Protokoły komunikacji

Wykład

dr inż. Robert Kazała

Modbus

- Protokół komunikacyjny stworzony w 1979 roku przez firmę Modicon.
- Służył do komunikacji z programowalnymi kontrolerami tej firmy.
- Opracowany z myślą do zastosowań w automatyce
- Protokół jest otwarty i wolny od opłat
- Przesyłane komunikaty są zabezpieczone przed przekłamaniami
- Sygnalizacja błędów
- Jest standardem przyjętym przez większość producentów sterowników przemysłowych
- Jest łatwy do wdrożenia i utrzymania
- www.modbus.org

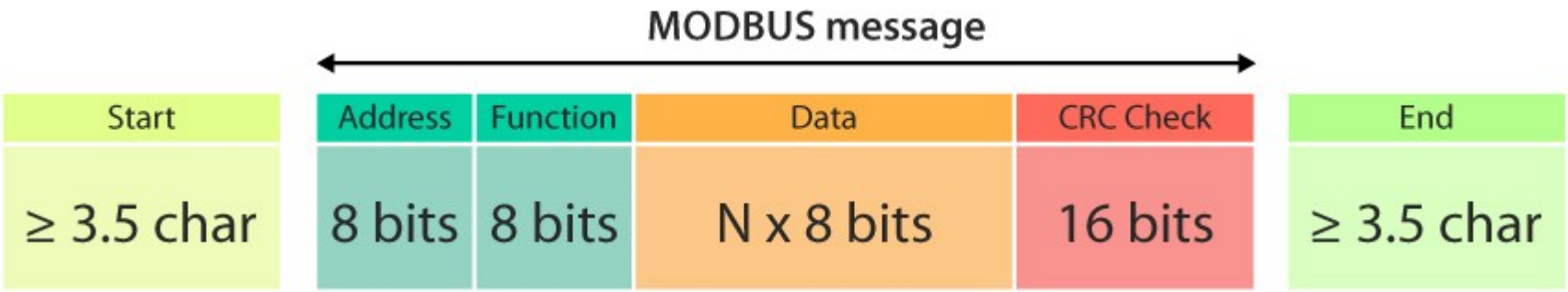
Modbus – sposób przesyłania

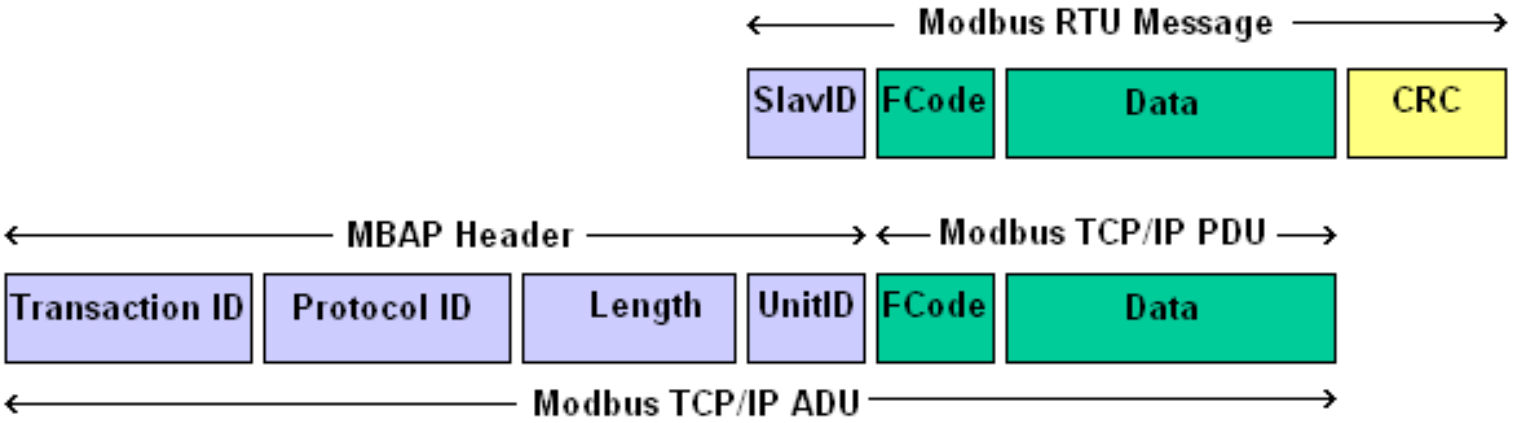
- Protokół Modbus może być implementowany na sieci w standardzie RS232, ale wtedy jest typu punkt-punkt., z jednym urządzeniem nadrzędnym (master) i jednym podrzędnym (slave).
- W przypadku sieci RS485 można uzyskać strukturę wielopunktową, z jednym urządzeniem nadrzędnym (master) i wieloma podrzędnymi (max. 247)
- ASCII - system kodowania heksadecymalny 0-9, A-F. Dane wysyłane szesnastkowo (po dwa kody ASCII). Każdy znak zajmuje 4 bity.
- RTU - system kodowania dwójkowy 0/1. Dane wysyłane binarnie jako liczby ośmiobitowe.
- TCP - dane wysyłane po sieci LAN zgodnie z protokołem TCP/IP.

