Komunikacja ze sterownikami Siemens S7

Wykład

dr inż. Robert Kazała

Metody komunikacji

- Sterownik S7-1200 obsługuje następujące bloki komunikacyjne T przeznaczone do obsługi wymiany danych:
  - *TSEND_C i TRCV_C (z zintegrowanymi funkcjami połączenia i rozłączenia)*
  - *TCON, TSEND, TRCV oraz TDISCON (z ręcznym łączeniem i rozłączaniem)*
- Urządzenie S7-1200 obsługuje następujące protokoły ethernetowe:
  - *TCP (RFC 793)*
  - *ISO-on-TCP (RFC 1006)*
- Dane mogą być przesyłane do bloków komunikacyjnych z adresowaniem:
  - *bezwzględnym lub*
  - *symbolicznym.*

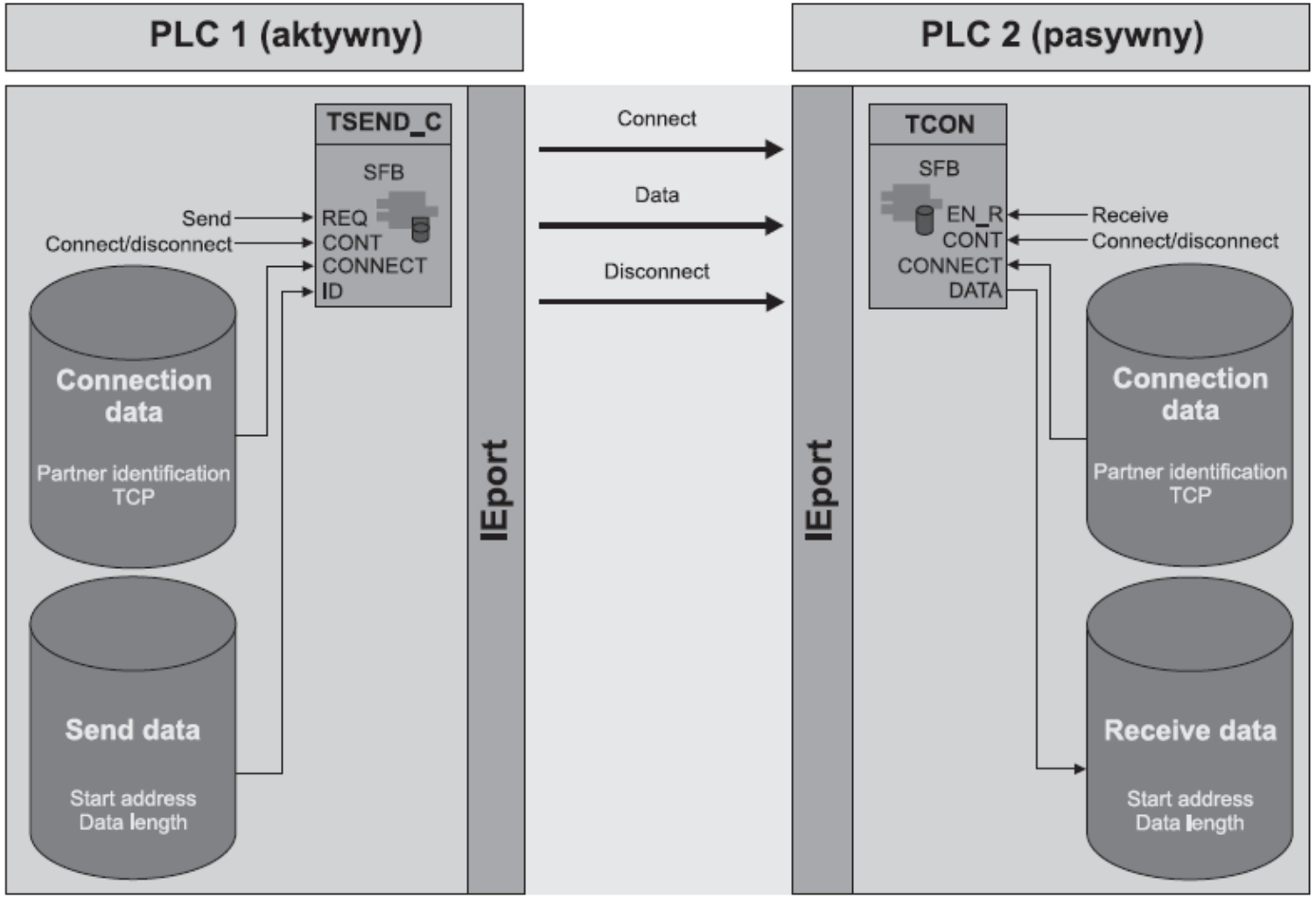
Protocol	Usage examples	Entering data in the receive area	Communication instructions	Addressing type
TCP	CPU-to-CPU communication Transport of frames	Ad hoc mode	Only TRCV_C and TRCV	Assigns port numbers to the Local (active) and Partner (passive) devices
		Data reception with specified length	TSEND_C, TRCV_C, TCON, TDISCON, TSEND, and TRCV	
ISO on TCP	CPU-to-CPU communication Message fragmentation and re-assembly	Ad hoc mode	Only TRCV_C and TRCV	Assigns TSAPs to the Local (active) and Partner (passive) devices
		Protocol-controlled	TSEND_C, TRCV_C, TCON, TDISCON, TSEND, and TRCV	
UDP	CPU-to-CPU communication User program communications	User Datagram Protocol	TUSEND and TURCV	Assigns port numbers to the Local (active) and Partner (passive) devices, but is not a dedicated connection
S7 communication	CPU-to-CPU communication Read/write data from/to a CPU	Data transmission and reception with specified length	GET and PUT	Assigns TSAPs to the Local (active) and Partner (passive) devices
PROFINET RT	CPU-to-PROFINET IO device communication	Data transmission and reception with specified length	Built-in	Built-in

