

Siemens SIMATIC S7 ISO on TCP

Protokol Siemens SIMATIC S7 ISO on TCP

[Podporované typy a verzie zariadení](#)
[Konfigurácia komunikačnej linky](#)
[Parametre protokolu linky](#)
[Konfigurácia komunikačnej stanice](#)
[Konfigurácia meraných bodov](#)
[Poznámka k Siemens TIA Portal verzii 12 a vyšším](#)
[Poznámka k Siemens S7 1200/1500](#)
[Literatúra](#)
[Zmeny a úpravy](#)
[Revízie dokumentu](#)

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

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 verzii 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 funkčná.

Pozn: bola vyskúšaná komunikácia s PLC automatom Siemens LOGO. as pamäte, ktorá je prístupná na ítanie/zápis je tzv. **V area**, viditená ako DB1.

Konfigurácia komunikačnej linky

- Kategórie komunikačnej 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 nepoužitá, nastavte hodnotu 1.

V prípade nastavenia kategórie linky **TCP Redundant** je možné nakonfigurova IP adresu a port záložného zariadenia. Komunikovaný 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 bodkoarkou).

Parametre protokolu linky

Dialóg [konfigurácia linky](#) - záložka **Parametre protokolu**.

Ovplyvujú niektoré volítené parametre protokolu. Môžu by zadané nasledovné parametre protokolu linky:

Tab. . 1

Parameter	Popis	Jednotka / rozmer	Náhradná hodnota
Rack	ísto Siemens Simatic rack number.	0 až 7	0
Slot	ísto Siemens Simatic slot number.	0 až 31	0
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 .	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 dĺžku 2 bajty. Krátky lokálny TSAP má formát: <ul style="list-style-type: none"> 1. bajt - vyšší bajt parametra Local TSAP 2. bajt - nižší bajt parametra Local TSAP Krátky remote TSAP má formát: <ul style="list-style-type: none"> 1. bajt - hodnota parametra Connection Resource 2. bajt - kombinácia parametrov $Rack * 32 + Slot$ Dlhý lokálny TSAP má dĺžku 28 bajtov. Posledné 2 bajty sú vyšší a nižší bajt parametra Local TSAP Dlhý remote TSAP má dĺžku 28 bajtov a obsahuje <ul style="list-style-type: none"> 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 posiadaná ako súas Remote TSAP, ak je nastavený parameter Use long TSAP na hodnotu True	0 až 126	1
S7 Subnet ID-part 1 (hex)	S7 subnet adresa posiadaná 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 posiadaná ako súas Remote TSAP, ak je nastavený parameter Use long TSAP na hodnotu True	0x0 až 0xFFFF	0
ISO TPDU Size Variable Parameter	Maximálna požadovaná veľkosť ISO TPDU. Hodnota parametra pri inicializácii ISO spojenia Connection-request.	8192, 4096, 2048, 1024, 512, 256 alebo 128 bajtov	1024 bajtov
Nr. of Parallel Network Threads	Maximálny počet paralelných komunikačných threadov. V prípade požiadavky na vyšší počet údajov ítaných zo zariadenia za kratší čas, zvýšte hodnotu parametra.	1 až 4	1
Cycle Time	Požadovaná dĺžka jedného cyklu ítania údajov. V podstate perióda ítania údajov zo zariadenia, keďže asové parametre na stanici sa neuplatňujú.	ms	1000 ms
Message Timeout	Maximálny čas čakania na dátový odpoveď 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 komunikačnej chybe.	sec.ms	2 sec
Connection Error Timeout	Po uplynutí tejto doby a v prípade komunikačnej chyby na všetkých komunikačných threadoch, je na staniciach nastavený stav komunikačnej chyby a na linke stav FALSE.	sec.ms	20 sec
S7 PDU Size	Maximálne PDU v bajtoch pri S7 komunikácii s partnerom.	240, 480, 960 bytes	480 bytes
Tcp No Delay	Nastavenie "Tcp No Delay"=True parametra spôsobí nastavenie nízkoúrovňového parametra socketov TCP_NODELAY, im sa vypne prednastavené spájanie paketov.	-	False
Debug Values	Zapína ladiace informácie o naitaných hodnotách meraných bodov. Odporúčame zapnú iba v prípade nutnosti ladenia komunikácie, pretože výrazne zvyšuje záťaž CPU a spomaľuje komunikáciu.	YES/NO	NO
Debug I/O Binary Packets Info	Zapína ladiace informácie o binárnom obsahu komunikačných paketov. Odporúčame zapnú iba v prípade nutnosti ladenia komunikácie, pretože výrazne zvyšuje záťaž CPU a spomaľuje 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 komunikačnej stanice

- Komunikačný protokol: **Siemens SIMATIC S7 ISO over TCP**.
- Nežadáva 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.