Modbus - RTU

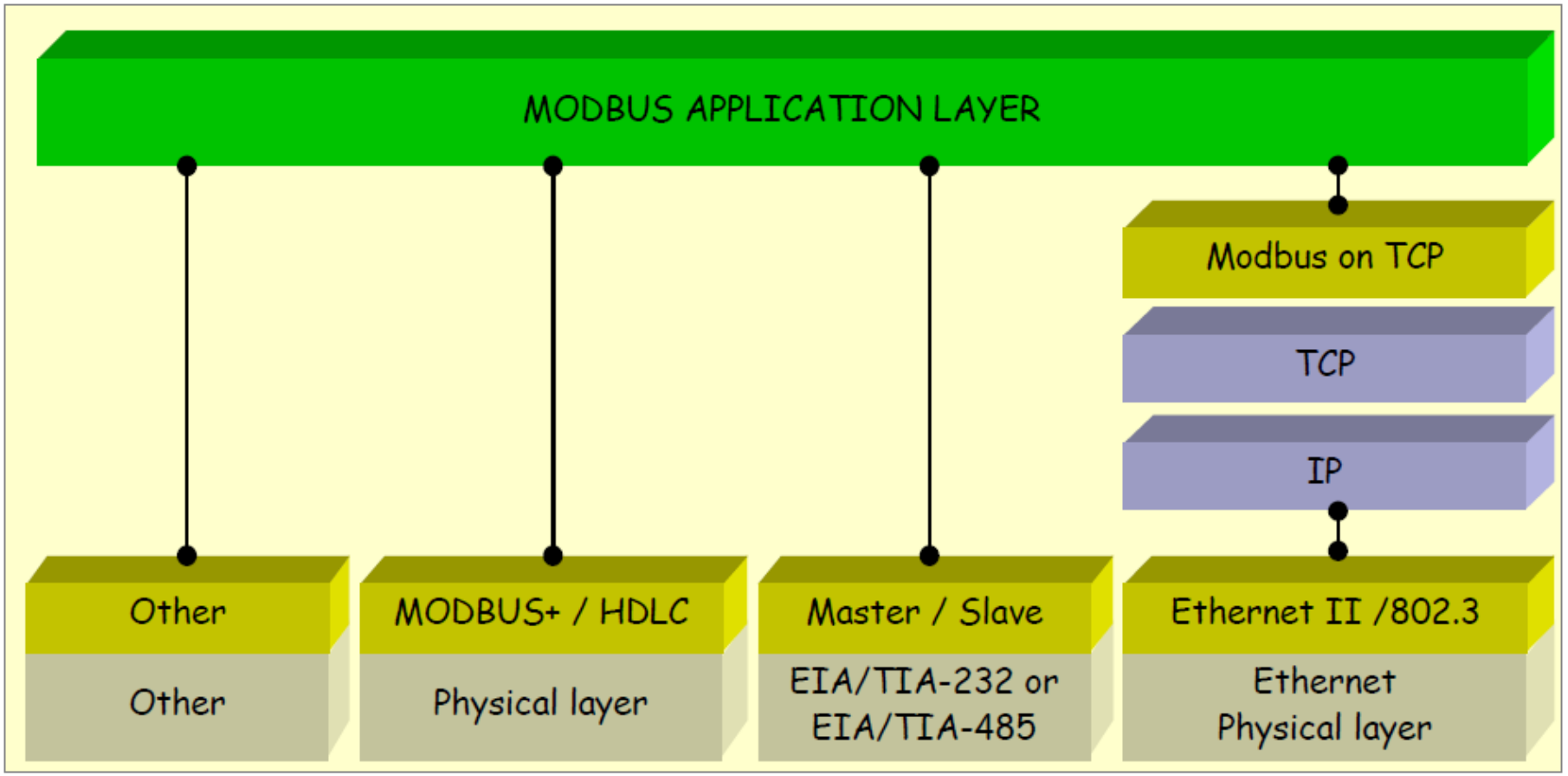
- W celu nawiązania komunikacji z modułami Slave sterownik Master wysyła komunikaty zawierające:
  - *adres modułu Slave,*
  - *kod funkcji,*
  - *dane,*
  - *bity kontrolne.*
- Adres urządzenia to liczby z zakresu 0247.
- Adres 0 zarezerwowany jest dla komunikatów typu broadcast – wysyłanych do wszystkich urządzeń Slave, zaś adresy od 1 do 247 wskazują już konkretne moduły.
- Z wyjątkiem komunikatów typu broadcast (tylko odbiór), urządzenia Slave zawsze odpowiadają na komunikaty wysyłane przez Mastera, który w ten sposób ma pewność, że odebrały one komunikat.