Bloki komunikacyjne T

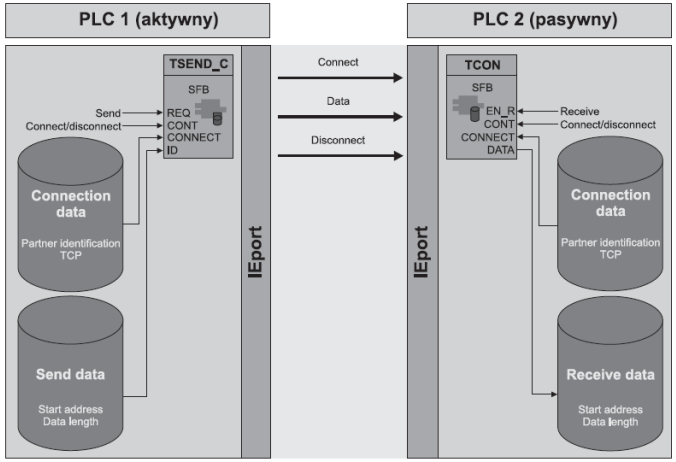
- Bloki komunikacyjne T sterownika S7-1200 umożliwiają nawiązanie jednocześnie do 8 połączeń w sieci Ethernet.
- Bloki komunikacyjne T zapewniające komunikację w sieci Ethernet obsługują następujące protokoły:
  - *Transport Connection Protocol (TCP): identyfikacja partnera połączenia za pomocą adresowania portów,*
  - *ISO Transport over TCP (ISO-on-TCP): identyfikacja partnera połączenia za pomocą usługi Transport Service Access Point (TSAP).*
- Za pomocą obu protokołów możliwa jest transmisja do 8192 bajtów na jedno zadanie.
- Podstawowa różnica między tymi protokołami polega na tym, że protokół ISO-on-TCP umożliwia przesyłanie danych o dynamicznie zmiennej długości danych, natomiast protokół TCP pozwala przesyłać tylko dane o stałej długości.

