Siemens SIMATIC S7 ISO on TCP

Siemens SIMATIC S7 ISO on TCP communication protocol

Supported device types and versions

This protocol supports a data reading/writing from the control PLC machines Siemens SIMATIC, types S7-300 and S7-400 which contain an ethernet interface for the communication S7 ISO over TCP.
Note: A 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 adapter's firmware was version V2.37 (8.august 2011), communication could not be correctly established.
Note: a communication with PLC machine Siemens LOGO was established. A part of memory that is accessible for read/write is the **V area** that is seen as DB1.

Communication line configuration

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

When the communication line is set as **TCP Redundant** you can configure IP address and port of a backup device. If a communication process lost the connection or is unable to connect to device, it will switch periodic between the configured devices. KOM process tries to connect to a primary device at first.

Line protocol parameters

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

The line protocol contains the following parameters:

Parameter	Meaning	Unit / size	Default value
Rack	Siemens Simatic rack number.	0 to 7	0
Slot	Siemens Simatic slot number.	0 to 31	0
Connection Resource (hex)	Connection resource, it inputs as MSB byte to calculation of the value of Remote TSAP at initialization of ISO Connection-request. See description of parameter Use long TSAP.	0x0 to 0xFF	3
Local TSAP (hex)	ISO Local TSAP (Transport Service Local Point). Source TSAP value at initialization of ISO Connection-request. See description of parameter Use long TSAP.	0x0 to 0xFFFF	0x1000
Source Reference	ISO Source Reference. Value of SRC-REF at connection of ISO Connection-request.	0 to 65535	1

Use long TSAP	Enables a long format of local and remote TSAP which is sent during connection setup phase. Short TSAP is 2 bytes long. Short local TSAP has following format: • 1. byte - higher byte of parameter Local TSAP • 2. byte - lower byte of parameter Local TSAP Short remote TSAP has following format: • 1. byte - value of parameter Connection Resource • 2. byte - combination of parameters Rack * 32 + Slot Long local TSAP is 28 bytes long. 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 - value of parameter MPI/Profibus Address • 27. byte - 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
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 adresa sent as a part of Remote TSAP, if parameter Use long TSAP is set to True	0x0 to 0xFFFF	0
ISO TPDU Size Variable Parameter	Maximum required size of ISO TPDU. The parameter value at 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 value if there is a request on more data read from device in shorter time.	1 to 4	1
Cycle Time	Required time of one data reading cycle.	ms	1000 ms
Message Timeout	Maximal wait time on reply from other device.	ms	2500 ms
Inter Message Delay	Delay which is used before sending a data request. When high data transfer rate is required, set 0 ms.	sec.ms	20 ms
Reconnect Delay	Delay before reconnection to other 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. FALSE state is set on the communication line.	sec.ms	20 sec
S7 PDU Size	Maximum PDU in bytes at S7 communication with other device.	240, 480, 960 bytes	480 bytes
Tcp No Delay	Setting *Tcp No Delay* parameter causes low level socket option TCP_NODELAY being set, thus turning off default packet coalesce feature.	-	False
Debug Values	Activates a debug info about the loaded values of I/O tags. Use this parameter only when communication must be debug because it highly uses CPU and slows down the communication.	YES/NO	NO
Debug I/O Binary Packets Info	Activates a debug info about a binary content of packets. Use this parameter only when communication must be debug because it highly uses CPU and slows down the communication.	YES/NO	NO
Debug Requests Info	Activates a basic debug info about requested data.	YES/NO	YES
Debug Answers Info	Activates a 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 station.
- Time parameter setting is ignored. See the line parameter Cycle Time.
- A time synchronization of 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 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:

<table>
<tr><td><b>;</b></td><td>Optional parameter. It disables the I/O tag from communication, stops I/O tag address check when it is saved, and can be useful when the communication with device is activated or debugged.</td></tr>
<tr><td><b>S7:[connectionname]</b></td><td>Optional parameter. It does not contains any useful information but it is supported only because of backward compatibility with Siemens SimaticNET OPC server.</td></tr>
<tr><td><b>DB</b></td><td>Data block. S7 variable identifier from "Data block".</td></tr>
<tr><td><b>DI</b></td><td>Instance data block. S7 variable identifier from " Instance data block".</td></tr>
<tr><td><b><no></b></td><td>Number of "data block" or "instance data block".</td></tr>
<tr><td><b><object></b></td><td>Specification of block or area in S7 PLC.
Possible values:
<table>
<tr><td><b>I</b></td><td>Input</td></tr>
<tr><td><b>Q</b></td><td>Output</td></tr>
<tr><td><b>PI</b></td><td>Peripheral input</td></tr>
<tr><td><b>PQ</b></td><td>Peripheral output</td></tr>
<tr><td><b>M</b></td><td>Memory bit</td></tr>
<tr><td><b>C</b></td><td>Counters (BCD coded integer numbers <0-999>)</td></tr>
<tr><td><b>T</b></td><td>Timers (BCD coded time values from intervals <0.00-9.99>, <00.0-99.9>, <000-999>, <0000-9.9990>)</td></tr>
<tr><td><b>S</b></td><td>SZL (System-ZustandsListen - system status lists) - lists with diagnostic information which 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)
<b>Note:</b> I/O tag S must be of TxtI type.</td></tr>
</table>
</td></tr>
</table>

