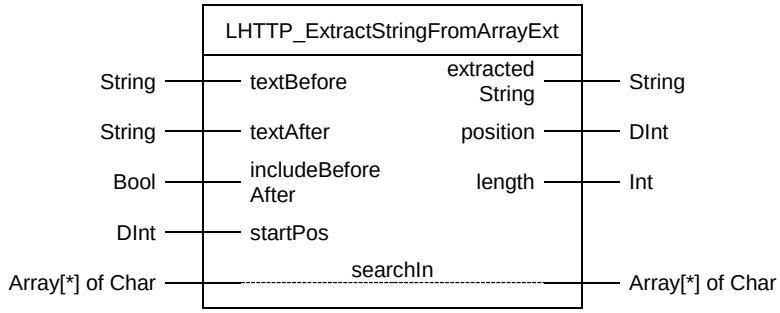


Table 2-7: Parameters of LHTTP_ExtractStringFromArrayExt

Name	Declaration	Data type	Description
textBefore	Input	String	Text part before the text that is to be extracted.
textAfter	Input	String	Text part after the text that is to be extracted.
includeBeforeAfter	Input	Bool	If TRUE, the text parts before and after are extracted as well.
startPos	Input	DInt	Position in the array from which the search is to be started
extractedString	Output	String	Extracted Text
position	Output	DInt	position (index) of the extracted text within the array
length	Output	Int	Length of the extracted text
searchIn	InOut	Array[*] of Char	Array of Char to be searched
Ret_Val	Return	Word	Return value: 16#0000: Successful, Text was found 16#9001: Only text before was found. String is output with max. length 16#9002: Neither text before nor after was found

2.2.6 LHTTP_typeTLS

The PLC data type "LHTTP_typeTLS" references the certificates required for secure connections via HTTPS.

Table 2-8: Parameters of LHTTP_typeTLS

Name	Data type	Value	Description
validateServerIdentity	Bool	FALSE	A set bit means that the client validates the subjectAlternateName in the server's X.509 V3 certificate to verify the server's identity. The certificates are checked when the connection is established.
serverCert	UDInt	0	ID of the X.509 V3 certificate (usually a CA certificate) used by the TLS client to validate the TLS server authentication. If this parameter is "0", the TLS client uses all (CA) certificates currently loaded in the client's Certificate Store to validate the server authentication.
clientCert	UDInt	0	ID of your own X.509 V3 certificate. This is only relevant if the TLS server requires client authentication and may be set to "0" otherwise.

Note The IDs of the certificates can be found in the global certificate manager under "Security settings > Security features > Certificate manager" or in the certificate manager of the respective device under "Device properties > Protection and Security > Certificate manager".

Detailed instructions can be found in the chapter 2.3.2.

2.3 Integration into the user project

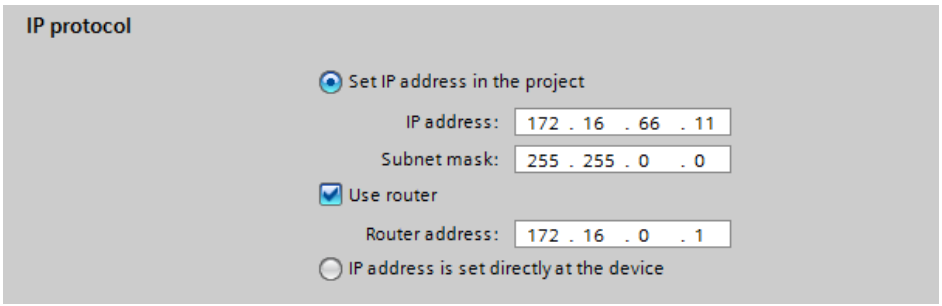
2.3.1 Configuring the Ethernet interface

Configure router

To operate HTTP communication across subnet boundaries, e.g. via the Internet, you must specify the IP address of your router in the device properties of your PLC. Proceed as follows:

1. Open the device properties of your PLC.
2. Open the "PROFINET interface [Xx] > Ethernet addresses" area of the PROFINET interface that you want to use for HTTP communication.
3. Select the Use router check box and specify the IP address of your router.