Zintegrowana obsługa połączeń

- Niezależnie od typu danych, przesyłanie danych o określonej długości z jednego S7-1200 CPU (PLC 1) do drugiego (PLC 2).

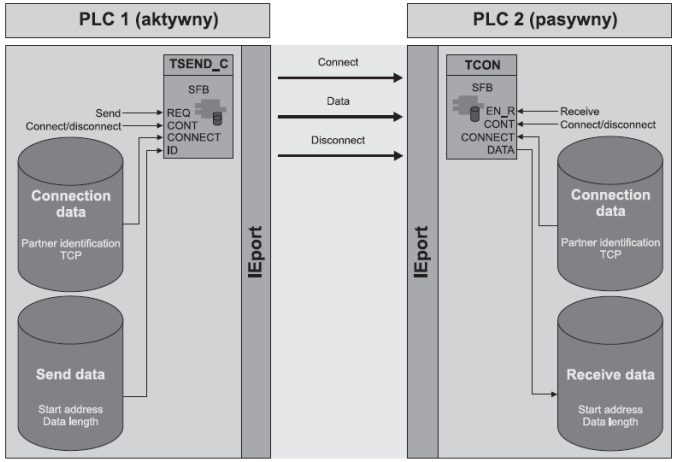


Zintegrowana obsługa połączeń



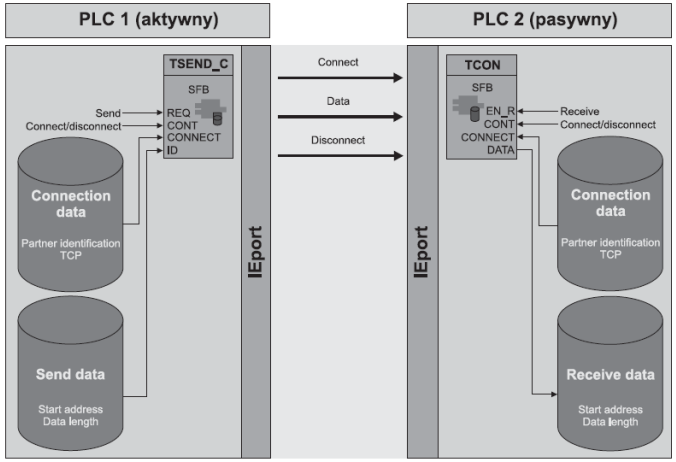
- Na rysunku jest widoczna struktura połączeń sieci Ethernet przy komunikacji z zintegrowaną obsługą połączeń.
- Sterownik PLC 1 wysyła dane z adresowaniem bezwzględnym do sterownika PLC 2 za pośrednictwem protokołu TCP (identyfikacja partnera komunikacyjnego za pomocą adresowania portów).
- Połączenie jest nawiązywane przy użyciu parametru CONT w trybie serwer-klient.
- Sterownik PLC 2 pasywnie oferuje swoje usługi (serwer), a sterownik PLC 1 aktywnie żąda nawiązania połączenia (klient).
- Po pomyślnym nawiązaniu połączenia jest ono podtrzymywane.

Zintegrowana obsługa połączeń



- Informacja o połączeniu jest pamiętana w jednym bloku danych dla TSEND_C i w jednym bloku danych dla TRCV_C (zaadresowanych poprzez parametr CONNECT).
- Zdefiniowany jest tu adres IP partnera komunikacji oraz używany protokół.
- Po stronie partnera komunikacji dane połączenia są pamiętane w analogiczny
- sposób.
- W razie wybrania innego protokołu, ustawienia powinny zostać zmienione także w bloku komunikacyjnym drugiego sterownika, co wymaga odpowiedniej modyfikacji w programie sterującym.
- Polecenia TSEND_C oraz TRCV_C są wykonywane asynchronicznie poprzez REQ lub EN_R.