Modbus - ramka

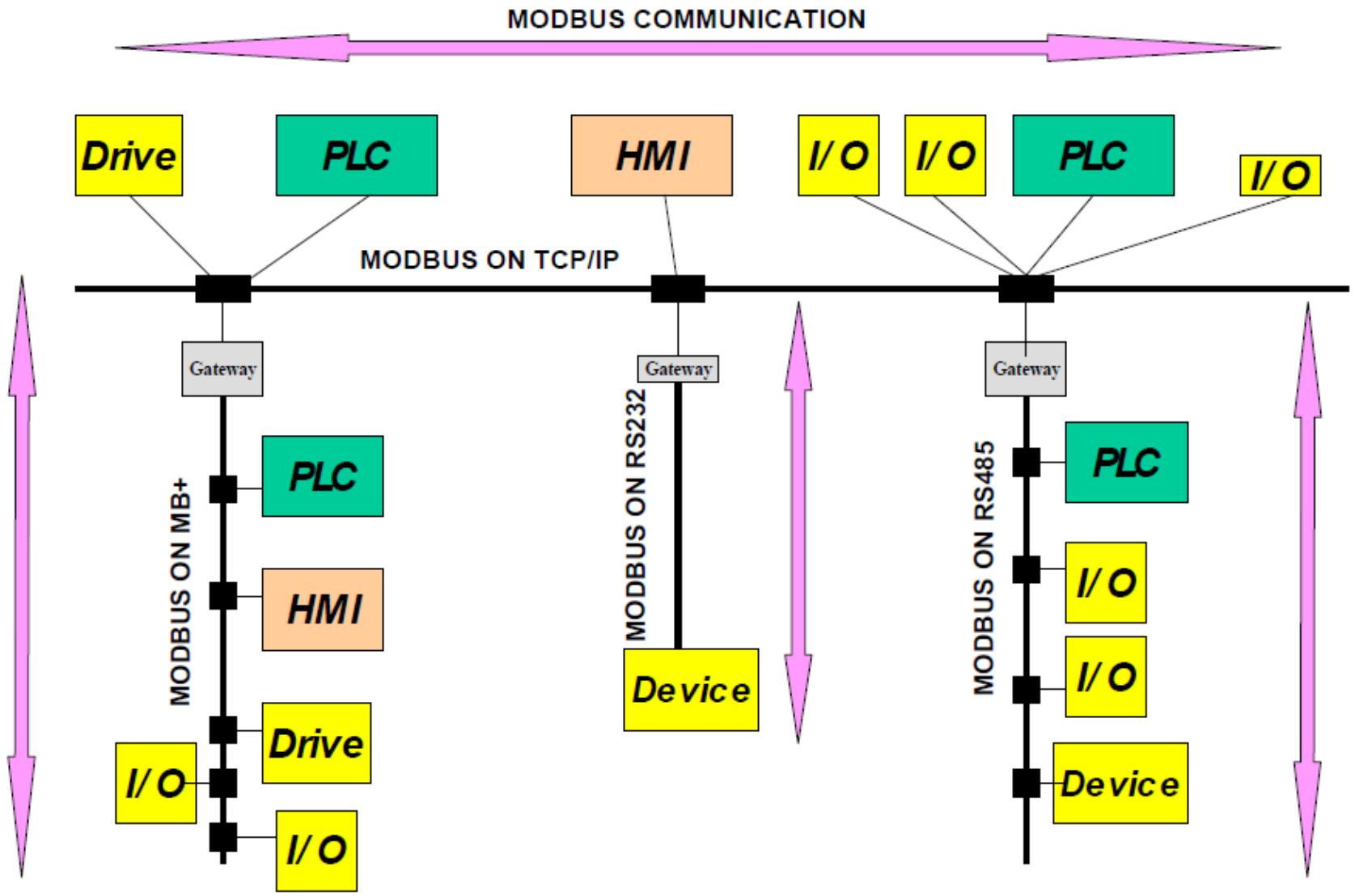




Modbus – stos komunikacyjny

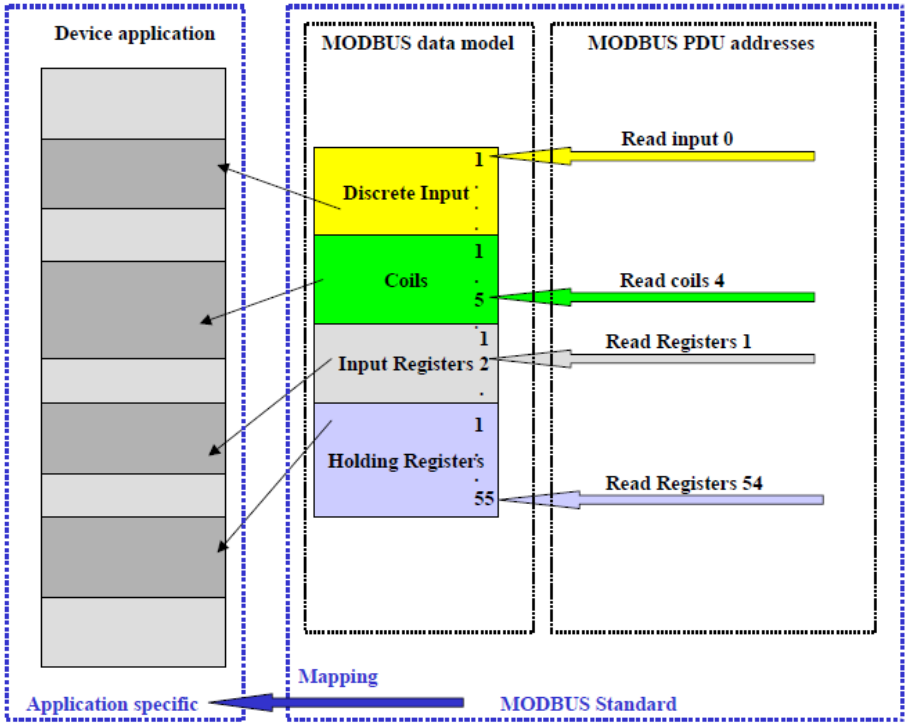


Modbus – przykładowa struktura sieci



Modbus – typy danych, adresowanie

Typ	Rodzaj zmiennej	Możliwość zapisu	Wykorzystanie
Discretes Input Wejścia dwustanowe	**Single bit** Jedno-bitowy	**Read** Tylko odczyt	dwustanowe wejścia albo wyjścia urządzeń
Coils Cewka , przekaźnik	**Single bit** Jedno-bitowy	**Read /Write** Odczyt / zapis	przekaźniki wewnętrzne, wyjścia urządzeń
Input Registers Rejestry wejściowe	**16-bit Word** Słowo 16-bitowe	**Read** Tylko odczyt	Liczbowe wartości na wejściach lub wyjściach
Holding Registers Rejestry pamietajace	**16-bit Word** Słowo 16-bitowe	**Read /Write** Odczyt / zapis	Odczyty i zapisy do rejestrów wewnętrznych