Adresa meraného bodu je znakový reazec podľa 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 **cievým stpcom**

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

Kde:

;	Je voliteľný parameter, ktorý slúži na vyradenie meraného bodu z komunikácie. Taktiež sa nekontroluje správnosť adresy meraného bodu pri jeho ukladaní. Môže byť nápomocný pri fáze vývoja alebo ladenia komunikácie so zariadením.																		
S7: [con necti onna me]	Je nepovinný parameter, ktorý neobsahuje žiadnu potrebnú informáciu a je podporovaný iba kvôli spätnej kompatibilitate 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".																		
<obj ect>	Špecifikácia bloku alebo oblasti v S7 PLC. Možné sú hodnoty: <table border="1" data-bbox="207 829 1485 1318"> <thead> <tr> <th>Skratka</th> <th>Popis (Nemecký názov)</th> </tr> </thead> <tbody> <tr> <td>I, E</td> <td>Input (Eingang, E)</td> </tr> <tr> <td>Q</td> <td>Output (Ausgang, A)</td> </tr> <tr> <td>PI</td> <td>Peripheral Input (Peripherie Eingang, PE)</td> </tr> <tr> <td>PQ</td> <td>Peripheral Output (Peripherie Ausgang, PA)</td> </tr> <tr> <td>M</td> <td>Memory bit (F)</td> </tr> <tr> <td>C</td> <td>Counter (Zähler, Z) - BCD kódované celočíselné hodnoty z intervalu <0-999></td> </tr> <tr> <td>T</td> <td>Timer (Timer, T) - BCD kódované asovae z intervalov <0.00-9.99>, <00.0-99.9>, <000-999>, <0000-9.9990></td> </tr> <tr> <td>S</td> <td>System Status Lists (System-ZustandsListen, 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 byť typu Txtl.</td> </tr> </tbody> </table>	Skratka	Popis (Nemecký názov)	I, E	Input (Eingang, E)	Q	Output (Ausgang, A)	PI	Peripheral Input (Peripherie Eingang, PE)	PQ	Peripheral Output (Peripherie Ausgang, PA)	M	Memory bit (F)	C	Counter (Zähler, Z) - BCD kódované celočíselné hodnoty z intervalu <0-999>	T	Timer (Timer, 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 byť typu Txtl.
Skratka	Popis (Nemecký názov)																		
I, E	Input (Eingang, E)																		
Q	Output (Ausgang, A)																		
PI	Peripheral Input (Peripherie Eingang, PE)																		
PQ	Peripheral Output (Peripherie Ausgang, PA)																		
M	Memory bit (F)																		
C	Counter (Zähler, Z) - BCD kódované celočíselné hodnoty z intervalu <0-999>																		
T	Timer (Timer, 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 byť typu Txtl.																		