<type>

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 (8 bits unsigned).
W	Word (16 bits unsigned).
D	Double word (32 bits unsigned).
CHAR	Character (8 bits signed).
INT	Integer (16 bits signed).
DINT	Double integer (32 bits signed).
REAL	Floating point number (32 bits according to IEEE754 standard).
LREAL	Long floating point number (64 bits according to IEEE754 standard).
STRING	String. Specify maximal length of string.
DT	Date and Time, 8 bytes in BCD format.
TIME	Time (32 bits signed) in ms.
TOD	Time of day (32 bits unsigned) in ms.

<address>

Address of variable. Possible types:

- Byte offset
- Byte offset.bit (only for X data type, bit number in the range of 0 to 7)
- Byte offset.String length (only for 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 range 0-65535 defining ID of specific system status list and index of item in this list
  - StringOffset and StringLength are byte offset (0..65535) and length (1..65535) of 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
- T20
- C7
- MB11
- MDINT30

<items>

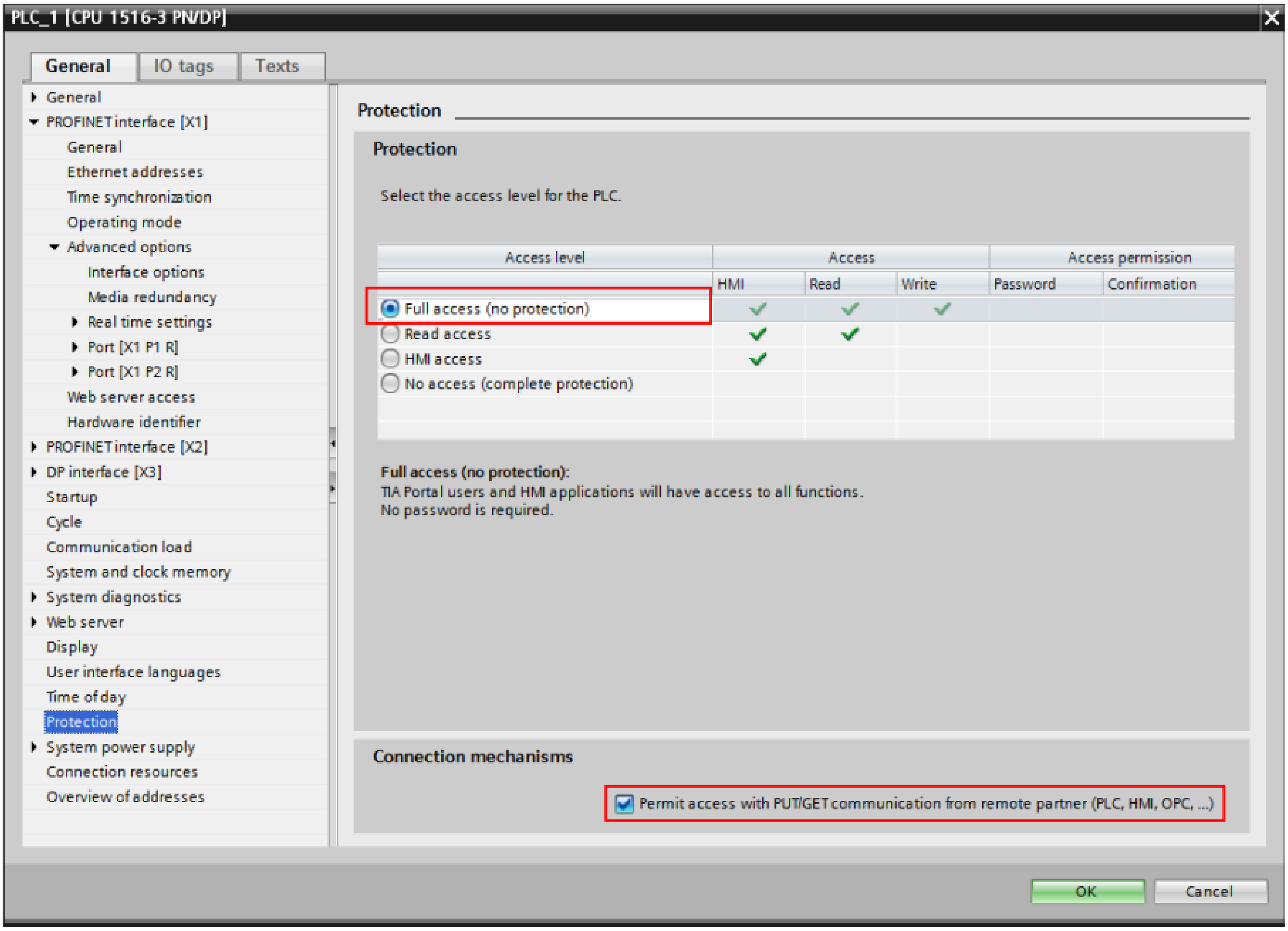
number of elements for structured I/O tags with configured Destination column. Every read element (1,2,3 .. *items*) will be written to one item of destination column.
Structured I/O tags are not supported for objects of type T (timers), C (counters) and S (system status lists) nor for data type STRING.
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 packet (S7 PDU size) is agreed on during establishment of connection, reading of this I/O tag will not be performed and trace file of 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 specific device.
Note: syntax of address when specifying number of elements is compatible with Siemens S7 OPC server (e.g. S7:[MyPLC]DB120,INT1050, 24), which facilitates simple transition from OPC communication to Siemens SIMATIC S7 ISO on TCP protokol by configuring a new line, a new station and then changing 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 a 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 that 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 remote partner" and set also "Access level" according to the following screenshot.