Figure 2-6

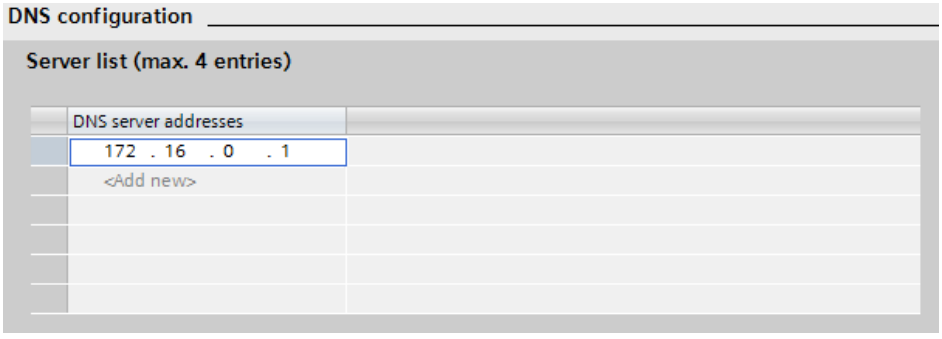


Configuring the DNS Server

To be able to use and resolve domain names in the URL, you must specify at least one DNS server in the device properties of your PLC. Often the router is also a DNS server. Proceed as follows:

1. If necessary, open the device properties of your PLC.
2. Open the "DNS configuration" section and enter the IP address of at least one DNS server.

Figure 2-7



2.3.2 Certificate management

With HTTPS, the user data is transmitted in encrypted form. Web server and client (in this case the PLC) exchange certificates with each other before data transfer. In order for the PLC to confirm the authenticity of the web server, it must know the root certificate from which the web server certificate is derived.

In the TIA Portal, the certificates are managed in a global certificate manager. The certificate manager contains an overview of all certificates used in the project. In the certificate manager, for example, you can import new certificates and export, renew, or replace existing certificates. Each certificate is assigned an ID that can be used to reference the certificate in the program modules.

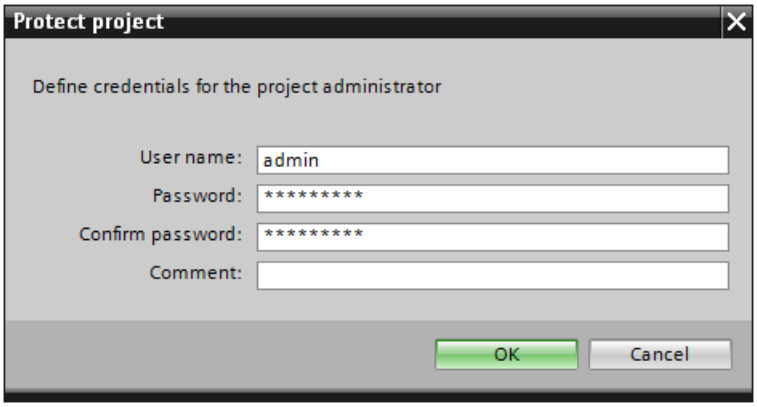
If you want to transfer data securely using HTTPS, perform the following steps:

TIA portal project protect with a password

In order to manage certificates in the TIA Portal, you must protect your project with a password. Proceed as follows:

1. Open the section "Security settings > Settings" from the project navigation.
2. Click on "Protect this project" and assign a user name and password.

