Internet rzeczy

IIoT – Przemysłowy Internet Rzeczy

Przemysłowe systemy sterowania

Protokoły i standardy komunikacyjne

Protokoły automatyki przemysłowej

Materiały

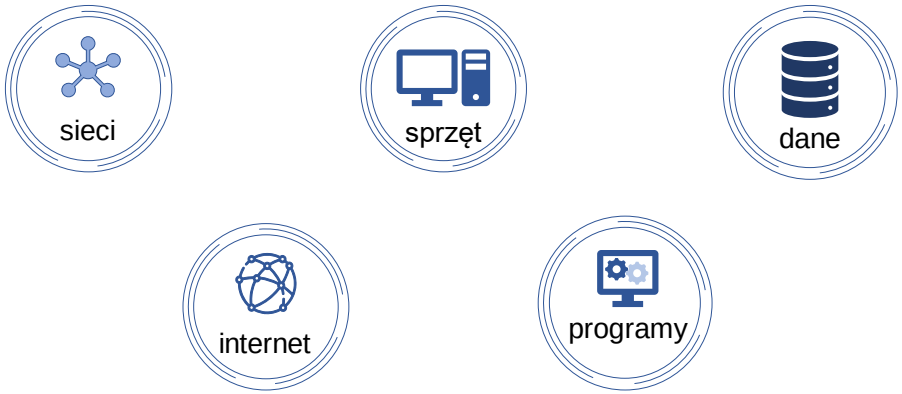
http://staff.uz.zgora.pl/gpajak

Przemysłowe systemy sterowania

IT

Technologia Informacyjna, IT (ang. Information Technology)

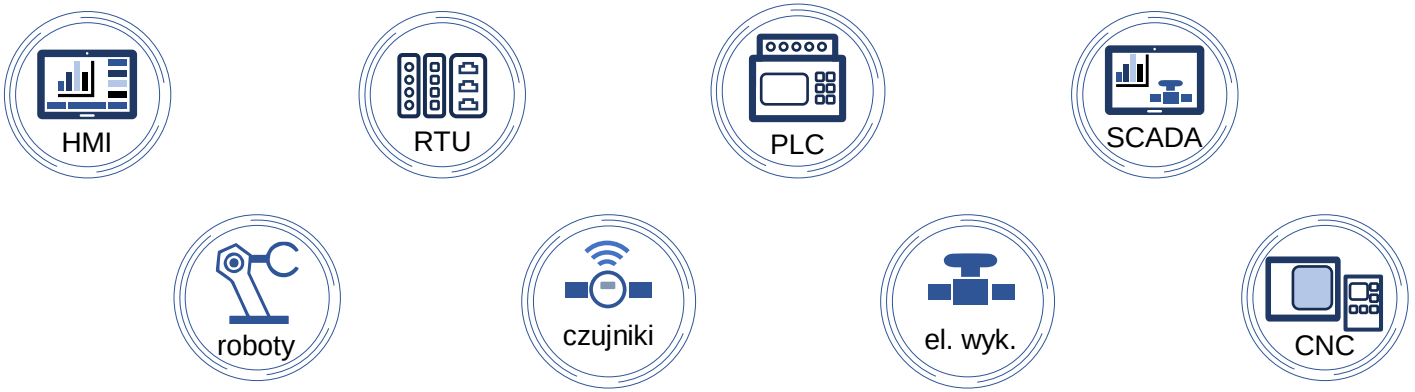
- dziedzina zajmująca się stosowaniem technologii komputerowych i komunikacyjnych do zbierania, przetwarzania, przechowywania, przesyłania i wykorzystywania informacji,
- obejmuje sprzęt (komputery, serwery, urządzenia peryferyjne, ...), oprogramowanie (systemy operacyjne, aplikacje użytkowe, ...), dane, sieci telekomunikacyjne (internet, sieci komórkowe, ...),
- zapewnia efektywne zarządzanie danymi.



OT

Technologia Operacyjna, OT (ang. OperationalTechnology)

- dziedzina zajmująca się projektowaniem, wdrażaniem i utrzymaniem systemów oraz narzędzi służących do monitorowania, kontrolowania i automatyzacji procesów przemysłowych,
- obejmuje roboty, przemysłowe systemy sterowania (ICS), systemy nadzoru i gromadzenia danych (SCADA), programowalne sterowniki logiczne (PLC), obrabiarki sterowanie numeryczne (CNC), urządzenia do zdalnego sterowania (RTU), interfejsy człowiek-maszyna (HMI), czujniki, elementy wykonawcze, ...
- zapewnia monitorowanie i kontrolę procesów przemysłowych w celu uzyskania optymalnej wydajności.