Protection

Protection

Select the access level for the PLC.

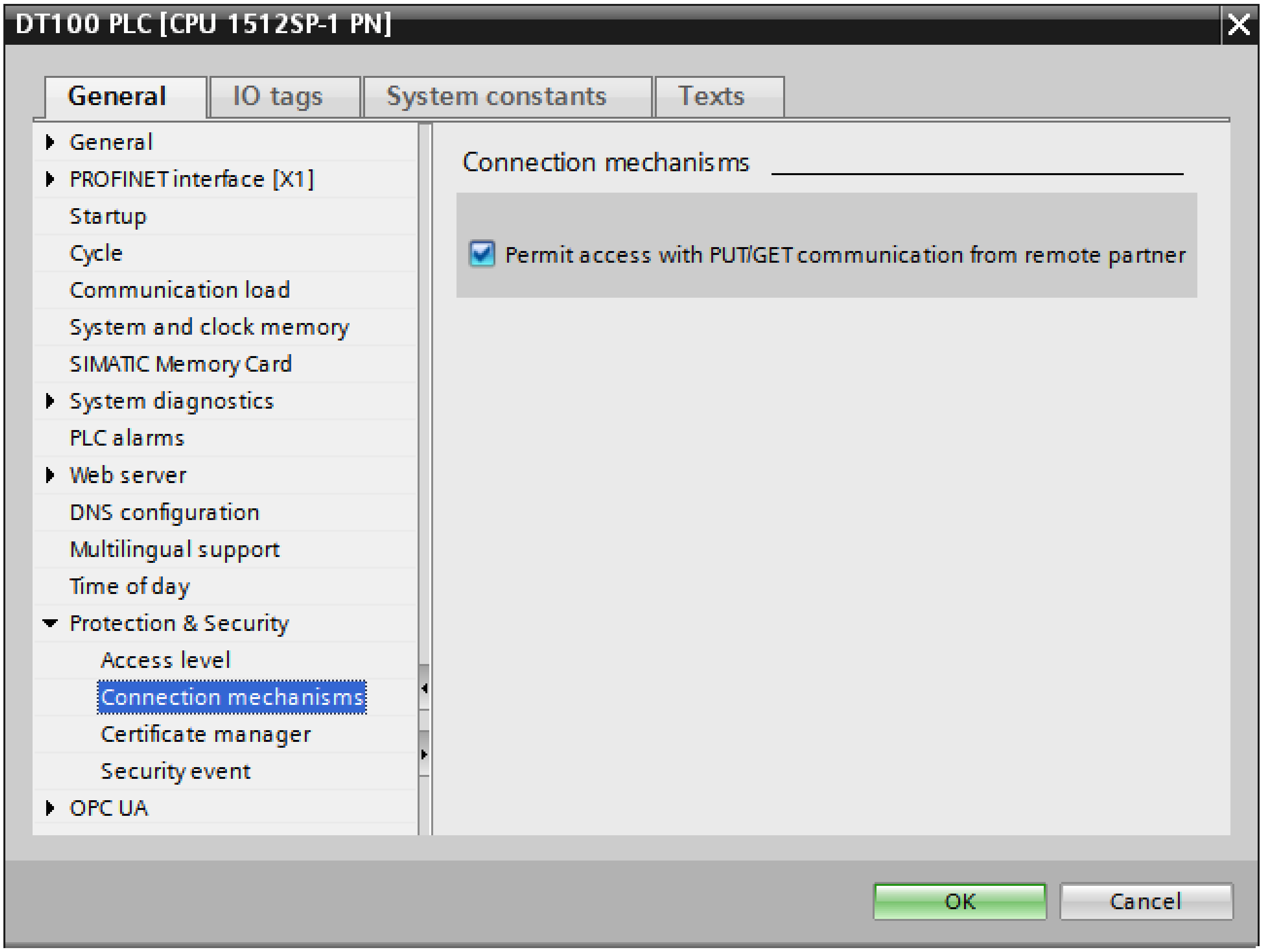
Access level	Access			Access permission	
	HMI	Read	Write	Password	Confirmation
● Full access (no protection)	✓	✓	✓		
○ Read access	✓	✓			
○ HMI access	✓				
○ No access (complete protection)					

