Siemens SIMATIC S7 ISO on TCP

Siemens SIMATIC S7 ISO on TCP communication protocol

Supported device types and versions
Communication line configuration
Line protocol parameters
Communication station configuration
I/O tag configuration
Note on Siemens TIA Portal version 12 and above
Note on Siemens S7 1200/1500
Literature
Changes and modifications
Document revisions

Supported device types and versions

This protocol supports data reading/writing from the control PLC machines Siemens SIMATIC:

- types S7-300 and S7-400 equipped by an ethernet interface for the S7 ISO over TCP communication .
- types S7-1200, S7-1500
- Siemens LOGO
- Siemens Microbox

Note: communication via Profinet/Profibus adapter ACCON-NetLink-PRO compact produced by company DELTALOGIC has been verified. Communication with multiple S-300 series PLCs on Profibus worked after firmware upgrade of adapter to version V2.54 (31. march 2015) with adapter's BIOS version V2.39 (7. June 2011). When the adapter's firmware was version V2.37 (8. august 2011), communication could not be correctly established.
Note: communication with PLC Siemens LOGO was tested. A part of memory that is accessible for reading/writing is the **V area** which is seen as DB1.
Note: the protocol has a "big-endian" data representation.

Communication line configuration

- Communication line category: TCP/IP-TCP, TCP Redundant.
- IP address (addresses) is set according to a network configuration of a specific Siemens SIMATIC device.
- The port number is 102 (according to specification RFC 1006).
- The line number is not used, set on 1.

When a **TCP Redundant** communication line is configured, you can configure an IP address and port of a backup device. If a communication process lost the connection or is unable to connect to the device, it will switch periodically between the configured devices. KOM process tries to connect to a primary device at first.
Note: Multiple IP addresses of primary/backup devices can also be configured (separated by commas or semicolons).

Line protocol parameters

A dialog window of communication line configuration - **Protocol parameters** tab.
They influence some optional protocol parameters.

The following line protocol parameters are defined:

Parameter	Meaning	Unit / size	Default value
Rack	Siemens Simatic rack number. Rack 0 is most often used. Note: when using the ACCON-NetLink-PRO compact adapter, the Rack/Slot parameters must be set so that the MPI address of the S7 with which the D2000 KOM process communicates is equal to 32 * Rack + Slot. It is therefore necessary to create a separate line with specific Rack/Slot values for each S7. It is also necessary to set "RFC Routing over CPs with TSAP" to ON in the adapter web interface.	0 to 7	0
Slot	Siemens Simatic slot number. Slot 2 is most often used.	0 to 31	0
S7 Subnet ID-part 1 (hex)	S7 subnet address sent as a part of Remote TSAP if parameter Use long TSAP is set to True	0x0 to 0xFFFF	0
S7 Subnet ID-part 2 (hex)	S7 subnet address sent as a part of Remote TSAP if parameter Use long TSAP is set to True	0x0 to 0xFFFF	0
Use Secondary	The parameter allows the use of redundant PLCs, which may differ in the settings of some parameters (Rack, Slot, S7 Subnet ID). If its value is True, the primary and secondary parameters are used alternately when connecting to the PLC using the specified IP addresses.	-	False

