Siemens SIMATIC S7 ISO on TCP

Protokol Siemens SIMATIC S7 ISO on TCP

Podporované typy a verzie zariadení

Protokol podporuje ítanie dát/zápis údajov z riadiacich PLC automatov Siemens SIMATIC:

- rady S7-300 a S7-400, vybavenými ethernetovými rozhraniami pre komunikáciu S7 ISO over TCP.
- rady S7-1200, S7-1500
- rady Siemens LOGO
- rady Siemens Microbox

Pozn: bola overená komunikácia cez Profinet/Profibus prevodník ACCON-NetLink-PRO compact od firmy DELTALOGIC. Komunikácia s viacerými PLC rady S7-300 na Profibus zbernici fungovala po aktualizácii firmware prevodníka na verziu V2.54 (31. marec 2015) s BIOS-om prevodníka na verzii V2.39 (7. jún 2011). Ke bol firmware prevodníka na verzii V2.37 (8.august 2011), komunikácia nebola funkná.
Pozn: bola vyskúšaná komunikácia s PLC automatom Siemens LOGO. as pamäte, ktorá je prístupná na ítanie/zápis je tzv. **V area**, viditená ako DB1.
Pozn: protokol má "big endian" reprezentáciu dát.

Konfigurácia komunikanej linky

- Kategórie komunikanej linky: TCP/IP-TCP, TCP Redundant.
- IP adresa (adresy) poda sieovej konfigurácie konkrétneho zariadenia Siemens SIMATIC.
- íslo portu je štandardne 102 (poda špecifikácie RFC 1006).
- íslo linky je nepoužité, nastavte hodnotu 1.

V prípade nastavenia kategórie linky **TCP Redundant** je možné nakonfigurova IP adresu a port záložného zariadenia. Komunikaný proces pri strate spojenia alebo nemožnosti nadviazania spojenia so zariadením cyklicky prepína medzi nakonfigurovanými zariadeniami. Najprv sa KOM proces pokúša nadviaza spojenie s primárnym zariadením.
Pozn: je možné nakonfigurova aj viacero IP adries primárneho/záložného zariadenia (oddelených iarkou alebo bodkoiarkou).

Pozn: ak sú všetky stanice v stave StOFF (alebo v simulácii), TCP spojenie bude zatvorené. Takto je možné riadi TCP komunikáciu zo skriptu pomocou tell príkazu STSTAT.

Parametre protokolu linky

Dialóg konfigurácia linky - záložka **Parametre protokolu**.
Ovplyvujú niektoré volitené parametre protokolu. Môžu by zadané nasledovné parametre protokolu linky:

Tab. . 1

Parameter	Popis	Jednotka / rozmer	Náhradná hodnota
Rack	íslo Siemens Simatic rack number. Rack 0 je najastejšie používaný. Pozn: pri použití prevodníka ACCON-NetLink-PRO compact je treba nastavi parametre Rack/Slot tak, aby MPI adresa S7, s ktorým sa komunikuje, bola rovná 32 * Rack + Slot. Pre každé S7 je teda nutné vytvori vlastnú linku so špecifickými hodnotami Rack/Slot. Je nutné aj nastavi "RFC Routing over CPs with TSAP" na hodnotu ON vo web rozhraní prevodníka.	0 až 7	0
Slot	íslo Siemens Simatic slot number. Slot 2 je najastejšie používaný.	0 až 31	0
S7 Subnet ID-part 1 (hex)	S7 subnet adresa posielaná ako súas Remote TSAP, ak je nastavený parameter Use long TSAP na hodnotu True	0x0 až 0xFFFF	0
S7 Subnet ID-part 2 (hex)	S7 subnet adresa posielaná ako súas Remote TSAP, ak je nastavený parameter Use long TSAP na hodnotu True	0x0 až 0xFFFF	0