Figure 2-8



Download Certificate from Web Server and Import to TIA Portal

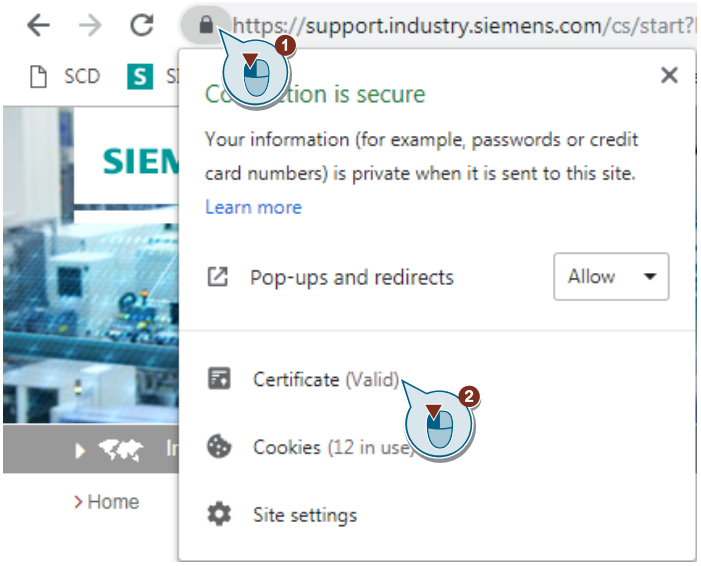
Proceed as follows to download the certificate from a Web page.

In the following the procedure with Google Chrome is described.

1. Open the desired web page in a web browser.

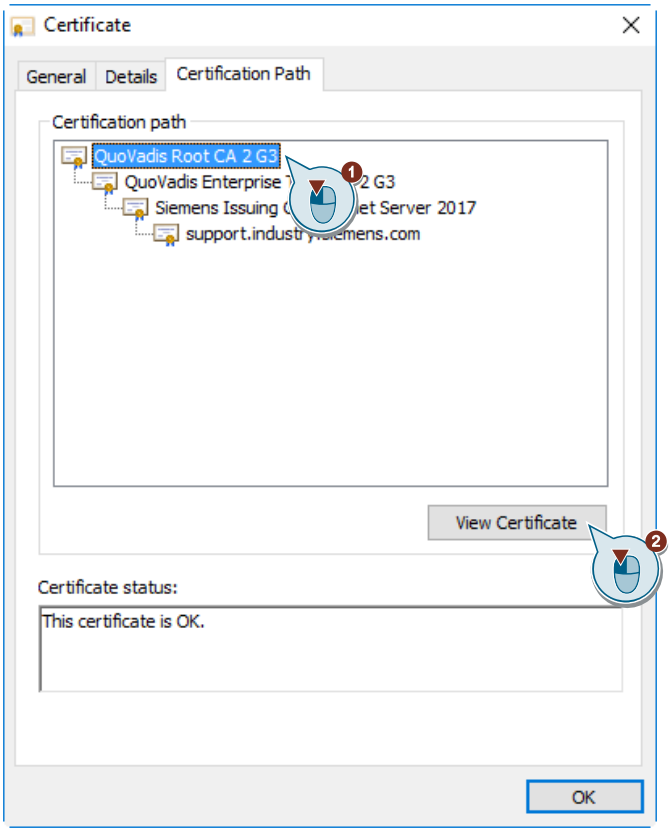
2. Click on the lock in the address bar and then on "Certificate (Valid)".

Figure 2-9



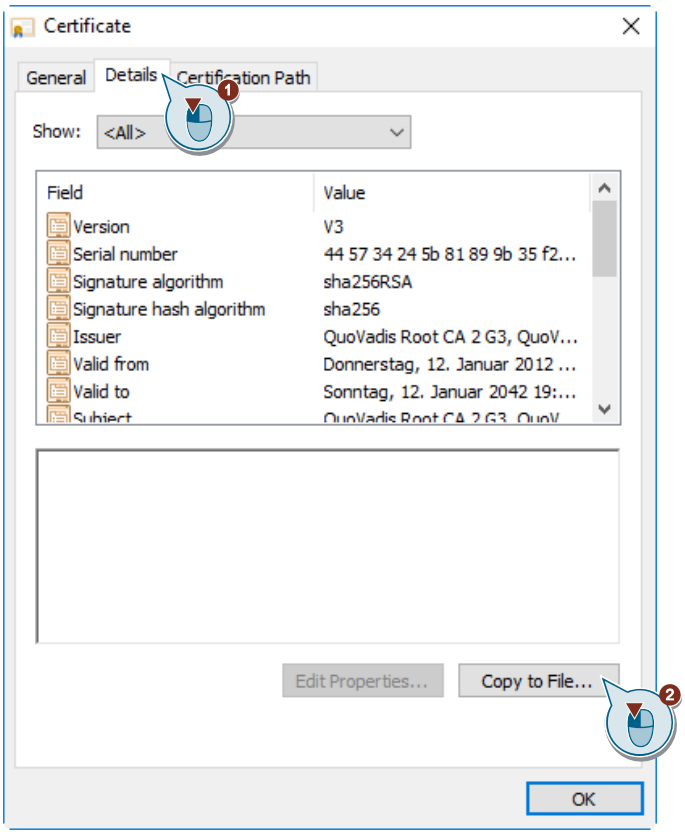
3. Open the "Certification Path" tab.
4. Select the top certificate (root certificate from which the others are derived) and click View Certificate.