Connection Resource (hex)	Connection resource, it enters as MSB byte to the calculation of the value of Remote TSAP at initialization of ISO Connection-request. See the description of parameter Use long TSAP. **Note:** in the specific case, when two systems (one of them D2000) needed to communicate with S7-300, they each had to have a different *Connection resource*, otherwise after sending the initial sequence of D2000 KOM process, the connection broke: /TSK1/Sending CR-TPDU: CLASS=0, SRC-REF=0x0001, TPDU size=1024, SRC-TSAP=10-00, DST-TSAP=03-02 /TSK1/OUT- <03><00><00><16><11><E0><00><00><00><01><00><C0><01><0A><C1><02><10><00><C2><02><03><02> recv error '10.94.11.237:102 (handle: 2888, objId: 2563271)' - WSA_ECONNRESET [10054] Task: L.N337-S7ExecTsk /TSK1/ After changing the *Connection resource* from 3 to 2, the communication started working. **Note**: according to Siemens documentation, the *Connection Resource* can be: • *0x01 - PG connection* (intended for programming) • *0x02 - OP connection* (designed for operator panel) • *0x03 - Other* (another purpose, can be used for multiple connections) • *0x10..0xDF - Connections with static or dynamic connection process* (various purposes, each usable for one configured connection) • *0xFD - S7 basic communication* (typically connections from CPU to another module within the subnet)	0x0 to 0xFF	3
Local TSAP (hex)	ISO Local TSAP (Transport Service Local Point). Source TSAP value during the initialization of ISO Connection-request. See the description of parameter Use long TSAP.	0x0 to 0xFFFF	0x1000
Source Reference	ISO Source Reference. Value of SRC-REF during the initialization of ISO Connection-request.	0 to 65535	1
Use long TSAP	Enables a long format of local and remote TSAP which is sent during the connection setup phase. Short TSAP is 2 bytes long. Short local TSAP has the following format: • 1. byte - higher byte of parameter Local TSAP • 2. byte - lower byte of parameter Local TSAP Short remote TSAP has the following format: • 1. byte - the value of parameter Connection Resource • 2. byte - combination of parameters Rack * 32 + Slot Long local TSAP is 28 bytes long. The last 2 bytes are higher and lower byte of parameter Local TSAP Full remote TSAP is 28 bytes long and it contains: • 5. byte - higher byte of parameter S7 subnet ID-part 1 • 6. byte - lower byte of parameter S7 subnet ID-part 1 • 9. byte - higher byte of parameter S7 subnet ID-part 2 • 10. byte - lower byte of parameter S7 subnet ID-part 2 • 11. byte - the value of parameter MPI/Profibus Address • 27. byte - the value of parameter Connection Resource • 28. byte - combination of parameters Rack * 32 + Slot	-	False
MPI/Profibus Address	MPI/Profibus address sent as a part of Remote TSAP if parameter Use long TSAP is set to True	0 to 126	1
ISO TPDU Size Variable Parameter	The maximum required size of ISO TPDU. The parameter value the initialization of ISO Connection-request.	8192, 4096, 2048, 1024, 512, 256 or 128 bytes	1024 bytes
Nr. of Parallel Network Threads	Maximum parallel communication threads. Increase the value if there is a demand for more data read from the device in a shorter time.	1 to 4	1
Cycle Time	The required time of one data reading cycle.	ms	1000 ms
Message Timeout	Maximal wait time on a reply from the device.	ms	2500 ms
Inter Message Delay	Delay before sending a data request. When a high data transfer rate is required, set 0 ms.	sec.ms	20 ms
Reconnect Delay	Delay before reconnection to the device if the connection has failed or some communication error has occurred.	sec.ms	2 sec
Connection Error Timeout	When Timeout passes and communication error occurs in all threads, a communication error status is set on the stations. The FALSE state is set on the communication line.	sec.ms	20 sec
S7 PDU Size	Maximum PDU in bytes at S7 communication with the device.	240, 480, 960 bytes	480 bytes
Tcp No Delay	Setting "*Tcp No Delay*" parameter causes the low-level socket option TCP_NODELAY to be set, thus turning off the default packet coalesce feature.	-	False

Debug Values	Activates debug info about the received values of I/O tags. Use this parameter only when communication must be debugged because it highly uses CPU and slows down the communication.	YES/NO	NO
Debug I/O Binary Packets Info	Activates debug info about the binary content of packets. Use this parameter only when communication must be debugged because it highly uses CPU and slows down the communication.	YES/NO	NO
Debug Requests Info	Activates basic debug info about requested data.	YES/NO	YES
Debug Answers Info	Activates basic debug info about received packets.	YES/NO	YES

Communication station configuration

- Communication protocol: **Siemens SIMATIC S7 ISO over TCP**.
- No station address, no protocol parameters on the station.
- The time parameter setting is ignored. See the line parameter Cycle Time.
- Time synchronization of the device is not supported.

I/O tag configuration

Possible I/O tag types: **Ai, Ao, Ci, Co, Di, Dout, TiA, ToA, TiR, ToR, TxtI**.