Use Secondary	Parameter umožuje použitie redundantných PLC, ktoré sa môžu líši v nastavení niektorých parametrov (Rack, Slot, S7 Subnet ID). Ak je jeho hodnota True, pri pripájaní sa k PLC pomocou zadaných IP adries sú striedavo použité primárne a sekundárne parametre.	-	False
Connection Resource (hex)	Connection resource, vstupuje ako MSB byte do výpotu hodnoty parametra Remote TSAP pri inicializácii ISO spojenia Connection-request. Vi popis parametra Use long TSAP. **Pozn:** v konkrétnom prípade, ke dva systémy (jeden z nich D2000) potrebovali komunikova s S7-300, museli ma každé odlišný *Connection resource*, v opanom prípade po poslaní úvodnej sekvencie D2000 KOM procesom došlo k rozpadu spojenia: /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/ Po zmene *Connection resource* z 3 na 2 zaala komunikácia fungova. **Pozn**: poda Siemens dokumentácie môže by *Connection resource:* • *0x01 - PG connection* (urené pre programovanie) • *0x02 - OP connection* (urené pre operátorský panel) • *0x03 - Other* (iný úel, použitené pre viacero spojení) • *0x10..0xDF - Connections with static or dynamic connection process* (iný úel, každý použitený pre jedno nakonfigurované spojenie) • *0xFD - S7 basic communication* (typicky spojenia z CPU do iného modulu v rámci podsiete)	0x0 až 0xFF	3
Local TSAP (hex)	ISO Local TSAP (Transport Service Local Point). Hodnota Source TSAP parametra pri inicializácii ISO spojenia Connection-request. Vi popis parametra Use long TSAP.	0x0 až 0xFFFF	0x1000
Source Reference	ISO Source Reference. Hodnota SRC-REF parametra pri inicializácii ISO spojenia Connection-request.	0 až 65535	1
Use long TSAP	Zapnutie dlhého formátu pri posielaní lokálneho a remote TSAP vo fáze nadväzovania spojenia. Krátky TSAP má džku 2 bajty. Krátky lokálny TSAP má formát: • 1. bajt - vyšší bajt parametra Local TSAP • 2. bajt - nižší bajt parametra Local TSAP Krátky remote TSAP má formát: • 1. bajt - hodnota parametra Connection Resource • 2. bajt - kombinácia parametrov Rack * 32 + Slot Dlhý lokálny TSAP má džku 28 bajtov. Posledné 2 bajty sú vyšší a nižší bajt parametra Local TSAP Dlhý remote TSAP má džku 28 bajtov a obsahuje • 5. bajt - vyšší bajt parametra S7 subnet ID-part 1 • 6. bajt - nižší bajt parametra S7 subnet ID-part 1 • 9. bajt - vyšší bajt parametra S7 subnet ID-part 2 • 10. bajt - nižší bajt parametra S7 subnet ID-part 2 • 11. bajt - hodnota parametra MPI/Profibus Address • 27. bajt - hodnota parametra Connection Resource • 28. bajt - kombinácia parametrov Rack * 32 + Slot	-	False
MPI/Profibus Address	MPI/Profibus adresa posielaná ako súas Remote TSAP, ak je nastavený parameter Use long TSAP na hodnotu True	0 až 126	1
ISO TPDU Size Variable Parameter	Maximálna požadovaná vekos ISO TPDU. Hodnota parametra pri inicializácii ISO spojenia Connection-request.	8192, 4096, 2048, 1024, 512, 256 alebo 128 bytov	1024 bytov
Nr. of Parallel Network Threads	Maximálny poet paralelných komunikaných threadov. V prípade požiadavky na vyšší poet údajov ítaných zo zariadenia za kratší as, zvýšte hodnotu parametra.	1 až 4	1
Cycle Time	Požadovaná džka jedného cyklu ítania údajov. V podstate perióda ítania údajov zo zariadenia, keže asové parametre na stanici sa neuplatujú.	ms	1000 ms
Message Timeout	Maximálny as akania na dátovú odpove od partnera.	ms	2500 ms
Inter Message Delay	Oneskorenie vkladané pred odoslaním každej žiadosti o dáta. V prípade požiadavky na vysoký prenosový výkon nastavte 0 ms.	sec.ms	20 ms
Reconnect Delay	Oneskorenie pred pokusom o spojenie s partnerom po rozpade spojenia alebo inej komunikanej chybe.	sec.ms	2 sec