<p><type> e></p>	<p>Dátový typ S7. Pre objekty T, C a S nie je špecifikovaný.</p> <table border="1" data-bbox="207 205 1024 842"> <thead> <tr> <th>Identifikátor <type></th> <th>Popis</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>Bit (boolean). Treba špecifikovať číslo bitu 0 až 7 - napr. DB9,X8.3</td> </tr> <tr> <td>B</td> <td>Byte (8 bitov neznamienkovo).</td> </tr> <tr> <td>W</td> <td>Word (16 bitov neznamienkovo).</td> </tr> <tr> <td>D</td> <td>Double word (32 bitov neznamienkovo).</td> </tr> <tr> <td>CHAR</td> <td>Character (8 bitov znamienkovo).</td> </tr> <tr> <td>INT</td> <td>Integer (16 bitov znamienkovo).</td> </tr> <tr> <td>DINT</td> <td>Double integer (32 bitov znamienkovo).</td> </tr> <tr> <td>REAL</td> <td>Floating point number (32 bitov podľa IEEE754).</td> </tr> <tr> <td>LREAL</td> <td>Long floating point number (64 bitov podľa IEEE754).</td> </tr> <tr> <td>STRING</td> <td>String. Treba špecifikovať maximálnu dĺžku stringu.</td> </tr> <tr> <td>DT</td> <td>Date and Time, 8 bajtov v BCD formáte.</td> </tr> <tr> <td>TIME</td> <td>Time (32 bitov znamienkovo) v milisekundách.</td> </tr> <tr> <td>TOD</td> <td>Time of day (32 bitov neznamienkovo) v milisekundách.</td> </tr> </tbody> </table>	Identifikátor <type>	Popis	X	Bit (boolean). Treba špecifikovať číslo bitu 0 až 7 - napr. DB9,X8.3	B	Byte (8 bitov neznamienkovo).	W	Word (16 bitov neznamienkovo).	D	Double word (32 bitov neznamienkovo).	CHAR	Character (8 bitov znamienkovo).	INT	Integer (16 bitov znamienkovo).	DINT	Double integer (32 bitov znamienkovo).	REAL	Floating point number (32 bitov podľa IEEE754).	LREAL	Long floating point number (64 bitov podľa IEEE754).	STRING	String. Treba špecifikovať maximálnu dĺžku stringu.	DT	Date and Time, 8 bajtov v BCD formáte.	TIME	Time (32 bitov znamienkovo) v milisekundách.	TOD	Time of day (32 bitov neznamienkovo) v milisekundách.
Identifikátor <type>	Popis																												
X	Bit (boolean). Treba špecifikovať číslo bitu 0 až 7 - napr. DB9,X8.3																												
B	Byte (8 bitov neznamienkovo).																												
W	Word (16 bitov neznamienkovo).																												
D	Double word (32 bitov neznamienkovo).																												
CHAR	Character (8 bitov znamienkovo).																												
INT	Integer (16 bitov znamienkovo).																												
DINT	Double integer (32 bitov znamienkovo).																												
REAL	Floating point number (32 bitov podľa IEEE754).																												
LREAL	Long floating point number (64 bitov podľa IEEE754).																												
STRING	String. Treba špecifikovať maximálnu dĺžku stringu.																												
DT	Date and Time, 8 bajtov v BCD formáte.																												
TIME	Time (32 bitov znamienkovo) v milisekundách.																												
TOD	Time of day (32 bitov neznamienkovo) v milisekundách.																												
<p><address></p>	<p>Adresa premennej. Možné sú varianty:</p> <ul style="list-style-type: none"> • Byte offset (offset v rámci bloku, číslo 0-65535) • Byte offset.bit (len pre dátový typ X, číslo bitu v rozsahu 0 až 7) • Byte offset.String length (len pre dátový typ STRING, dĺžka stringu 1 až 254 znakov) • Id.Index[.StringOffset[.StringLength]] - len pre objekt S (system status list), pričom: <ul style="list-style-type: none"> • Id a Index sú 16 bitové čísla v rozsahu 0-65535 udávajúce ID konkrétneho zoznamu a index položky v ňom • StringOffset a StringLength sú bajtové offset (0..65535) a dĺžka (1..65535) podreazca v odpovedi, ktorý bude priradený do meraného bodu. <p>Príklad: adresa S237.1.10.20 zodpovedá stavovému zoznamu 237 (0x0111), index 1 (Identification of the module). S7-300 ako odpoveď na dotaz vráti odpoveď s dĺžkou 36 bajtov (bajty 0..35), pričom bajty 10..29 (t.j. Offset=10, dĺžka=20) udávajú "Order number of the module", napr. '6GK7 342-5DA02-0XE0'.</p> <p>Príklady adries:</p> <ul style="list-style-type: none"> • DB10,W35 • DB8,X10.0 • DB1,REAL12 • DB5,STRING5.14 • T20 • C7 • MB11 • MDINT30 • QX3.7 																												
<p><items></p>	<p>Počet elementov pre štruktúrované merané body s nakonfigurovaným cieovým stpcom. Každý načítaný element (1,2,3 .. <i>items</i>) bude zapísaný do jednej položky cieového stpca.</p> <p>Štruktúrované merané body nie sú podporované pre objekty typu T (timers), C (counters) a S (system status lists) ani pre dátový typ STRING.</p> <p>Pozn: Celý počet <i>item</i> elementov je vyíťavaný naraz. Pokiaľ je nakonfigurovaných napr. 100 elementov typu D (double word), jedná sa o íťanie bloku 400 bajtov. Pokiaľ pri nadviazaní komunikácie je dohodnutá menšia veľkosť paketu (S7 PDU size), íťanie takéhoto meraného bodu sa neuskutí a v logu linky bude o tom chybová hláška. Dohodnutá veľkosť S7 PDU size je minimom možností D2000 (parameter S7 PDU Size) a možnosť konkrétneho zariadenia.</p> <p>Pozn: syntax adresy pri zadaní počtu elementov je kompatibilná so Siemens S7 OPC serverom (napr. S7:[MyPLC]DB120,INT1050, 24), o umožňuje 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).</p> <p>Príklady adries:</p> <ul style="list-style-type: none"> • DB10,W35, 20 íťa sa blok 20 wordov (t.j. 40 bajtov) z adries 35-54 • DB8,X10.0, 100 íťa sa blok 100 bitov (t.j. 13 bajtov) z adries 10-22 																												