Modbus – definicje podstawowych kodów

Opis funkcji	Kod funkcji (dziesiętnie)	Kod funkcji (szesnastkowo)
Read Coils Odczyt stanów wyjść binarnych. Np. wyjść PLC	**01**	**0x 01**
Read Discrete Inputs Odczyt stanów wejść binarnych. Np. wejść PLC	**02**	**0x 02**
Read Holding Register Odczyt rejestrów pamiętających	**03**	**0x 03**
Read Input Register Odczyt rejestrów wejściowych np. wartości z wejść analogowych PLC	**04**	**0x 04**
Write SingleCoils Zapis jednego wyjścia binarnego, ustawianie przekaźnika	**05**	**0x 05**
Write single Register Zapis do jednego rejestru pamiętającego	**06**	**0x 06**
Write Multiple Coils Zapis wielu wyjść binarnych, ustawianie przekaźników	**15**	**0x0F**
Write Multiple Registers Zapis do wielu rejestrów	**16**	**0x 10**
Diagnostyka, zgłaszanie błędów	**03**	**0x08**

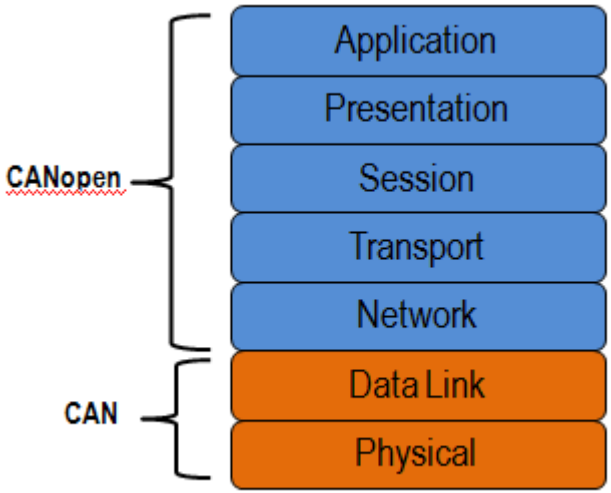
Profibus

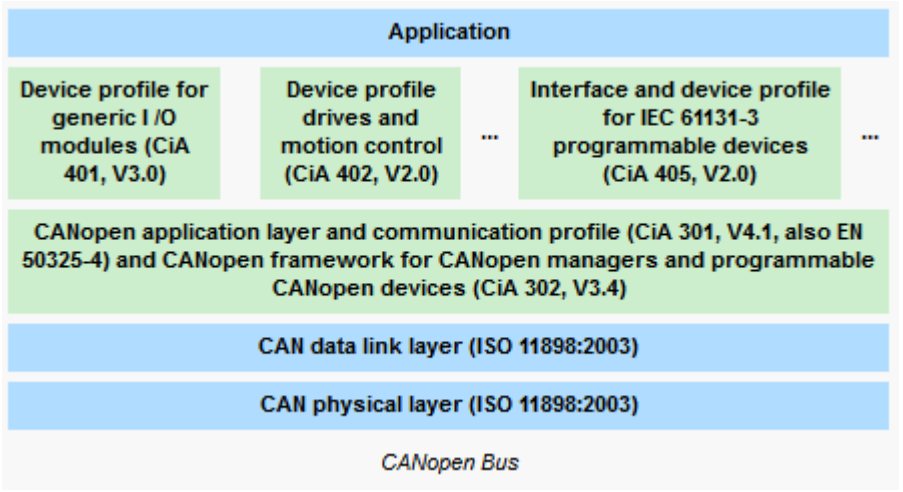
- Profibus jest siecią przemysłowa czasu rzeczywistego opracowana przez konsorcjum firm koordynowane przez firmę Siemens. Przeznaczona do rozproszonego sterowania i nadzoru.
- W warstwie fizycznej możliwe jest zastosowanie dwóch przewodów miedzianych, skrętki lub światłowodu.
- Odmiany Profibus:
  - *DP (ang. DecentralizedPerhipals) sied czasu rzeczywistego zorientowana na przesyłanie krótkich komunikatów*
  - *FMS (ang. FieldbusMessageSpecification) –zastosowanie do sieci wymagających przesyłania większych porcji danych (np. SCADA<>PC)*
  - *PA (ang. ProcessAutomation) –możliwość stosowania w środowiskach zagrożonych wybuchem, te same linie służą do zasilania i do transmisji danych.*