Connection Error Timeout	Po uplynutí tejto doby a v prípade komunikanej chyby na všetkých komunikaných threadoch, je na staniciach nastavený stav komunikanej chyby a na linke stav FALSE.	sec.ms	20 sec
S7 PDU Size	Maximálne PDU v bytoch pri S7 komunikácii s partnerom.	240, 480, 960 bytes	480 bytes
Tcp No Delay	Nastavenie "Tcp No Delay"=True parametra spôsobí nastavenie nízkoúrovového parametra socketov TCP_NODELAY, ím sa vypne prednastavené spájanie paketov.	-	False
Debug Values	Zapína ladiace informácie o naítaných hodnotách meraných bodov. Odporúame zapnú iba v prípade nutnosti ladenia komunikácie, pretože výrazne zvyšuje záaž CPU a spomauje komunikáciu.	YES/NO	NO
Debug I/O Binary Packets Info	Zapína ladiace informácie o binárnom obsahu komunikaných paketov. Odporúame zapnú iba v prípade nutnosti ladenia komunikácie, pretože výrazne zvyšuje záaž CPU a spomauje komunikáciu.	YES/NO	NO
Debug Requests Info	Zapína základné ladiace informácie o požadovaných dátach.	YES/NO	YES
Debug Answers Info	Zapína základné ladiace informácie o získaných paketoch.	YES/NO	YES

Konfigurácia komunikanej stanice

- Komunikaný protokol: **Siemens SIMATIC S7 ISO over TCP**.
- Nezadáva sa žiadna adresa stanice ani parametre protokolu na stanici.
- Nastavenie asových parametrov stanice sa ignoruje, bližšie informácie vi parameter protokolu linky Cycle Time.
- asová synchronizácia zariadenia nie je možná.

Konfigurácia meraných bodov

Možné typy hodnôt bodov: **Ai, Ao, Ci, Co, Di, Dout, TiA, ToA, TiR, ToR, Txtl**.

Adresa meraného bodu je kompatibilná so Siemens SimaticNET OPC serverom (s výnimkou typu CHARARR).

Adresa meraného bodu je znakový reazec poda pravidiel:

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

resp. pre štruktúrované merané body s nakonfigurovaným cieovým stpcom

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

Kde:

;	Je volitený parameter, ktorý slúži na vyradenie meraného bodu z komunikácie. Taktiež sa nekontroluje správnos adresy meraného bodu pri jeho ukladaní. Môže by nápomocný pri fáze vývoja alebo ladenia komunikácie so zariadením. Pozn: aj meraný bod s adresou, ktorá sa zaína *%IGNORE*, bude ignorovaný.
S7:[connectionname]	Je nepovinný parameter, ktorý neobsahuje žiadnu potrebnú informáciu a je podporovaný iba kvôli spätnej kompatibilite so Siemens SimaticNET OPC serverom.
DB	Data block. Identifikátor S7 premennej z "Data block".
DI	Instance data block. Identifikátor S7 premennej z " Instance data block".
<no>	íslo "data block" alebo "instance data block".

<object>

Špecifikácia bloku alebo oblasti v S7 PLC.
Možné sú hodnoty:

Skratka	Popis (Nemecký názov)
I, E	**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 kódované celoíselné hodnoty z intervalu <0-999>
T	**T**imer (**T**imer, T) - BCD kódované asovae z intervalov <0.00-9.99>, <00.0-99.9>, <000-999>, <0000-9.9990>
S	System Status Lists (**S**ystem-**Z**ustands**L**isten, SZL) - zoznamy s diagnostickými informáciami, ktoré sú k dispozícii na CPU rodiny S7-300 a S7-400. Obsah informácií sa pre rôzne triedy PLC líši a detaily sú popísané v manuáloch (napr. System Software for S7-300/400 System and Standard Functions, Volume 1/2) **Pozn:** meraný bod S musí by typu TxtI.