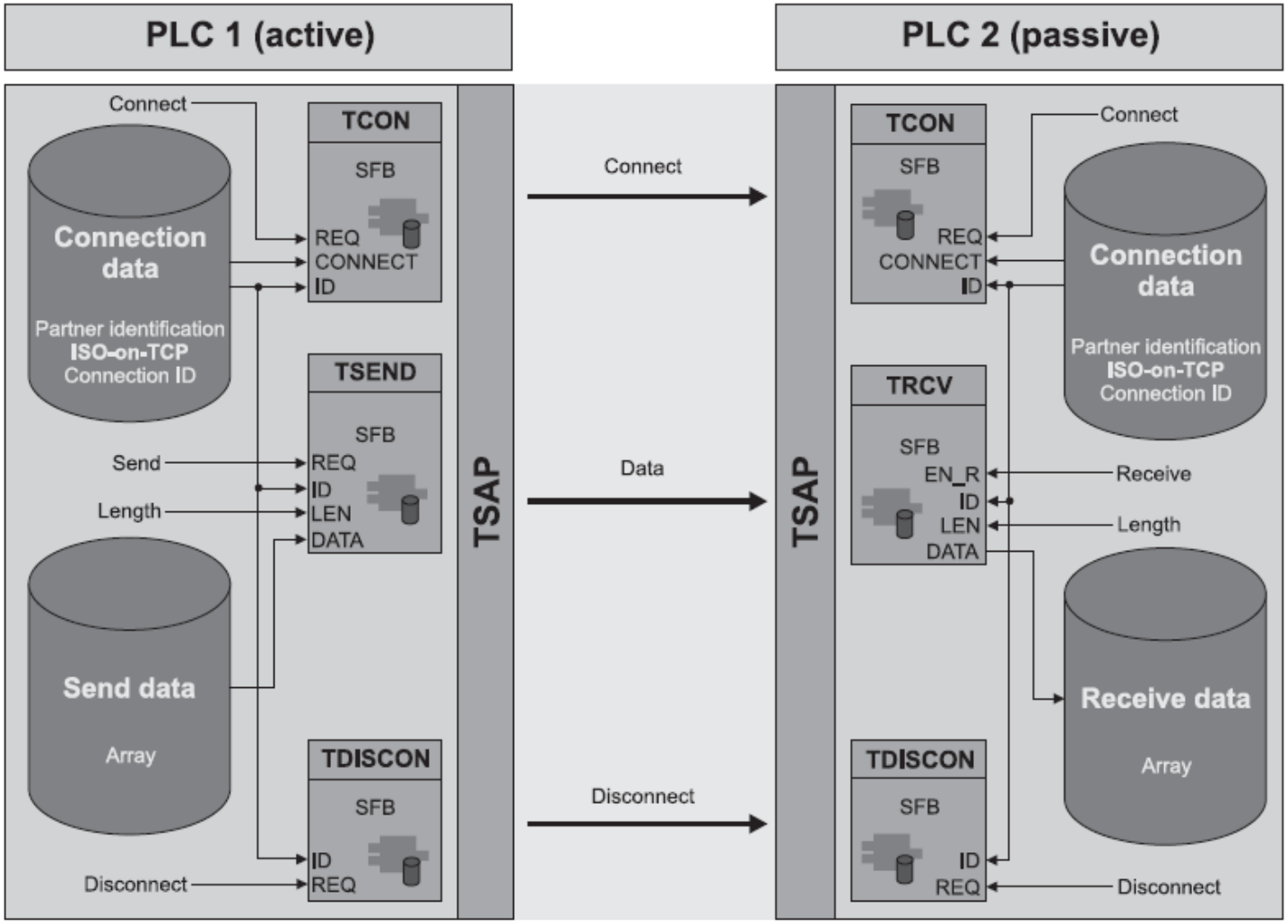
Zintegrowana obsługa połączeń



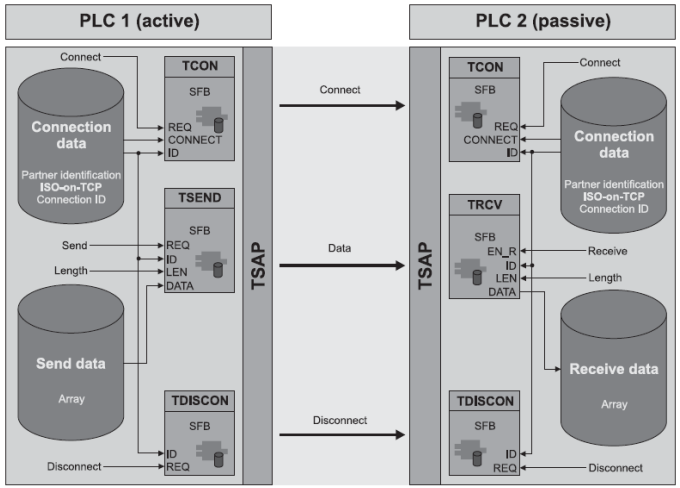
- Podczas wykonywania zadania nadawania przy dodatnim zboczu sygnału REQ, nie jest wymagana gotowość bloku TRCV_C do odbioru (EN_R = 1), ponieważ dane są buforowane.
- Dane te mogą być odebrane później w wyniku zezwolenia na odbiór (ustawienia EN_R = 1) (ale tylko ostatnio wysłane dane).
- Parametr DATA określa dane do wysłania lub skrzynkę odbiorczą za pomocą bezwzględnego adresu początkowego i długości.
- Zakończenie połączenia następuje po zresetowaniu parametru CONT.

Ręczna obsługa połączenia

- Należy przesłać dane o dynamicznie zmiennej długości z jednego S7-1200 CPU (PLC 1) do drugiego (PLC 2).