Figure 2-10



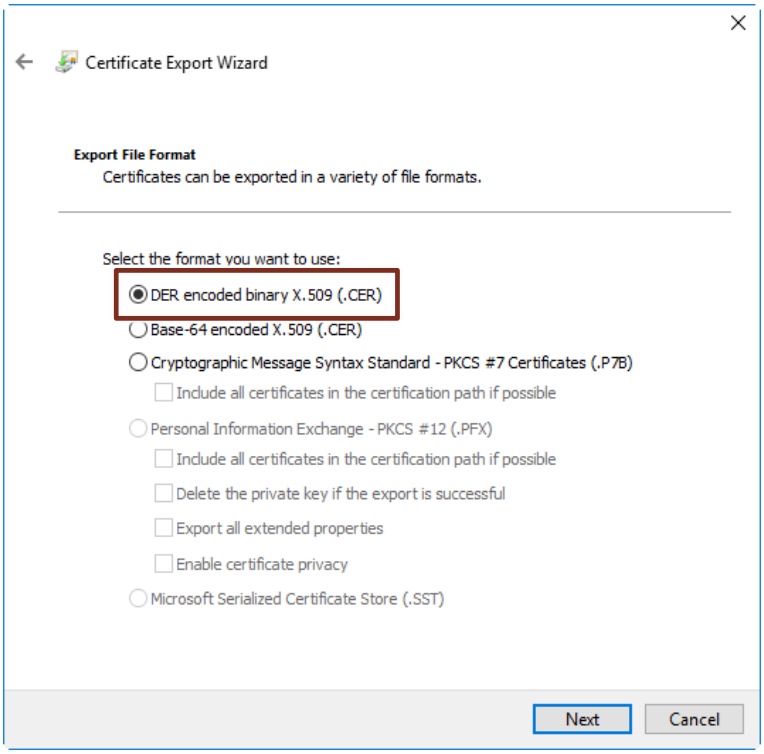
5. Open the "Details" tab, click on "Copy to file...".

Figure 2-11



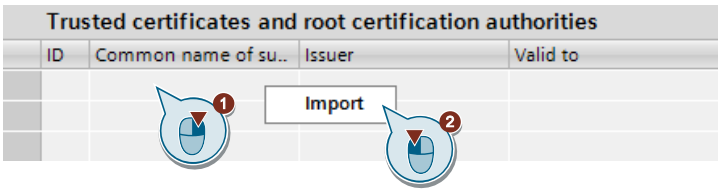
6. Save the DER-coded certificate.

Figure 2-12



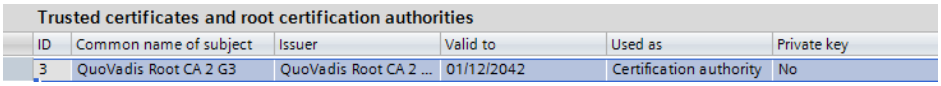
7. From the project navigation, open the "Security settings > Security features > Certificate manager" area.
8. Open the "Trusted certificates and root certification authorities".
9. Right-click in the workspace and select "Import".