<type>

Dátový typ S7. Pre objekty T, C a S nie je špecifikovaný.

Identifikátor <type>	Popis
X	Bit (boolean). Treba špecifikova číslo bitu 0 až 7 - napr. DB9,X8.3
B BYTE	Byte (8 bitov neznamiekovo).
W WORD	Word (16 bitov neznamienkovo).
D DWORD	Double word (32 bitov neznamienkovo).
CHAR	Character (8 bitov znamienkovo).
INT	Integer (16 bitov znamienkovo).
DINT	Double integer (32 bitov znamienkovo).
BCD	BCD-kódované 2-bajtové číslo (0-9 999)
LBCD	BCD-kódované 4-bajtové číslo (0-99 999 999)
REAL	Floating point number (32 bitov poda IEEE754).
LREAL	Long floating point number (64 bitov poda IEEE754).
STRING	String. Treba špecifikova maximálnu dĺžku stringu.
CHARARR	Pole CHAR-ov interpretované ako String. Treba špecifikova dĺžku poa.
DATE	Date, 2 bajty (poet dní od 1.1.1990)
DT	Date and Time, 8 bytov v BCD formáte, s presnosou na milisekundy
DTL	Date and Time, 12 bytov v BCD formáte, s presnosou na nanosekundy Pozn: D2000 pracuje iba s milisekundovou presnosou
TIME	Time (32 bitov znamienkovo) v milisekundách. Pozn: ak je meraný bod typu TiR, treba zabezpei konverziu nakonfigurovaním lineárneho prevodu (A=0.001, B=0) na záložke Prevod
S5TIME	Dvojbajtový as - formát Simatic S5 (0 - 9990 sekúnd s variabilnou presnosou 0.01 - 10 sekúnd). Podporené sú merané body typu Ai/Ao, Ci/Co, TiR/ToR. Poznámka: alternatívou k tomuto dátovému typu je použitie typu "W" a nastavenie "Simatic S5Time" prevodu.
TOD	Time of day (32 bitov neznamienkovo) v milisekundách.

Pozn: typ CHARARR je D2000 rozšírenie, ktoré umožuje íta/zapisova pole CHAR-ov ako reazec. Tento typ nie je kompatibilný so Siemens SimaticNET OPC serverom.
Rozdiel medzi CHARARR a STRING je nasledovný:

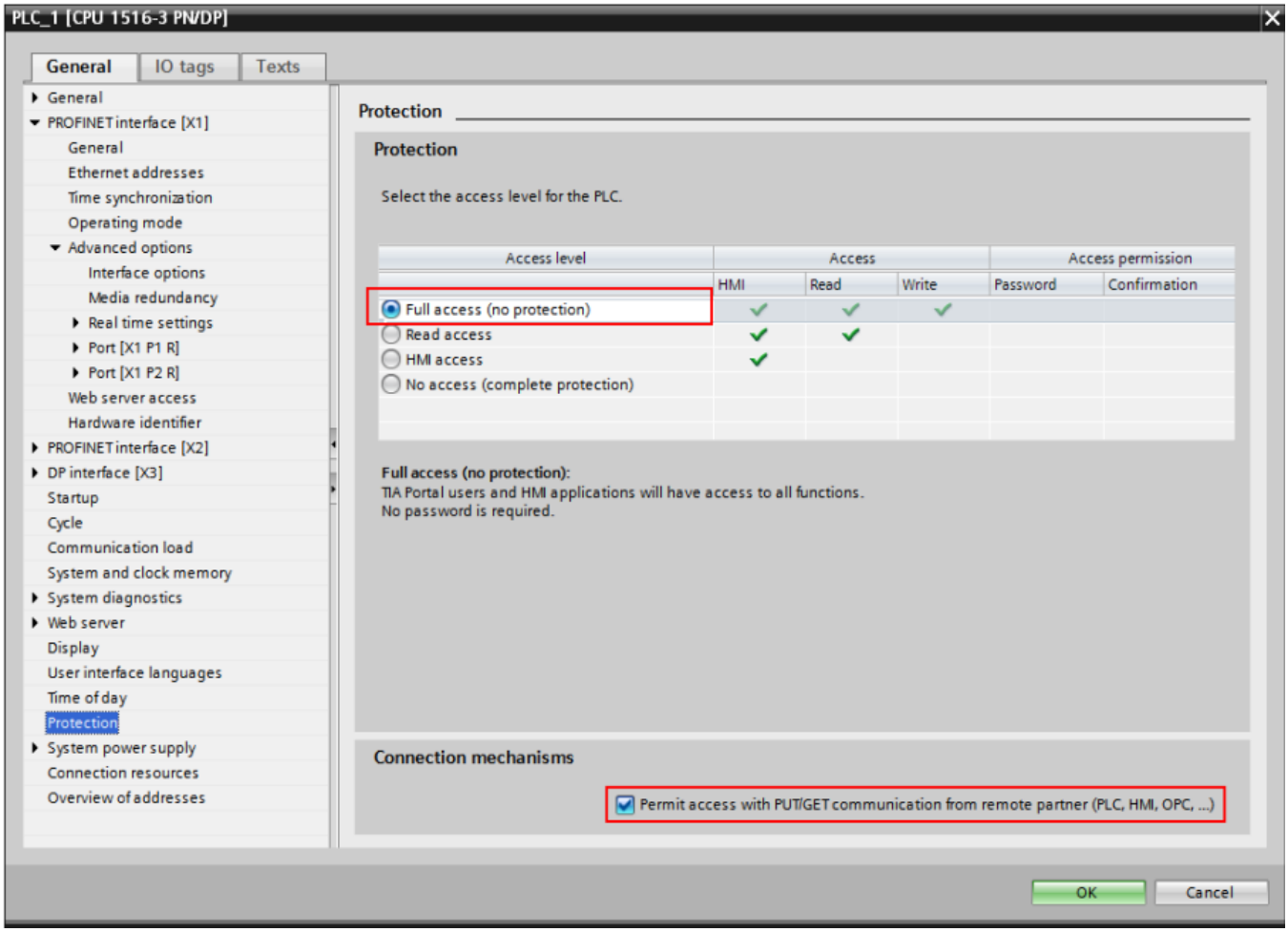
- STRING - štandardný formát reazca S7, ke pred samotným reazcom sa nachádzajú ešte 2 bajty (maximálna a aktuálna dĺžka reazca). Tj. STRING s dĺžkou 10 znakov zaberá 12 bajtov.
- CHARARR - pole znakov bez 2-bajtovej hlaviky. Tj. CHARARR s dĺžkou 10 znakov zaberá 10 bajtov.

<address>	Adresa premennej. Možné sú varianty:
	
	• Byte offset (offset v rámci bloku, íslo 0-65535)
	• Byte offset.bit (len pre dátový typ X, íslo bitu v rozsahu 0 až 7)
	• Byte offset.String length (len pre dátový typ STRING, džka stringu 1 až 254 znakov)
	• Id.Index[.StringOffset[.StringLength]] - len pre objekt S (system status list), priom:
	  ◦ Id a Index sú 16 bitové ísla v rozsahu 0-65535 udávajúce ID konkrétneho zoznamu a index položky v om
	  ◦ StringOffset a StringLength sú bajtový offset (0..65535) a džka (1..65535) podreazca v odpovedi, ktorý bude priradený do meraného bodu.
	Príklad: adresa S237.1.10.20 zodpovedá stavovém zoznamu 237 (0x0111), index 1 (Identification of the module). S7-300 ako odpove na dotaz vráti odpove s džkou 36 bajtov (bajty 0..35), priom bajty 10..29 (tj. Offset=10, džka=20) udávajú "Order number of the module", napr. '6GK7 342-5DA02-0XE0 '.
	