I/O tag address is compatible with Siemens SimaticNET OPC server.

I/O tag address is a character string according to the following:

```
{;}{S7:[connectionname]}DB<no>,<type><address>
{;}{S7:[connectionname]}DI<no>,<type><address>
{;}{S7:[connectionname]}<object>{<type>}<address>
```

or for structured I/O tags with configured Destination column

```
{;}{S7:[connectionname]}DB<no>,<type><address>{, <items>}
{;}{S7:[connectionname]}DI<no>,<type><address>{, <items>}
{;}{S7:[connectionname]}<object>{<type>}<address>{, <items>}
```

Where:

;	Optional parameter. It disables the I/O tag from communication, stops the I/O tag address check when it is saved, and can be useful when the communication with the device is being developed or debugged. Note: Also an I/O tag with an address starting with %IGNORE will be ignored.
S7:[connectionname]	Optional parameter. It does not contain any useful information but it is supported only because of backward compatibility with the Siemens SimaticNET OPC server.
DB	Data block. S7 variable identifier from "Data block".
DI	Instance data block. S7 variable identifier from " Instance data block".
<no>	A "data block" number or "instance data block" number.

<object>

Specification of block or area in S7 PLC.
Possible values:

Value	Description (German name)
I	**I**nput (**E**ingang, E)
Q	**O**utput (**A**usgang, A)
PI	**P**eripheral **I**nput (**P**eripherie **E**ingang, PE)
PQ	**P**eripheral Output (**P**eripherie **A**usgang, PA)
M	**M**emory bit (**F**)
C	**C**ounter (**Z**ähler, Z) - BCD coded integer numbers <0-999>
T	**T**imer (**T**imer, T) - BCD coded time values from intervals <0.00-9.99>, <00.0-99.9>, <000-999>, <0000-9.9990>
S	System Status Lists (**S**ystem-**Z**ustands**L**isten, SZL) - lists with diagnostic information that are available on CPU family S7-300 and S7-400. Diagnostic information differs for various classes of PLC and details are described in manuals (e.g. System Software for S7-300/400 System and Standard Functions, Volume 1/2) **Note:** I/O tag S must be of TxtI type.

<type>

The data type of S7. It is not specified for T, C, and S objects.

Identifier <type>	Description
X	Bit (boolean). Specify a bit number 0 to 7 - e.g. DB9,X8.3
B BYTE	Byte (8 bits unsigned).
W WORD	Word (16 bits unsigned).
D DWORD	Double word (32 bits unsigned).
CHAR	Character (8 bits signed).
INT	Integer (16 bits signed).
DINT	Double integer (32 bits signed).
BCD	BCD-coded 2-byte number (0-9 999)
LBCD	BCD-kódované 4-byte number (0-99 999 999)
REAL	Floating-point number (32 bits according to IEEE754 standard).
LREAL	Long floating-point number (64 bits according to IEEE754 standard).
STRING	String. Specify the maximal length of the string.
CHARARR	An array of CHARs interpreted as a string. The array length must be specified.
DATE	Date, 2 bytes (the number of days since January 1st, 1990)
DT	Date and Time, 8 bytes in BCD format, millisecond accuracy
DTL	Date and Time, 12 bytes in BCD format, nanosecond accuracy Note: D2000 uses only a millisecond accuracy
TIME	Time (32 bits signed) in ms. Note: if the I/O tag is of the TiR type, it is necessary to ensure the conversion by configuring the linear conversion (A=0.001, B=0) on the *Conversion* tab
S5TIME	Double byte time - Simatic S5 format (0 - 9990 seconds with variable accuracy 0.01 - 10 seconds). Measured points of the type Ai/Ao, Ci/Co, TiR/ToR are supported. Note: An alternative to this data type is to use the "W" type and set the "Simatic S5Time" conversion.
TOD	Time of day (32 bits unsigned) in ms.