Figure 2-13



10. Import the previously saved certificate from the web server.

Figure 2-14

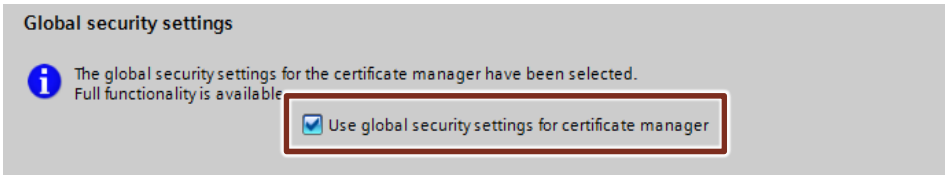


Create device certificate

For the encrypted connection for HTTPS, the client (in this case the PLC) must also provide a certificate. Proceed as follows to create the device certificate:

1. Open the device properties of your PLC.
2. Open the "Protection & Security > Certificate Manager" area.
3. To use the imported certificate from the Global Certificate Manager and derive a device certificate from the root certificate of the TIA Portal project, select the Use global security settings for certificate manager check box.

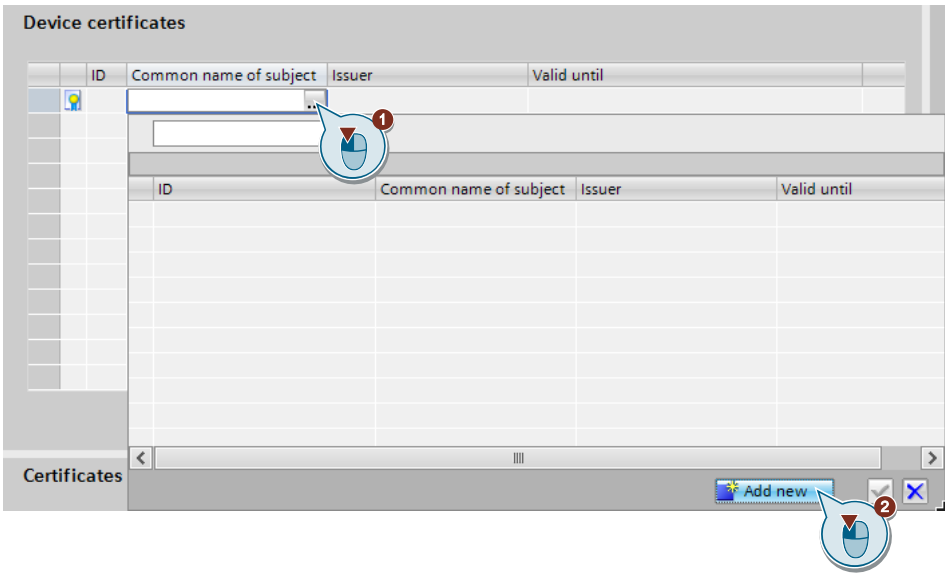