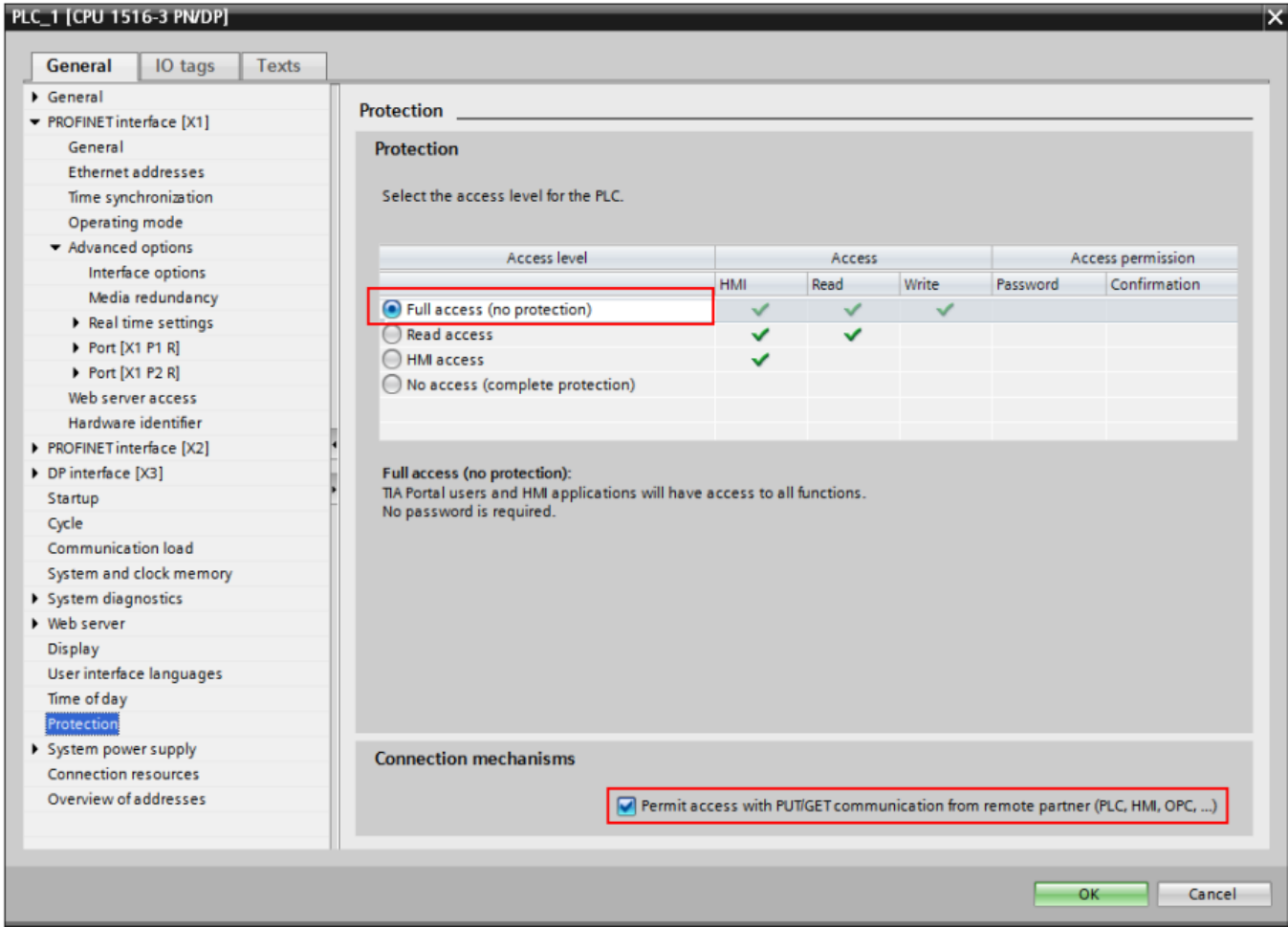
Poznámka k Siemens TIA Portal verzii 12 a vyšším