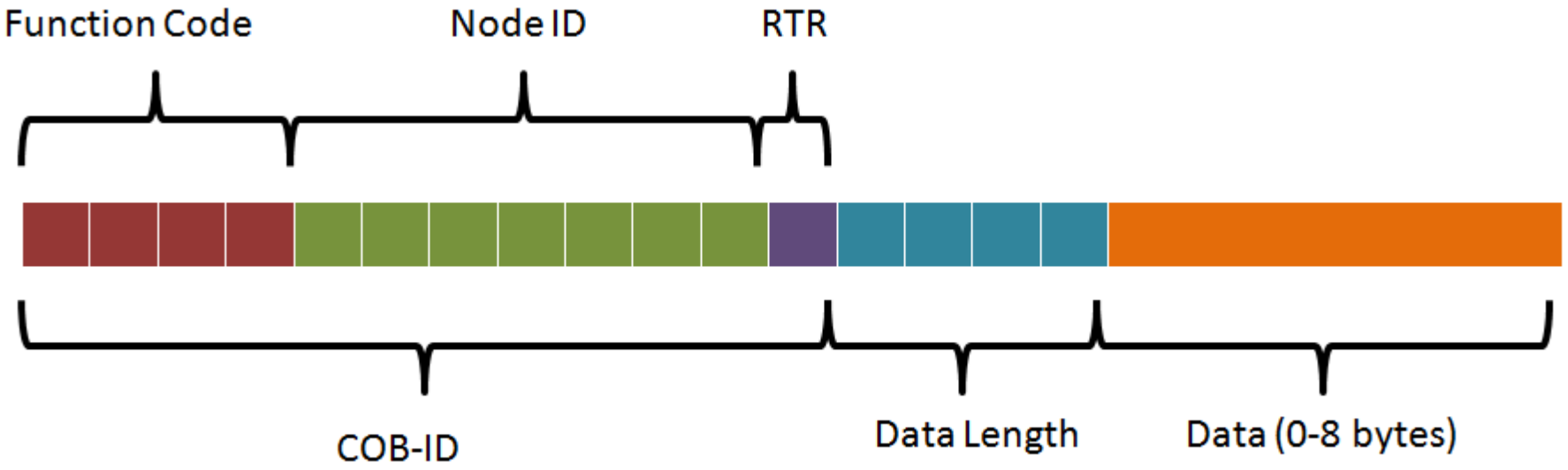
CANOpen

- Protokół wysokiego poziomu CANopen, bazuje bezpośrednio na podstawowym protokole CAN i został opracowany z myślą o zastosowaniu w przemysłowych sieciach wbudowanych, lokalnych.
- CANopen to standard europejski – EN 50325-4.
- Zapewnia on integratorom i klientom przemysłowym swobodę organizacji sieci i dołączania do niej nowych urządzeń w praktyce wg zasady plug-and-play, bez większych problemów z kompatybilnością i otwartością standardu.
- Opracowaniem profili dla różnych zastosowań zajmuje się grupa użytkowników i producentów urządzeń standardu CAN (CiA – CAN In Automation), zrzeszająca obecnie ok. 520 podmiotów.
- Profile aplikacyjne ułatwiają działanie wszystkim osobom zaangażowanym na etapach produkcji, instalacji i integracji sieciowej zaawansowanych, specjalistycznych urządzeń.

CANOpen


CANopen
CAN
Application
Presentation
Session
Transport
Network
Data Link
Physical


Application
Device profile for generic I /O modules (CiA 401, V3.0)
Device profile drives and motion control (CiA 402, V2.0)
...
Interface and device profile for IEC 61131-3 programmable devices (CiA 405, V2.0)
...
CANopen application layer and communication profile (CiA 301, V4.1, also EN 50325-4) and CANopen framework for CANopen managers and programmable CANopen devices (CiA 302, V3.4)
CAN data link layer (ISO 11898:2003)
CAN physical layer (ISO 11898:2003)
CANopen Bus


Function Code
Node ID
RTR
COB-ID
Data Length
Data (0-8 bytes)

CANopen Object Dictionary

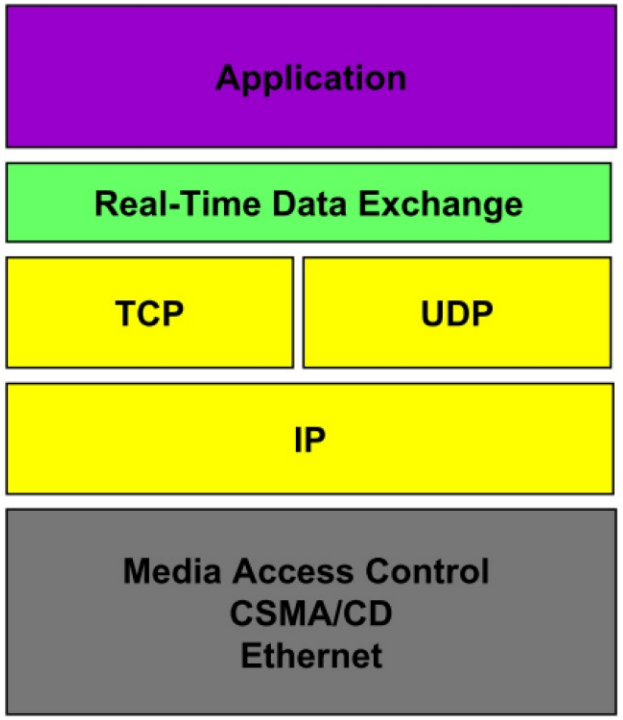
- CANopen Object Dictionary jest uporządkowaną grupą obiektów.
- Każdy obiekt posiada swój 16bitowy indeks, oraz dodatkowo 8-bitowy subindeks.
- Każdy węzeł w sieci posiada swój własny Object Dictionary, który całościowo opisuje wszystkie jego parametry oraz zachowanie w sieci.
- Pełny opis Object Dictionary dla konkretnego typu urządzenia jest dostarczany przez producenta i znajduje się w Electronic Data Sheet (EDS), który jest plikiem ASCII z rozszerzeniem *.eds.
- Na podstawie EDS powstaje opis konkretnego, sparametryzowanego urządzenia w sieci – Device Configuration File (DCF).
- DCF posiada taką samą składnie jak EDS, zdefiniowaną w specyfikacji opracowanej przez CIA – CiA 306 DS V1.3.
- Pliki te są używane przez Menadżery sieci CANOpen w celu łatwej parametryzacji transmisji i urządzeń w sieci.