Figure 2-15



4. Under "Device certificates", double-click the "<Add new>" cell.

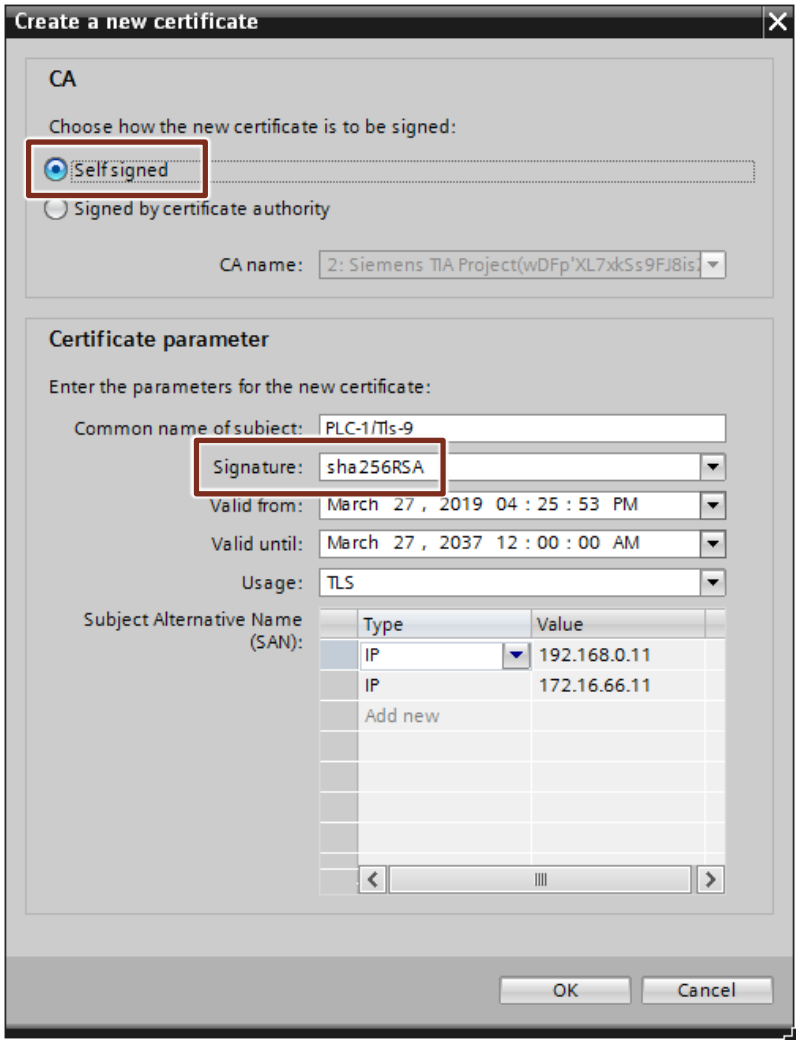
5. Click on the same cell again and then on "Add new".

Figure 2-16



6. Select "Self signed" and the encryption algorithm "sha256RSA" for the highest compatibility and confirm with "OK".

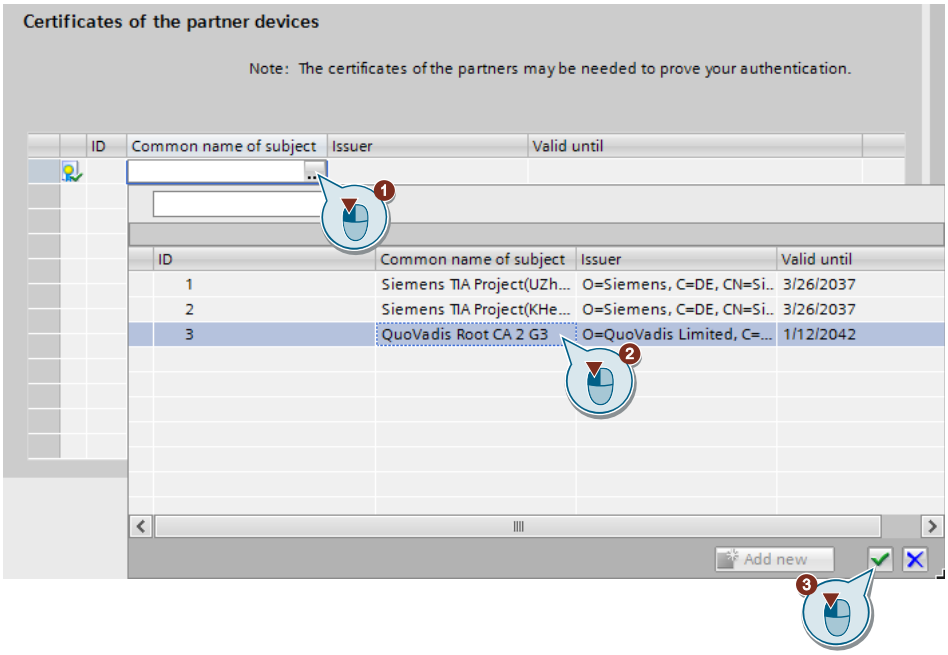
Figure 2-17



7. Under "Certificates of partner devices", double-click the cell "<Add new>".

8. Click the same cell again and select the Web server's imported root certificate.

Figure 2-18



2.3.3 Integrating blocks into the user program

For general information on dealing with libraries in the TIA Portal, see section 3.1.