Note: The CHARARR type is a D2000 extension that allows you to read/write an array of CHARs as a string. This type is not compatible with the Siemens SimaticNET OPC server addressing.
The difference between CHARARR and STRING is as follows:

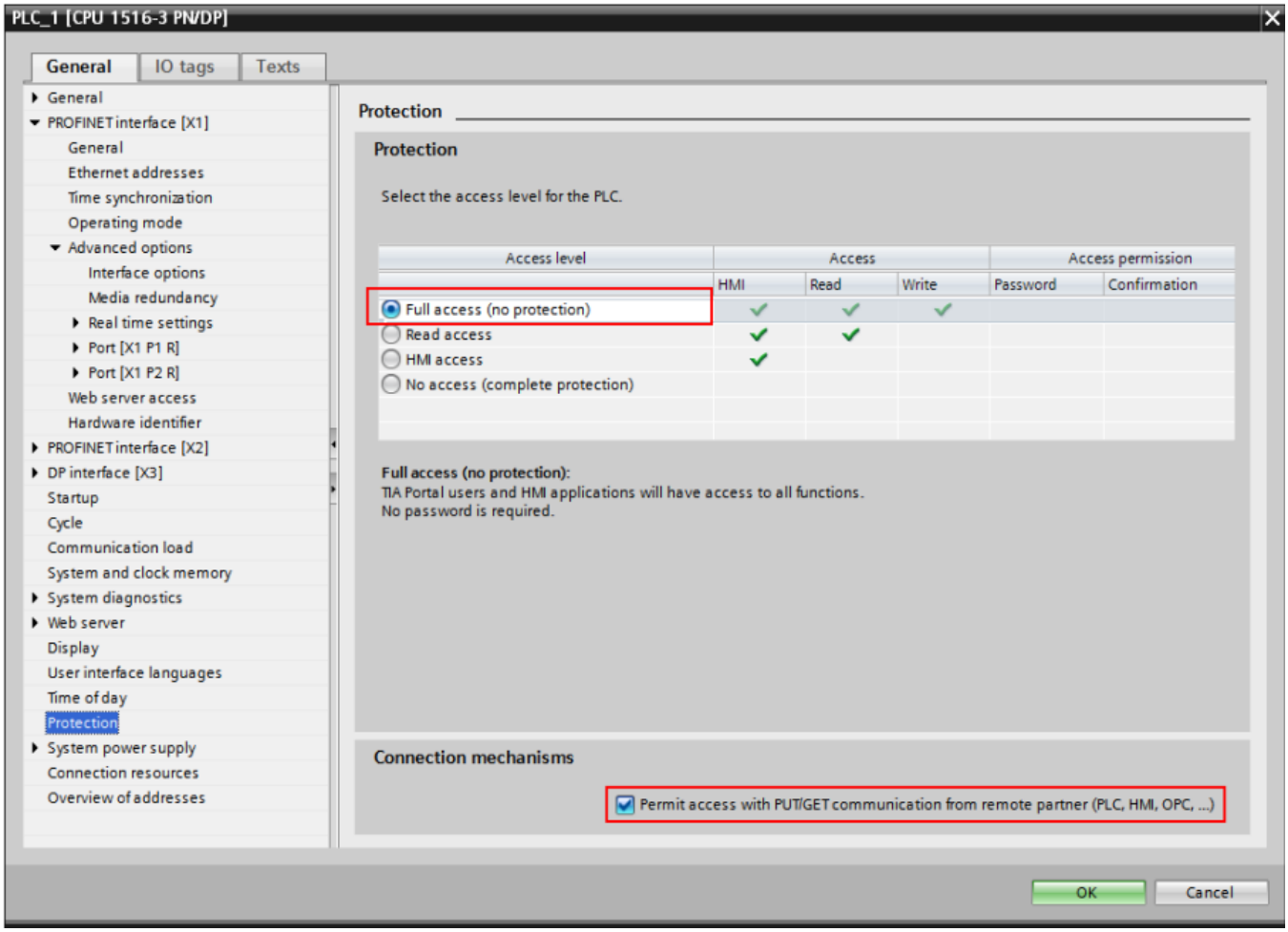
- STRING - standard format of the S7 string, when there are 2 bytes in front of the string itself (maximum and current string length). For example, a 10-character STRING takes up 12 bytes.
- CHARARR - an array of characters, without a 2-byte header. For example, CHARARR with a length of 10 characters takes up 10 bytes.