	Príklady adries:
	
	• DB10,W35
	• DB8,X10.0
	• DB1,REAL12
	• DB5,STRING5.14
	• DB5,CHARARR5.14
	• T20
	• C7
	• MB11
	• MDINT30
	• QX3.7

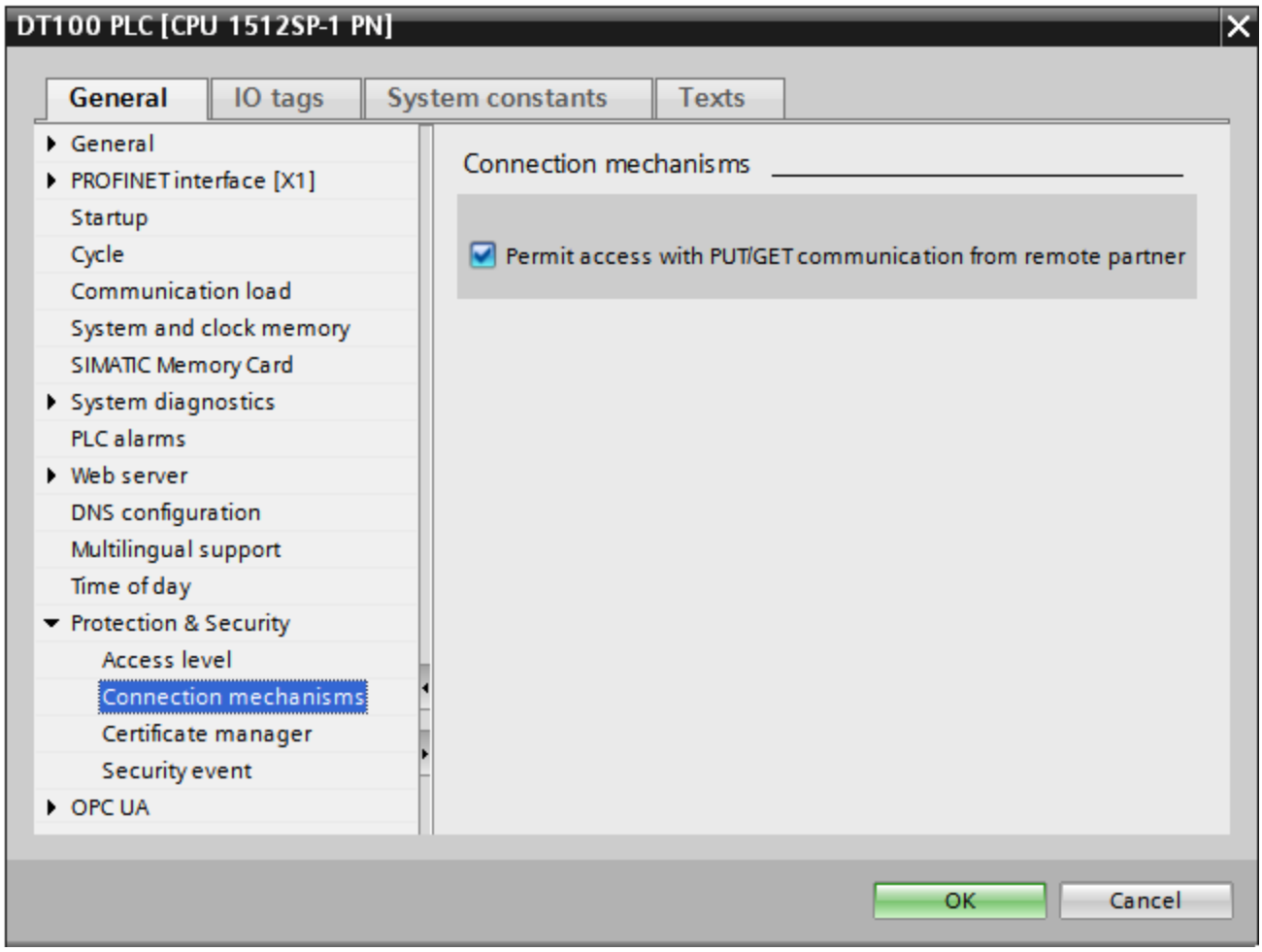
<items>	Poet elementov pre štruktúrované merané body s nakonfigurovaným cieovým stpcom. Každý naítaný element (1,2,3 .. *items*) bude zapísaný do jednej položky cieového stpca. Štruktúrované merané body nie sú podporené pre objekty typu T (timers), C (counters) a S (system status lists) ani pre dátový typ STRING. **Pozn:** Celý poet *item* elementov je vyítavaný naraz. Pokia je nakonfigurovaných napr. 100 elementov typu D (double word), jedná sa o ítanie bloku 400 bajtov. Pokia pri nadviazaní komunikácie je dohodnutá menšia vekos paketu (S7 PDU size), ítanie takéhoto meraného bodu sa neuskutoní a v logu linky bude o tom chybová hláška. Dohodnutá vekos S7 PDU size je minimom možností D2000 (parameter S7 PDU Size) a možnosti konkrétneho zariadenia. **Pozn:** syntax adresy pri zadaní potu elementov je kompatibilná so Siemens S7 OPC serverom (napr. S7:[MyPLC]DB120,INT1050, 24), o umožuje jednoduchý prechod z OPC komunikácie na protokol Siemens SIMATIC S7 ISO on TCP nakonfigurovaním novej linky, stanice a zmenou rodia meraných bodov (napr. CSV alebo XML exportom a importom). Príklady adries: • DB10,W35, 20 íta sa blok 20 wordov (t.j. 40 bajtov) z adries 35-54 • DB8,X10.0, 100 íta sa blok 100 bitov (t.j. 13 bajtov) z adries 10-22