1. Open the library "LHTTP" in the TIA Portal.
2. Open the folder "Types > LHTTP" and drag the FB for the desired HTTP method into the folder "Program blocks" of your PLC. The corresponding functions and PLC data types are automatically copied into your project.
3. Create a DB for controlling and evaluating the FB and open it.
4. Create at least the following variables:

Figure 2-19

HttpParam

	Name	Data type	Start value
1	Static		
2	get	Struct	
3	execute	Bool	false
4	url	String	''
5	data	String	''

5. If you use HTTPS, also create a variable of the PLC data type "LHTTP_typeTLS" (see section 2.2.6 for information on the PLC data type).

   Figure 2-20

HttpParam			
	Name	Data type	Start value
1	Static		
2	get	Struct	
3	execute	Bool	false
4	url	String	''
5	data	String	''
6	tls	"LHTTP_typeTLS"	

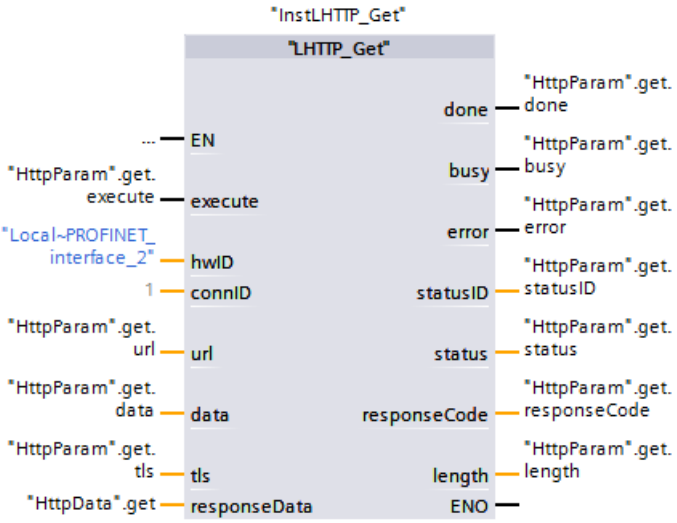
6. Create a DB for the data to be received and open it.
7. Create a variable of the data type "Array[x] of Char" with sufficient size for your application. Note that the array must start with "0".

   Figure 2-21

HttpData		
	Name	Data type
1	Static	
2	get	Array[0..8191] of Char

8. Call the FB at the desired location and create an instance.
9. Connect the parameters of the FB with the variables from the previously created DBs.

   Figure 2-22



10. Load the PLC.

Note Use different connection IDs at the parameter "connID" if you use "LHTTP_Get" and "LHTTP_Post" in parallel, use the FBs several times or use the OUC blocks for other functions in your program.

2.4 Error handling

The function modules "LHTTP_Get" and "LHTTP_Post" output both internal status/error codes describing the status of the function module and the HTTP status code received from the partner.

Table 2-9: Internal status/error codes

statusID	status	Meaning
0	16#0000	Order completed without errors
	16 #7000	No order active
	16#7001	First call of the instruction
	16#7002	Follow-up call of the instruction (instruction still running, "busy" = true)
	16#8101	The array at the parameter "responseData" does not begin with "0".
	16#8102	The size of the array at the parameter "responseData" is not sufficient to store the received user data. The array was completely filled and the length of the received user data is output at the parameter "length".
	16#8103	Invalid URL. Check the spelling.
	16#8104	The message header of the received reply is invalid.
	16#8105	Encoding of the received message could not be detected or is not supported.
	16#8106	The length of the user data could not be read.
	16#8107	Chunk-coded message could not be decoded.
	16#8300	The web server responded with a redirection. Redirections are not supported by the LHTTP library.
	16#8408	Request timeout. Check the Ethernet connection of the PLC and the URL.
	16#8600	The FB is in an invalid state.
1	--	Error in subordinate statement TSEND_C. See TIA Portal Information System for Workaround.
2	--	Error of subordinate statement TRCV. See TIA Portal Information System for Workaround.
3	--	Error of subordinate statement MOV_BLK_VARIANT in region "TE_IDENTITY". See TIA Portal Information System for Workaround.
4	--	Error of subordinate statement MOV_BLK_VARIANT in region "TE_CHUNKED". See TIA Portal Information System for Workaround.
5	16#9xxx	The web server responded with an error message. The received HTTP status code is output in the back digits of the output "status".