CANopen - Mechanizmy komunikacji: PDO i SDO

- W sieci wyróżniamy dwie główne metody komunikacji: Service Data Object oraz Process DataObject.
  - *Service Data Object pozwalają na dostęp do Object Dictionary urządzeń sieci oraz transmisje większej niż 8 bajtów ilości danych. Mechanizm transmisji z potwierdzeniem odbioru, stąd każde SDO posiada dwa różne identyfikatory. Typowo SDO jest używany do konfiguracji węzłów sieci.*
  - *Process Data Object, może być opisany jako komunikacja typu Producent – Konsument. Został zoptymalizowany do szybkiej transmisji danych. Jest wykorzystywany do transmisji danych w czasie rzeczywistym (stany Wejść/ Wyjść, wartości analogowych etc.). Nie wymaga potwierdzenia odbioru, wykorzystuje wyższe priorytety wiadomości (COB-ID, CAN-ID). Struktura zawartości ramki PDO musi być wcześniej zdefiniowana i znana zarówna nadawcy jak i odbiorcy. Ilość danych w jednym PDO jest ograniczona od 1 do 8 bajtów. Przykładowo, jeden PDO może transmitować stan maksymalnie 64 wartości I/O lub czterech 16-bitówych wartości analogowych. Obiekty PDO, w zależności od konfiguracji, mogą być transmitowane cyklicznie, na żądanie innego urządzenia lub wyzwalane przez zmianę wartości mapowanej w PDO.*

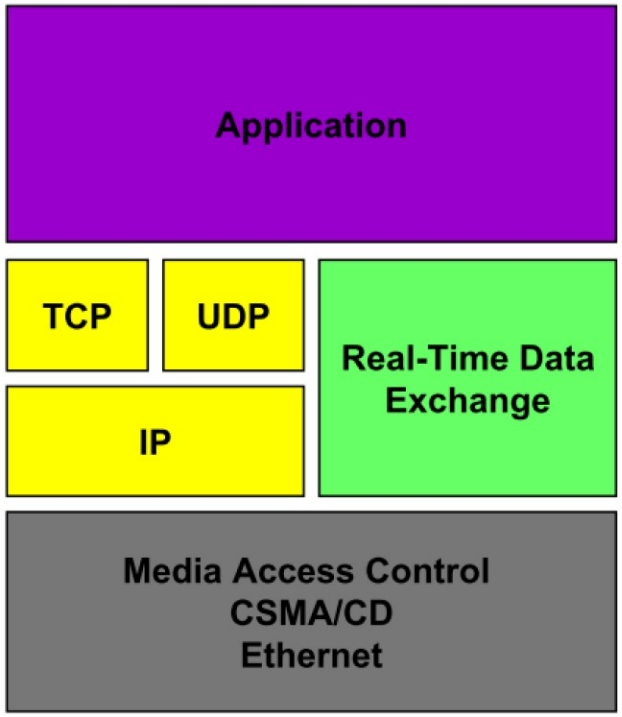
Warianty architektury RT Ethernet

Architecture 1



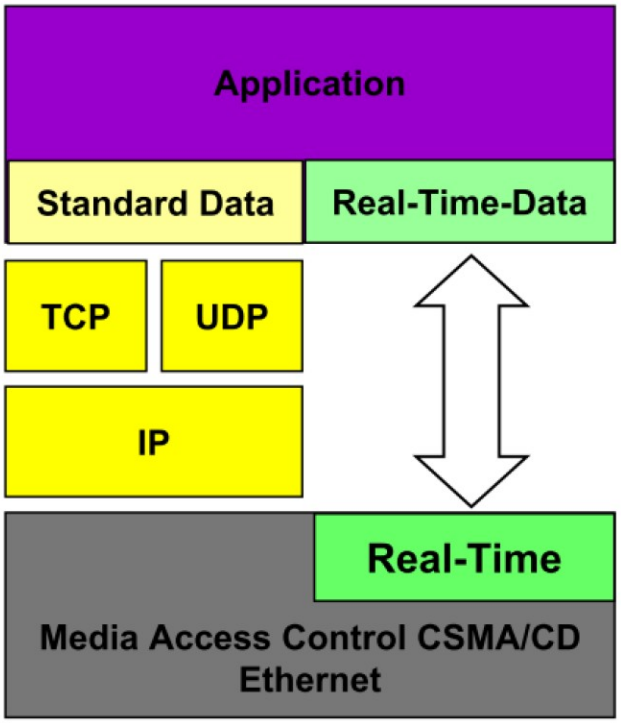
Standard Ethernet TCP/IP:
EtherNet/IP, HSE, JetSync, ModbusTCP, PNet, Safeethernet, VNET

Architecture 2



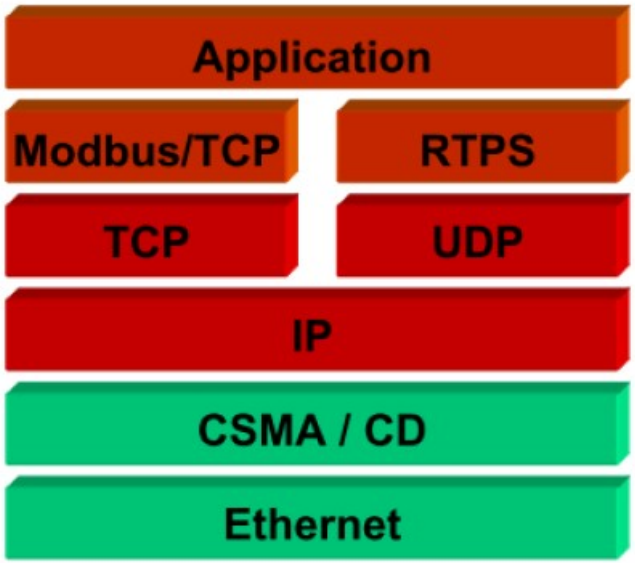
Software (S/W) By-Passing Layer 3 und 4:
ETHERNET Powerlink, PROFInet V2