<address>	Address of variable. Possible types:
	
	• Byte offset (offset within a block, a number 0-65535)
	• Byte offset.bit (only for the X data type, bit number in the range of 0 to 7)
	• Byte offset.String length (only for the STRING data type, string length from 1 to 254 characters)
	• Id.Index[.StringOffset[.StringLength]] - only for object S (system status list):
	  ◦ Id and Index are 16-bit numbers in the range 0-65535 defining ID of specific system status list and index of the item in this list
	  ◦ StringOffset and StringLength are byte offset (0..65535) and length (1..65535) of the substring in answer, which will be parsed as a value of I/O tag.
	Example: address S237.1.10.20 represents status list 237 (0x0111), index 1 (Identification of the module). S7-300 will answer to this request by a 36 byte-long string (bytes 0..35) in which bytes 10..29 (i.e. offset=10, length=20) represent "Order number of the module", e.g. '6GK7 342-5DA02-0XE0 '.
	
	Example of addresses:
	
	• DB10,W35
	• DB8,X10.0
	• DB1,REAL12
	• DB5,STRING5.14
	• DB5,CHARARR5.14
	• T20
	• C7
	• MB11
	• MDINT30
	• QX3.7

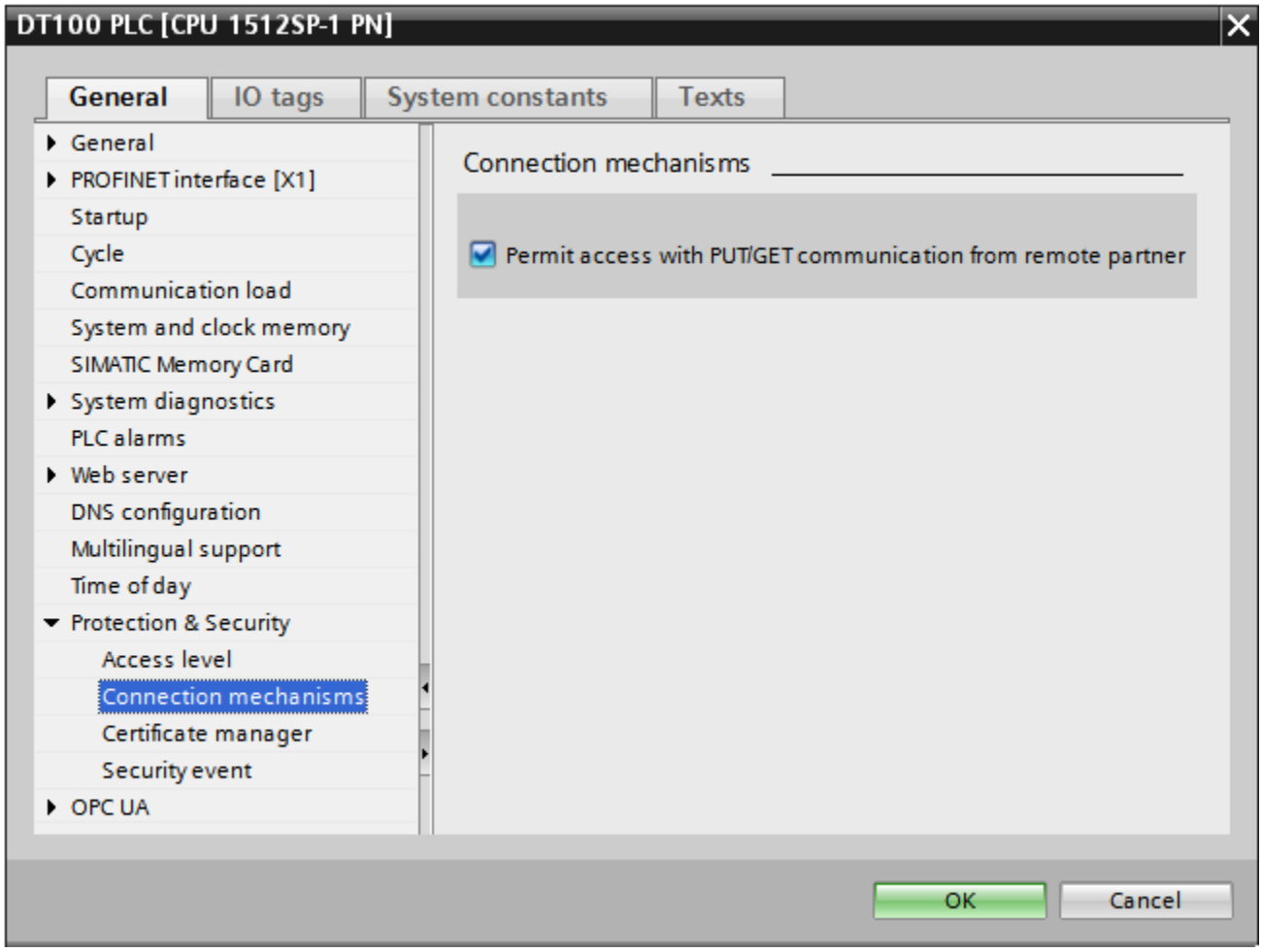
<items>	The number of elements for structured I/O tags with configured Destination column. Every read element (1,2,3 .. *items*) will be written to one item of the destination column. Structured I/O tags are not supported for objects of type T (timers), C (counters), and S (system status lists) nor for data type STRING. **Note:** All "*items*" elements are read at once. If e.g. 100 elements of type D (double word) are configured, it means reading of a block of 400 bytes. If a smaller size of the packet (S7 PDU size) is agreed on during the establishment of connection, reading of this I/O tag will not be performed and the trace file of the line will contain an error message. Agreed S7 PDU size is minimum of size offered by D2000 (parameter S7 PDU Size) and supported size of a specific device. **Note:** the syntax of address when specifying the number of elements is compatible with Siemens S7 OPC server (e.g. S7:[MyPLC]DB120, INT1050, 24), which facilitates a simple transition from OPC communication to Siemens SIMATIC S7 ISO on TCP protocol by configuring a new line, a new station and then changing the parent of I/O tags (e.g. via CSV or XML export and import). Example of addresses: • DB10,W35, 20 a block of 20 words will be read (i.e. 40 bytes) from addresses 35-54 • DB8,X10.0, 100 a block of 100 bits will be read (i.e. 13 bytes) from addresses 10-22