V praxi sa vyskytli prípady, keď sa komunikácia so zariadením (išlo o Simatic S7-1200) síce rozbehla, ale po poslaní požiadavky na íťanie dát zariadenie

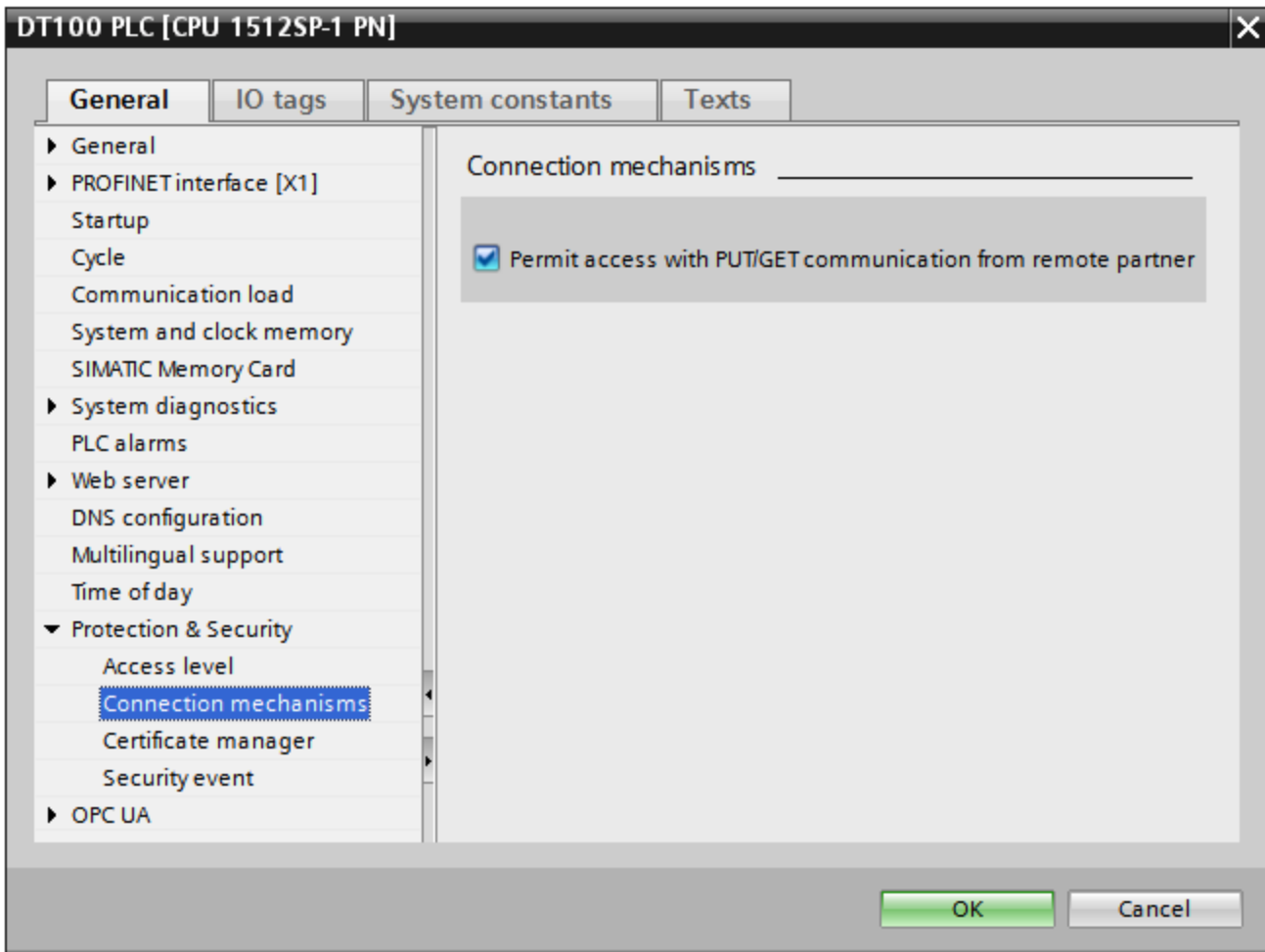
ako odpove neposlalo dáta, ale paket s ResultCode = 0x8104 tj. decimálne 33028.