IT vs. OT

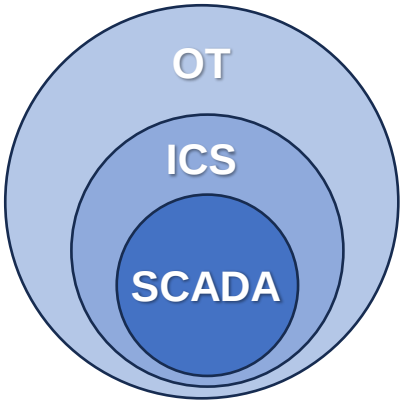
Porównanie IT i OT		
kryterium	**Sieć informatyczna IT**	**Przemysłowa sieć OT**
cel	bezpieczne zarządzanie komputerami, danymi i system komunikacji	utrzymanie działanie firmy 24/7
odpowiedzialność	przepływ danych w przedsiębiorstwie	wyposażenie obiektów przemysłowych
bezpieczeństwo	uwierzytelnianie użytkowników w sieci	kontrola fizycznego dostępu do urządzeń
konsekwencje awarii	może ale nie musi wpływać na działalność biznesową (w zależności od branży)	bezpośredni wpływ na działalność biznesową
aktualizacje sieci (oprogramowanie lub sprzęt)	wymaga przerw w pracy, wpływ można złagodzić	tylko w okresach konserwacji operacyjnej
podatność na zagrożenia	wysoka: wymagane jest ciągłe aktualizowanie hostów, sieć jest połączona z Internetem i wymaga ochrony	niska: sieci OT są izolowane i często korzystają z zastrzeżonych protokołów

Cisco Press, IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things

ICS

ICS (ang. Industrial Control System)

przemysłowe systemy sterowania, systemy używane do monitorowania i sterowania procesami przemysłowymi



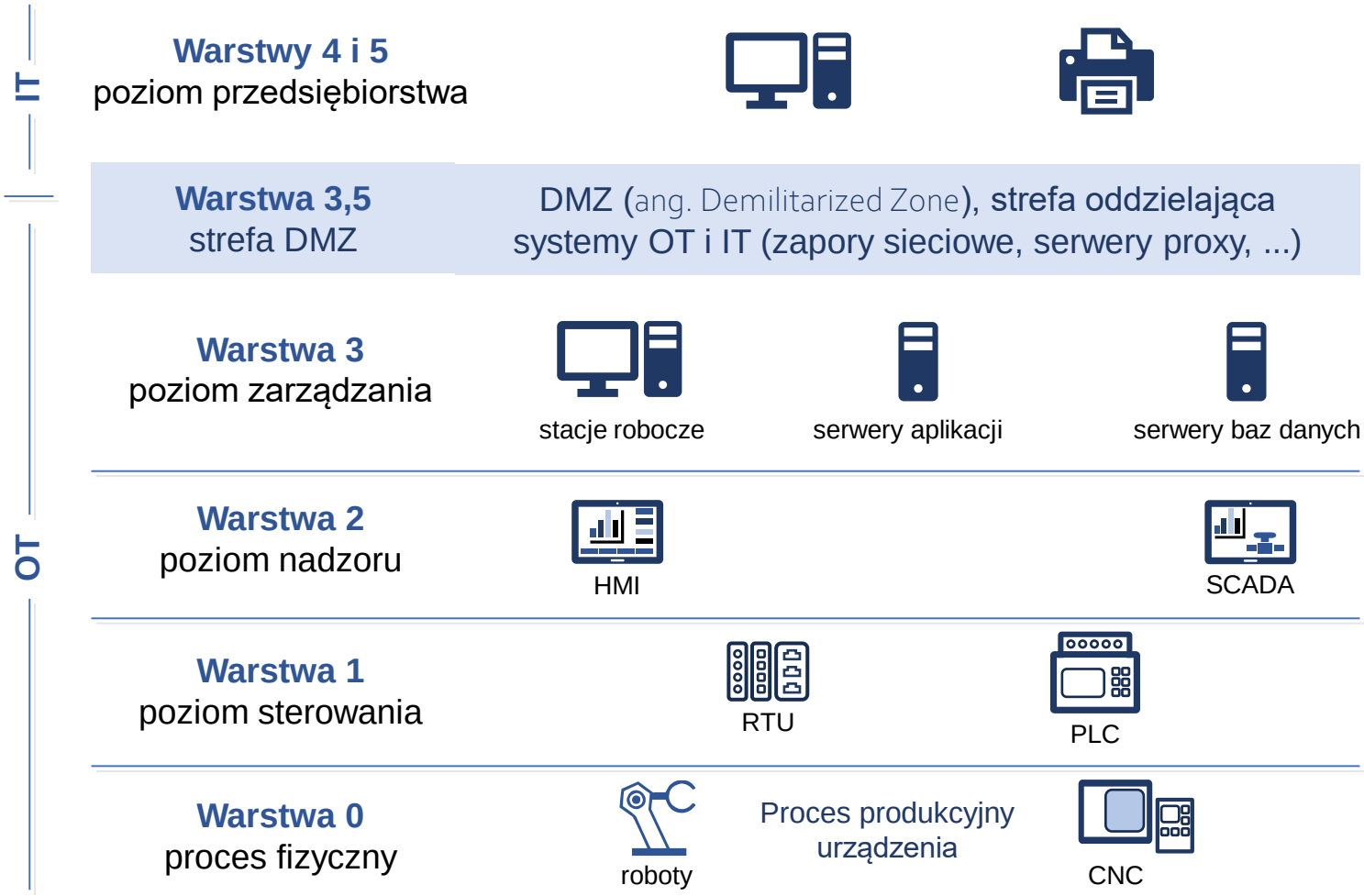
SCADA (ang. Supervisory Control and Data Acquisition)