Poznámka k Siemens TIA Portal verzie 12 a vyšším

V praxi sa vyskytli prípady, ke sa komunikácia so zariadením (išlo o Simatic S7-1200) síce rozbehla, ale po poslaní požiadavky na ítanie dát zariadenie ako odpove neposlalo dáta, ale paket s ResultCode = 0x8104 tj. decimálne 33028.
Poda http://stackoverflow.com/questions/23745407/libnodave-error-while-reading-from-siemens-s7-1200-0x8104 je problém v nedostatonýchprístupových právach. Príinou je vyššia úrove zabezpeenia v TIA Portal verzii 12 a vyšších, ktorá štandardne zakazuje prístup k read/update blokom. Bez explicitného povolenia iba Siemens nástroje majú prístup k dátam.
Konfigurácia: V TIA, pod vlastnosami CPU projektu je treba ís na "Protection" a tam zaškrtnú "Permit access with PUT/GET communications from remote partner" a nastavi "Access level" poda obrázku.
Pozn: v praxi bolo odskúšané s Simatic S7-1500 ítanie/zápis aj pri nastavení "Access level" = "HMI access", so zapnutým "Permit access with PUT/GET communications from remote partner".

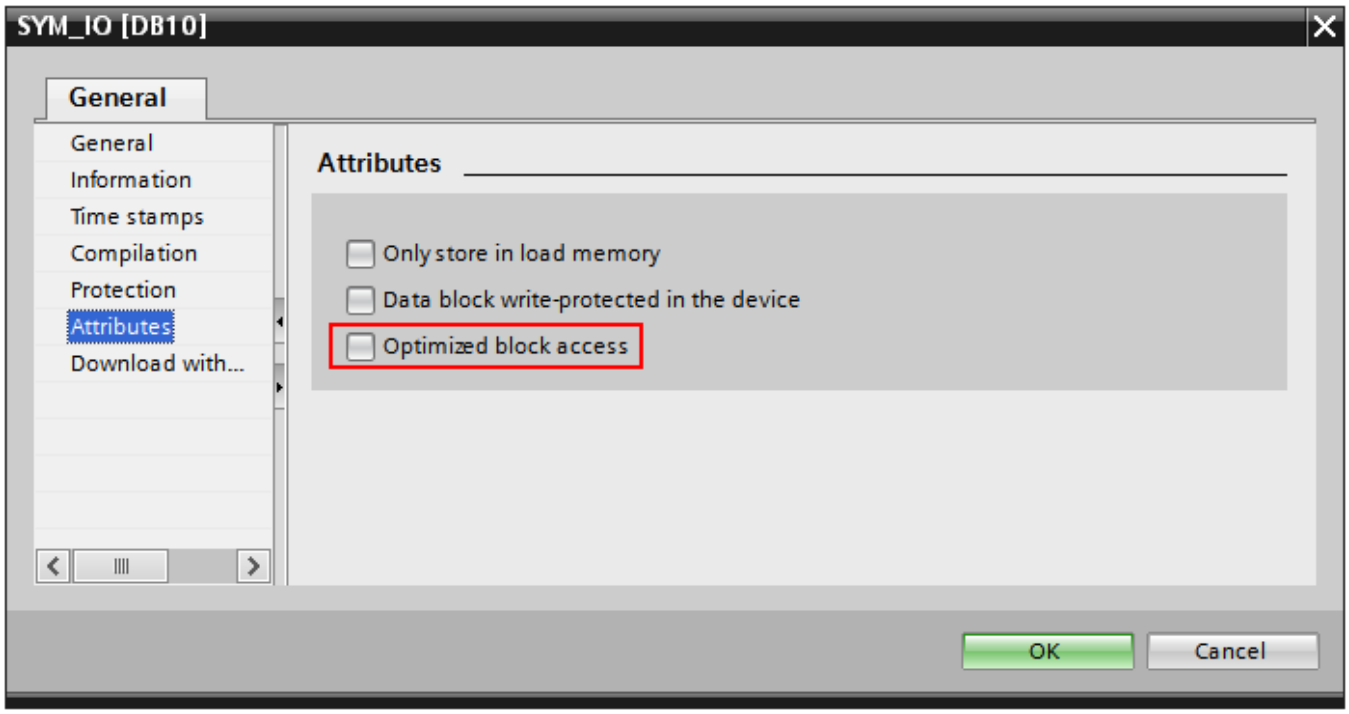


V prípade TIA Portal verzie 14 je nastavenie "Permit access with PUT/GET communications from remote partner" na samostatnej záložke "Connection mechanisms" pod "Protection & Security":