The following table lists common HTTP status codes:

Table 2-10: Common HTTP status codes

status code	Message	Meaning
2xx - Successful operation		
200	OK	The request was processed successfully.
3xx - Redirection		
301	Moved Permanently	The requested resource is now available at the address specified in the "Location" header field. The old address is no longer valid.
304	Not Modified	The content of the requested resource has not changed since the last request from the client and is therefore not transferred.
4xx – Client error		
400	Bad Request	The request message was structured incorrectly.
401	Unauthorized	The request cannot be performed without valid authentication.
403	Forbidden	The request was not executed due to lack of client authorization.
404	Not Found	The requested resource is not available in the required form.
5xx – Server error		
500	Internal Server Error	Unexpected service error.
502	Bad Gateway	The server could not fulfill its functionality as a gateway or proxy because it received an invalid response.
503	Service Unavailable	The server is temporarily unavailable.
504	Gateway Timeout	The server could not perform its function as a gateway or proxy because it did not receive a response from the servers or services it was using within a specified period of time.

Further HTTP status codes can be found on Wikipedia, for example:
https://de.wikipedia.org/wiki/HTTP-Statuscode

3 Additional information

3.1 Libraries in the TIA Portal

Most of the blocks are stored as types in the library. Thus the modules are versioned and can use the following advantages:

- Central update function for library elements
- Versioning of library elements

Note For information on library use in general, see the Guide to Library Use:

https://support.industry.siemens.com/cs/ww/en/view/109747503

Note All blocks in the library were created according to the programming style guide:

https://support.industry.siemens.com/cs/ww/en/view/81318674

For more information on libraries, visit the TIA Portal:

- How can you open, edit, and upgrade global libraries in the TIA Portal?
  https://support.industry.siemens.com/cs/ww/en/view/37364723
- In less than 10 minutes, TIA Portal: Time Savers – Global libraries
  https://support.industry.siemens.com/cs/ww/en/view/78529894
- Which elements from STEP 7 (TIA Portal) and WinCC (TIA Portal) can be stored in a library as a type or as a copy template?
  https://support.industry.siemens.com/cs/ww/en/view/109476862
- How can you automatically open a global library when starting TIA Portal V13 or higher and use it as a corporate library, for example?
  https://support.industry.siemens.com/cs/ww/en/view/100451450

4 Appendix

4.1 Service and support

Industry Online Support

Do you have any questions or need assistance?

Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.

The Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs, application examples and videos – all information is accessible with just a few mouse clicks:
https://support.industry.siemens.com

Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers – ranging from basic support to individual support contracts. Please send queries to Technical Support via Web form:
www.siemens.com/industry/supportrequest

SITRAIN – Training for Industry

We support you with our globally available training courses for industry with practical experience, innovative learning methods and a concept that's tailored to the customer's specific needs.

For more information on our offered trainings and courses, as well as their locations and dates, refer to our web page:
www.siemens.com/sitrain

Service offer

Our range of services includes the following:

- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog web page:
https://support.industry.siemens.com/cs/sc

Industry Online Support app

You will receive optimum support wherever you are with the "Siemens Industry Online Support" app. The app is available for Apple iOS, Android and Windows Phone:
https://support.industry.siemens.com/cs/ww/en/sc/2067

4.2 Links and literature

Table 4-1: Links and literature

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to the entry page of the application example https://support.industry.siemens.com/cs/ww/en/view/109763879
\3\	Specification of HTTP/1.1 (RFC 2616) https://tools.ietf.org/html/rfc2616
\4\	General information about HTTP by MDN https://developer.mozilla.org/en-US/docs/Web/HTTP
\5\	HTTP status codes https://en.wikipedia.org/wiki/List_of_HTTP_status_codes
\6\	Simple HTTP request & response service to test the blocks https://httpbin.org/#/

4.3 Change documentation

Table 4-2: Change documentation

Version	Date	Change
V1.0.0	05/2019	First version