system informatyczny (oprogramowanie + sprzęt) umożliwiający kontrolowanie i monitorowanie procesów przemysłowych, elementy sprzętowe systemu to:

- sprzęt fizyczny (urządzenia mające bezpośredni kontakt ze sterowanym procesem, zawory, pompy, czujniki, siłowniki, ...),
- urządzenia sterujące: kontrolery PLC (ang. Programmable Logic Controller) i RTU (ang. Remote Terminal Unit), realizują sterowanie i zbierają dane,
- komputery i panele HMI (ang. Human-Machine Interface), zbierają, analizują dane, wyświetlają informacje o procesie, pozwalają na zmianę przebiegu procesu,
- system komunikacyjny (sieć przewodowa, bezprzewodowa).

Model Purdue (ang. Purdue Reference Model)

Model architektury systemów przemysłowych opracowany w latach 90 w Purdue University (Indiana, USA) w celu ułatwienia projektowania, implementacji i zarządzania systemami przemysłowymi z uwzględnieniem ich bezpieczeństwa.



Model Purdue – wersja ENISA

Poprawiony model opracowany przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa ENISA (ang. European Union Agency for Cybersecurity) w celu uwzględnienia urządzeń Przemysłowego Internetu Rzeczy IIoT (ang. Industrial Internet of Things).

IT

Warstwy 4 i 5
poziom przedsiębiorstwa


OT

Warstwa 3,5
strefa DMZ

Warstwa 3
poziom zarządzania


platforma IIoT


stacje robocze


serwery

Warstwa 2
poziom nadzoru


RTU


PLC


HMI


SCADA

Warstwa 1
poziom IIoT


czujniki i el. wyk. IIoT

Warstwa 0
proces fizyczny


roboty

Proces produkcyjny
urządzenia


CNC

7	warstwa aplikacji	HTTP/HTTPS, SMTP, IMAP, FTP (TELNET, DNS, DHCP, ...)
6	warstwa prezentacji	TLS, SSL, SSH
5	warstwa sesji	PAP, PPTP, RTCP
4	warstwa transportowa	TCP, UDP
3	warstwa sieciowa	ICMP, IPv4, IPv6
2	warstwa łącza danych	ARP, Ethernet (IEEE 802.3), FDDI, IEEE 802.11, I^2C (IIC), UART
1	warstwa fizyczna	Bluetooth, DSL, Ethernet, GSM, RF link, USB, WiFi

Protokoły i standardy komunikacyjne

Protokoły komunikacyjne, pakiety protokołów

Protokół komunikacyjny

system reguł, który określa sposób przesyłania informacji pomiędzy kilkoma jednostkami systemu komunikacyjnego poprzez zmianę pewnej wielkości fizycznej; protokół określa składnię, semantykę i synchronizację komunikacji oraz metody usuwania błędów; może być implementowany za pomocą sprzętu, oprogramowania lub ich kombinacji.

Pakiet protokołów, stos protokołów (ang. protocol suite, protocol stack)

koncepcja używana przy projektowaniu protokołów komunikacyjnych; zestaw protokołów zapewniających połączenie pomiędzy kilkoma jednostkami systemu; poszczególne protokoły zestawu są projektowane do realizacji ściśle określonych funkcji, protokoły na wyższych warstwach stosu dodają dodatkowe funkcjonalności (modularyzacja ułatwia implementację nowych funkcji).

Formalnie: pakiet protokołów to definicja zestawu, a stos jest jego implementacją.

Port protokołu

liczba określająca w sposób unikalny specyficzne procesy/usługi wymiany danych.