Poznámka k Siemens S7 1200/1500

Aby fungovala komunikácia s týmito zariadeniami, okrem nastavení popísaných v poznámke vyššie, v nástroji TIA Portal je nutné vypnú "Optimized block access". Nasledujúci obrázok je z TIA Portal verzie 12:



Po zmene bezpenostných nastavení v TIA Portal je nutné v menu vybra Compile "Software (Rebuild all)" a po skompilovaní projekt nahra do PLC. iastoný rebuild nemusí postaova.

Od verzie STEP 7 V17 na sfunknenie komunikácie môže by potrebný nasledujúci postup: použite "Online & diagnostics" na vykonanie *Reset to Factory Settings* a oznate políko oznaené "*Delete password for protection of confidential PLC configuration data*".

Literatúra

- 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

O protokole Siemens SIMATIC S7 ISO on TCP si môžete preíta aj blogy

- Simatic S7-300 and D2000

Zmeny a úpravy

-

Revízie dokumentu

- Ver. 1.0 - 17. september 2010 - Vytvorenie dokumentu.
- Ver. 1.1 - 2. júl 2020 - Podpora CHARARR.
- Ver. 1.2 - 9. júl 2020 - Podpora BCD a LBCD.
- Ver. 1.3 - 27.august 2020- Podpora Siemens Microbox

Súvisiace stránky:

Komunikané protokoly