Architecture 3



Hardware (H/W) By-Passing Layer 3 und 4:
EPA, EtherCat, PROFInet V3, SERCOS III, TCnet

Modbus/TCP



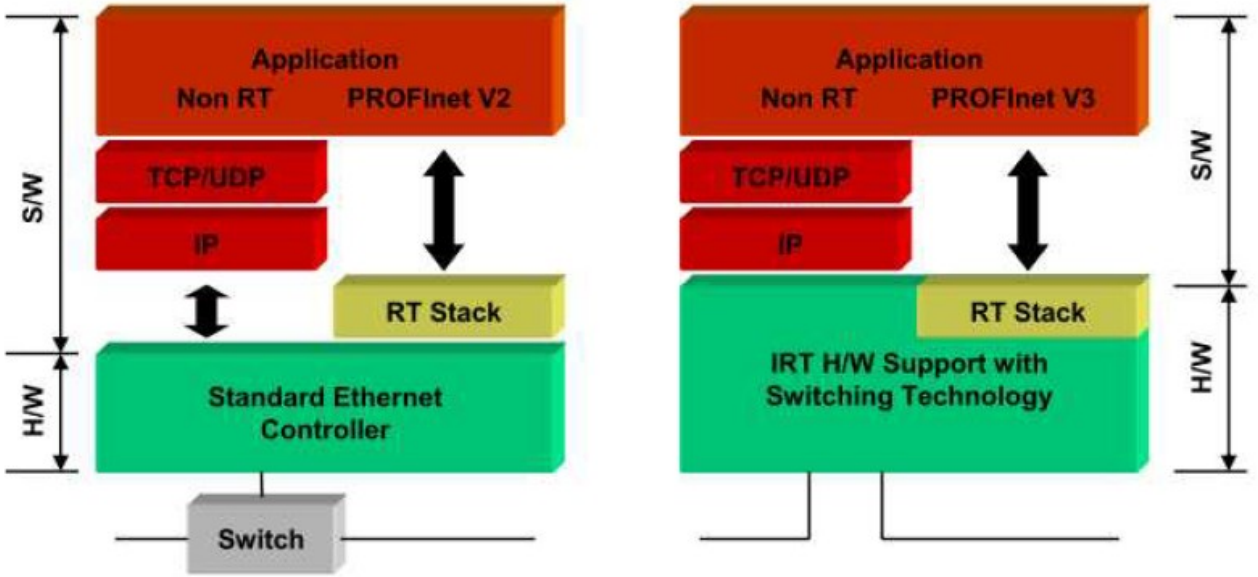
- User Organization : Modbus-IDA
- Developed by Modicon (Schneider Electric), France
- Porting of the Modbus-protocol to TCP
- ModbusTCP is very simple and easy to implement
- RTPS (Real-Time Publish and Subscribe) as enhancement
- Specification is publicly available

Profinet

- Profinet jest przez rozwijany przez konsorcjum PROFIBUS International.
- Profinet pozwala na integrację w jednej sieci prostych urządzeń polowych oraz aplikacji krytycznych czasowo.
- Komunikacja ma trzy poziomy wydajności:
  - *TCP, UDP i IP dla danych niekrytycznych czasowo,*
  - *Soft Real Time (SRT) dla danych krytycznych czasowo,*
  - *izochroniczny tryb Real Time (IRT) do wyjątkowo wymagających zastosowań.*
- Jako elementy aktywne wykorzystywane są specjalne switche.

Profinet

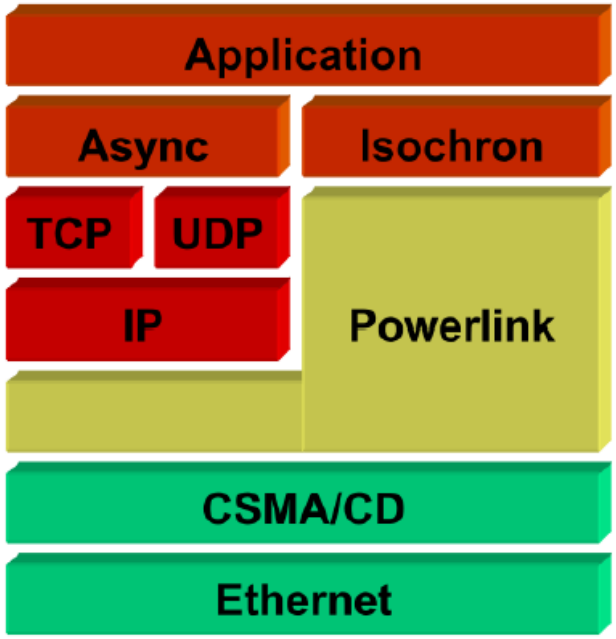
- User organization: Profibus Nutzerorganisation
- ProfiSafe is in development (Porting from Profibus to ProfiNet)
- Developed by Siemens, Germany
- V2: Software implemented (RT)
  V3: Hardware implemented (IRT)
- Communication mode:
  ProfiNet IO (RT & IRT)
  ProfiNet CBA (TCP/IP or RT)



Ethernet Powerlink

- Ethernet Powerlink-wspierany przez EPSG.
- Składa się z podsieci (domen) czasu rzeczywistego.
- Aby uniknąć kolizji, mechanizm CSMA/CD jest wyłączony.
- Dostęp do sieci jest podzielony na cykliczne szczeliny czasowe, przydzielane każdemu punktowi sieci przez stację zarządzającą.