Note on Siemens TIA Portal version 12 and above

There have been reported cases when communication with a device (specifically, Simatic S7-1200) was established, but after sending a read request the device didn't send required data but a packet with ResultCode = 0x8104, that is 33028 decimal.
According to http://stackoverflow.com/questions/23745407/libnodave-error-while-reading-from-siemens-s7-1200-0x8104, the problem is insufficient access rights. The cause is a new security option that was added to TIA Portal 12 and higher, which by default disallows remote access to read/update blocks. Without this option disabled, only Siemens tools have access to the data.
Configuration: in TIA, under the properties for the CPU project, select "Protection"; there is an option for "Permit access with PUT/GET communications from the remote partner" and set also "Access level" according to the following screenshot.
Note: in practice, read/write access has been tested with Simatic S7-1500 even with "Access level" = "HMI access", with "Permit access with PUT/GET communications from remote partner" enabled.

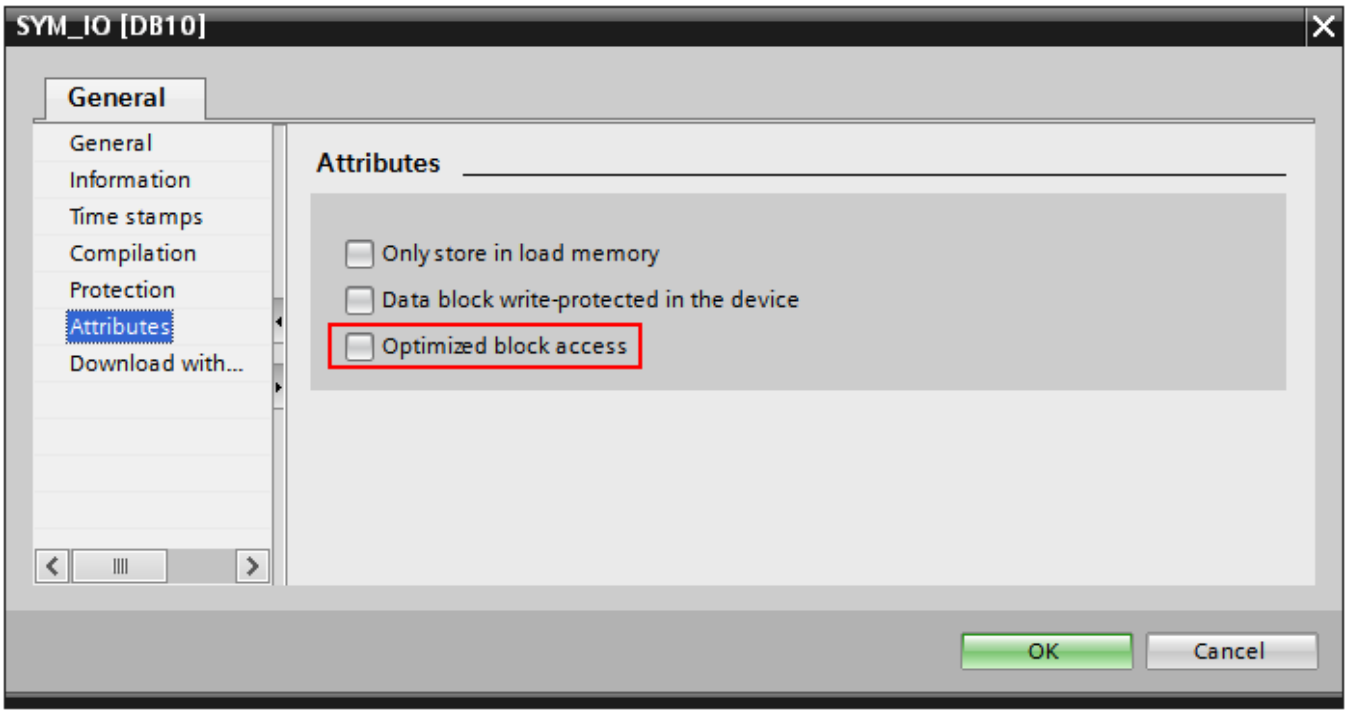


In the case of TIA Portal version 14, the setting "Permit access with PUT/GET communications from the remote partner" is on a dedicated tab "Connection mechanisms" under "Protection & Security":



Note on Siemens S7 1200/1500

For the communication with these devices to work, besides the settings described in the note above, it is necessary to disable "Optimized block access" in the TIA Portal tool. The following screenshot is taken in TIA Portal version 12:



After changing the security settings in TIA Portal, it is necessary to go to the menu Compile "Software (Rebuild all)" and after compiling to upload the project to PLC. A partial rebuild may not be sufficient.

As of STEP 7 V17, the following procedure is advised to get the communication working: use Online & diagnostics to perform a Reset to Factory Settings and mark the box labeled "Delete password for protection of confidential PLC configuration data".

Literature

- RFC 1006, "ISO Transport Service on top of the TCP, Version: 3", May 1987.
- International Standard ISO/IEC 8073:1997, "Information technology - Open Systems Interconnection - Protocol for providing the connection-mode transport service."
- International Standard ISO/IEC 8072:1996, "Information technology - Open Systems Interconnection - Transport service definition."

Blog

You can read blogs about the Siemens SIMATIC S7 ISO on TCP communication protocol:

- Simatic S7-300 and D2000

Changes and modifications

-

Document revisions

- Ver. 1.0 - September 17, 2010 - Document written.
- Ver. 1.1 - July 2, 2020 - Support for CHARARR.
- Ver. 1.2 - July 9, 2020 - Support for BCD and LBCD.
- Ver. 1.3 - August 27, 2020- Support for Siemens Microbox

Related pages:

Communication protocols