Full access (no protection):
TIA Portal users and HMI applications will have access to all functions.
No password is required.

Connection mechanisms

☑ Permit access with PUT/GET communication from remote partner (PLC, HMI, OPC, ...)

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



DT100 PLC [CPU 1512SP-1 PN]

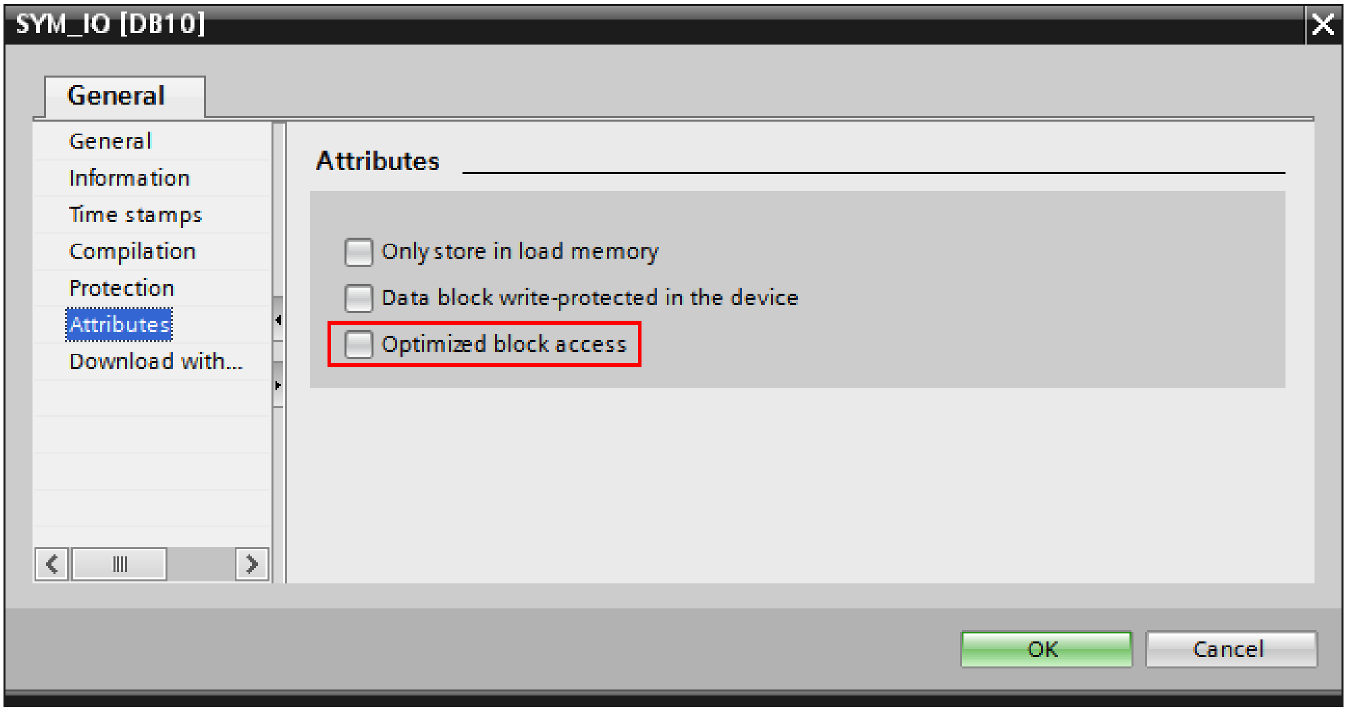
Connection mechanisms

☑ Permit access with PUT/GET communication from remote partner

Siemens SIMATIC S7 ISO on TCP

Note on Siemens S7 1200/1500

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



Attributes

□ Only store in load memory

□ Data block write-protected in the device

□ Optimized block access

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."

Changes and modifications

-

Document revisions

- Ver. 1.0 - September 17, 2010 - Document written.

Related pages:

Communication protocols