Podľa <http://stackoverflow.com/questions/23745407/libnodave-error-while-reading-from-siemens-s7-1200-0x8104> je problém v nedostatočných prístupových právach. Príčinou je vyššia úroveň zabezpečenia 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 vlastnosťami CPU projektu je treba ísť na "Protection" a tam zaškrtnúť "Permit access with PUT/GET communications from remote partner" a nastaviť "Access level" podľa obrázku.

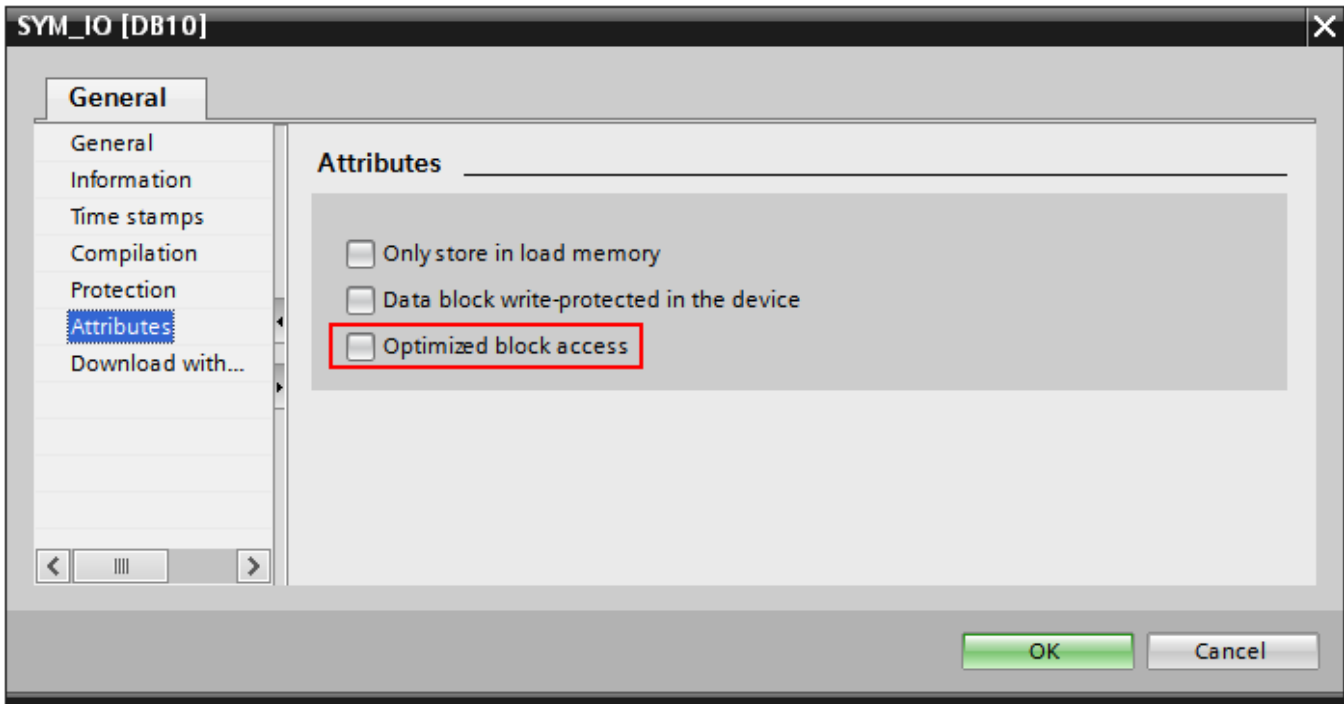


V prípade TIA Portal verzie 14 je nastavenie "Permit access with PUT/GET communications from remote partner" na samostatnej záložke "Connection mechanisms" pod "Protection & Security":



Poznámka k Siemens S7 1200/1500

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



Po zmene bezpečnostných nastavení v TIA Portal je nutné v menu vybrať Compile "Software (Rebuild all)" a po skompilovaní projekt nahrá do PLC. iastoný rebuild nemusí postačovať.

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."

Zmeny a úpravy

-

Revízie dokumentu

- Ver. 1.0 - 17. september 2010 - Vytvorenie dokumentu.



Súvisiace stránky:

[Komunikované protokoly](#)