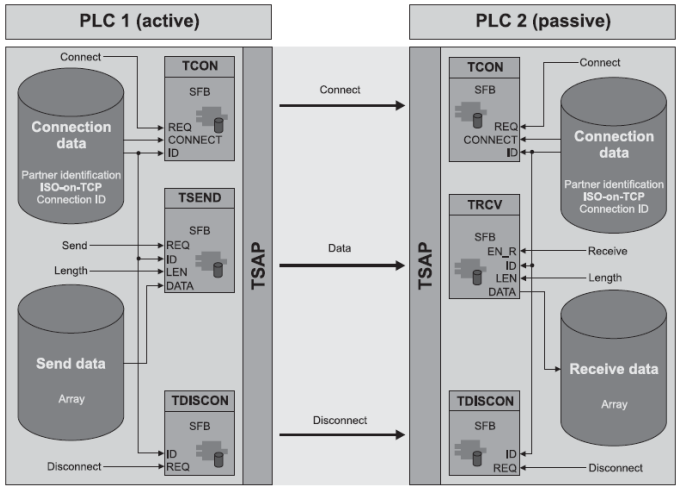


Ręczna obsługa połączenia



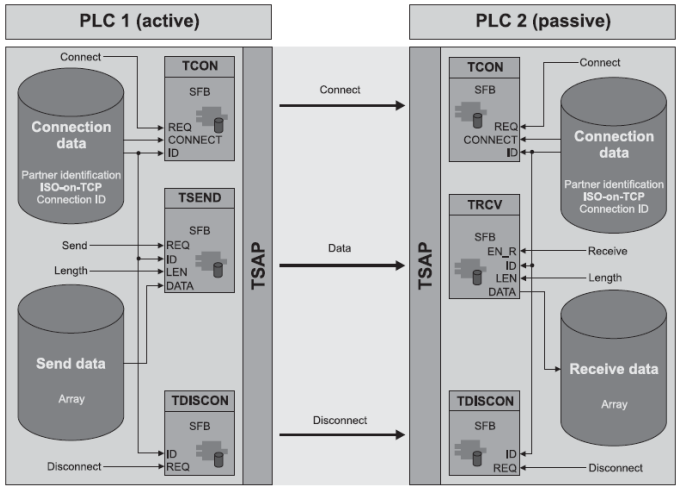
- Połączenie w sieci Ethernet z ręczną obsługą połączenia: wymiana danych za pośrednictwem bloków nadawania (TSEND) i odbioru (TRCV) wymaga nawiązania połączenia przez blok TCON, a do zakończenia transmisji jest wymagany blok TDISCON po każdej stronie kanału transmisyjnego.
- Na rysunku pokazano sposób realizacji transmisji ethernetowej z ręczną obsługą połączenia przy wykorzystaniu protokołu ISO-on-TCP.
- Sterownik PLC 1 wysyła dane zaadresowane symbolicznie do sterownika PLC 2 za pośrednictwem protokołu ISO-on-TCP (identyfikacja partnera połączenia za pomocą TSAP).
- Na dodatnim zboczu sygnału REQ blok TCON próbuje nawiązać połączenie z partnerem (zdefiniowanym w bloku danych CONNECT, identyfikowanym przez ID).

Ręczna obsługa połączenia



- Po wykonaniu przez obydwu partnerów transmisji rozkazu REQ połączenie zostaje nawiązane i utrzymywane.
- Informacja o połączeniu (partner transmisji, wybrany protokół i ID połączenia) jest pamiętana w bloku danych połączenia (zaadresowanym przez parametr CONNECT w bloku połączenia TCON).
- Blok nadawania (TSEND), blok odbioru (TRCV) oraz blok rozłączania TDISCON otrzymują informację o połączeniu jedynie przez przypisanie parametru ID połączenia do odpowiedniego parametru wejściowego ID bloku danych połączenia.

Ręczna obsługa połączenia



- Na dodatnim zboczu sygnału REQ blok TSEND wysyła symbolicznie zaadresowane dane DATA o długości LEN do partnera transmisji o identyfikatorze ID (zdefiniowanym w bloku połączenia TCON przez parametr CONNECT).
- Przesyłane dane są buforowane.
- Przy aktywnym zezwoleniu na odbiór (EN_R = 1) blok TRCV odbiera i zapamiętuje w parametrze DATA dane odebrane od partnera transmisji o identyfikatorze ID (zdefiniowanym w bloku połączenia TCON przez parametr CONNECT).
- Na dodatnim zboczu sygnału REQ blok TDISCON zamyka połączenie z partnerem transmisji scharakteryzowanym przez parametr połączenia ID.
- TDISCON musi być wykonany zarówno po stronie nadawania, jak i odbioru.

Bezpieczeństwo

- Jeśli atakujący może fizycznie uzyskać dostęp do sieci, atakujący może odczytać i zapisać dane.
- TIA Portal, CPU i HMI (z wyjątkiem HMI używających GET / PUT) używają bezpiecznej komunikacji, która chroni przed atakami typu "man-in-the-middle".
- Po włączeniu komunikacji wymiana podpisanych wiadomości odbywa się w przejrzystym tekście, który umożliwia atakującemu odczytanie danych, ale chroni przed nieautoryzowanym zapisaniem danych.
- TIA Portal , a nie proces komunikacji, szyfruje dane bloków chronionych.
- Wszystkie inne formy komunikacji (wymiana I / O przez PROFIBUS, PROFINET, AS-i lub inne magistrale I / O, GET / PUT, T-Block i moduły komunikacyjne (CM)) nie mają żadnych zabezpieczeń.
- Należy chronić te formy komunikacji, ograniczając fizyczny dostęp. Jeśli atakujący może fizycznie uzyskać dostęp do sieci za pomocą tych form komunikacji, osoba atakująca może odczytać i zapisać dane.