Ethernet Powerlink

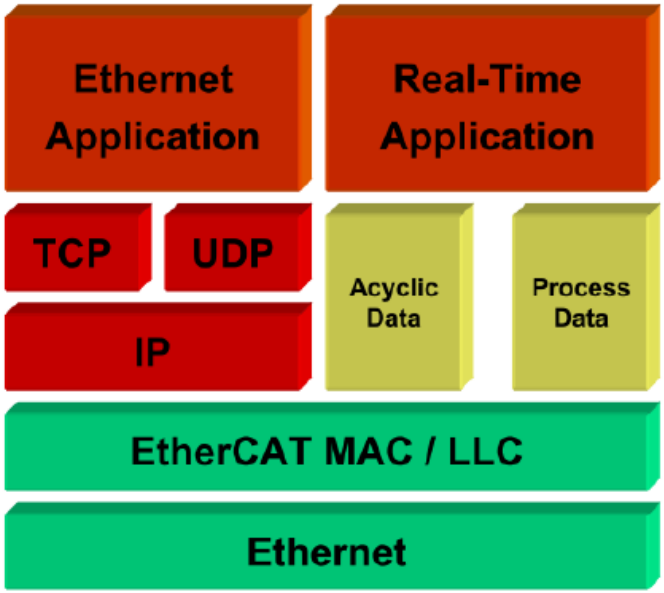


- User organization : Ethernet Powerlink Standardization Group
- Developed by Firma B&R, Austria
- IEEE 1588 is part of the concept
- EPL Safety up to SIL 3 (4)
- EPL is based on a fixed access control to the bus. A master informs the Slaves about their time slots. One free slot for CSMA/CD.
- (Transparent) Gateway for communication to the outside.
- [ ] profiles based on CANopen

EtherCAT

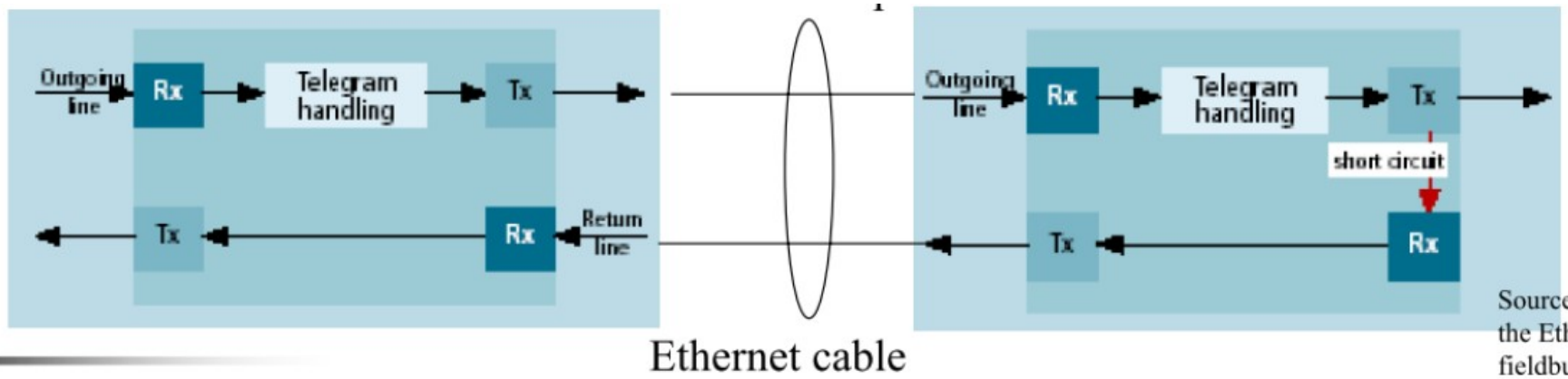
- Protokół rozwijany przez EtherCAT Technology Group.
- Protokół wykorzystuje ramki ethernet.
- Interpretacja danych odbywa się "w locie", w pełni sprzętowo.
- EtherCAT jest najszybszym protokołem wykorzystujący Ethernet osiąga 1000 I/O binarnych w 30µs.
- Masterem może być dowolny komputer wyposażony w kartę sieciową.
- W przypadku urządzeń podrzędnych (slave) nie jest możliwe wykorzystanie typowej karty sieciowej i wymagane są interfejsy sieciowe realizowane na specjalizowanych układach scalonych.

EtherCAT



- User organization: EtherCAT Technology Group
- Developed by Beckhoff, Germany
- Bases directly on MAC-Layer
- IP-Protocol is tunnelled within EtherCAT
- Ethernet-Frames are processed on-the-Fly
- IEEE 1588 part of the concept
- EPL Safety up to SIL 3
- [redacted] profiles based on CANopen & ServoDrive

EtherCAT



Source: EtherCat the Ethernet fieldbus,

EtherNet/IP

- EtherNet/IP -wspierany przez ODVAi ControlNet. Używa CommonInterfaceProtocol(CIP), który jest wspólny dla sieci Ethernet/IP, ControlNeti DeviceNet. W sieci Ethernet/IP, wymiana danych krytycznych czasowo oparta jest na modelu producer/consumer. Największą zaletą tego modelu jest większa efektywnośd wykorzystania pasma. Dane konfiguracyjne, diagnostyczne i I/O przesyłane są przez standardowy ethernet.
- •Ethernet Powerlink-wspierany przez EPSG. Ethernet Powerlinkskłada się z podsieci (domen) czasu rzeczywistego. Aby uniknąd kolizji, mechanizm CSMA/CD jest wyłączony. Dostęp do sieci jest podzielony na cykliczne szczeliny czasowe, przydzielane każdemu punktowi sieci przez stację zarządzającą.