Protokoły komunikacyjne w warstwach modelu OSI

7	warstwa aplikacji	HTTP/HTTPS, SMTP, IMAP, FTP (TELNET, DNS, DHCP, …)
6	warstwa prezentacji	TLS, SSL, SSH
5	warstwa sesji	PAP, PPTP, RTCP
4	warstwa transportowa	TCP, UDP
3	warstwa sieciowa	ICMP, IPv4, IPv6
2	warstwa łącza danych	ARP, Ethernet (IEEE 802.3), FDDI, IEEE 802.11, I^2C (IIC), UART
1	warstwa fizyczna	Bluetooth, DSL, Ethernet, GSM, RF link, USB, WiFi

HTTP/HTTPS - Hypertext Transfer Protocol (Secure)
SMTP - Simple Mail Transfer Protocol
IMAP - Internet Message Access Protocol
FTP - File Transfer Protocol

TLS - Transport Layer Security
SSL - Secure Sockets Layer
SSH - Secure Shell

PAP - Password Authentication Protocol
PPTP - Point-to-Point Tunneling Protocol
RTCP - Real-time Transport Control Protocol

TCP - Transmission Control Protocol
UDP - User Datagram Protocol

ICMP - Internet Control Message Protocol
IPv4/IPv6 - Internet Protocol (v.4/v.6)

ARP - Address Resolution Protocol
FDDI - Fiber Distributed Data Interface
I2C - Inter-Integrated Circuit
UART - Universal Asynchronous Receiver-Transmitter

https://osi-model.com/

TCP – protokół kontroli transmisji

Protokół kontroli transmisji (ang. TCP – Transmission Control Protocol)

zapewnia usługę komunikacji na poziomie pośrednim pomiędzy aplikacją a protokołem internetowym (IP); gwarantuje wyższym warstwom komunikacyjnym dostarczenie wszystkich pakietów w całości, bez błędów i duplikatów z zachowaniem kolejności; TCP i IP tworzą pakiet (stos) TCP/IP.

Cechy protokołu TCP

- ustanawia połączenie pomiędzy jednostkami przed rozpoczęciem transmisji danych,
- wykrywa zduplikowane i utracone pakiety IP,
- przeprowadza detekcję błędów w odebranych pakietach IP (sumy kontrolne),
- jeżeli jest to konieczne żąda retransmisji danych,
- porządkuje pakiety i przekazuje do warstwy wyższej odtworzony strumień danych.

Protokół TCP jest zoptymalizowany pod kątem dokładnego dostarczania danych i może powodować duże opóźnienia (rzędu sekund) podczas oczekiwania na wiadomości o nieodpowiedniej kolejności lub retransmisje utraconych wiadomości.

UDP – protokół pakietów użytkownika

Protokół pakietów użytkownika (ang. UDP – User Datagram Protocol)

zapewnia usługę komunikacji na poziomie pośrednim pomiędzy aplikacją a protokołem internetowym (IP); nie zapewnia mechanizmów kontroli przesyłanych danych (datagramów) i nie gwarantuje wyższym warstwom komunikacyjnym dostarczenia wszystkich pakietów, bez duplikatów z zachowaniem kolejności.

Cechy protokołu UDP

- wykorzystuje prosty model komunikacji bezpołączeniowej z minimalną liczbą mechanizmów połączenia,
- nie zawiera mechanizmów detekcji błędów i retransmisji danych (nie gwarantuje dostawy i ochrony przed duplikacją),
- jest wrażliwy na zawodność podstawowej sieci.

Protokół UDP eliminuje narzuty czasowe związane z kontrola poprawności, jest zoptymalizowany pod kątem szybkości przesyłania danych, wykorzystywany głównie w systemach zorientowanych na przesyłanie krótkich komunikatów, w których priorytetem jest czas odebrania pakietu.

Standardy transmisji szeregowej

Transmisja szeregowa

rodzaj cyfrowej transmisji danych, podczas której bity informacji są przesyłane kolejno po sobie wraz z dodatkowym sygnałem pozwalającym na kontrolę przebiegu transmisji.

Przykłady transmisji szeregowej: RS-232, I^2C, USB, Ethernet, CAN, Serial ATA, PCI.

RS-232, EIA-232 (ang. Recommended Standard 232, Electronic Industries Association 232)

standard szeregowej transmisji danych (rok 1960), zaprojektowany do komunikacji z urządzeniami lokalnymi; obsługuje jedno urządzenie transmisyjne (DCE) i jedno końcowe (DTE); powszechnie używany w systemach przemysłowych; zasięg 30-60m (tr. asynchroniczna), lub 15m (tr. synchroniczna), transmisja do 20kb/s.

RS-422, EIA-422 (1975 r.)

wykorzystuje różnicową linię symetryczną (mniejsza podatność na zakłócenia); transmisja 10Mb/s do 12m, 90kb/s do 1200m; jeden sterownik i max. 10 odbiorników.

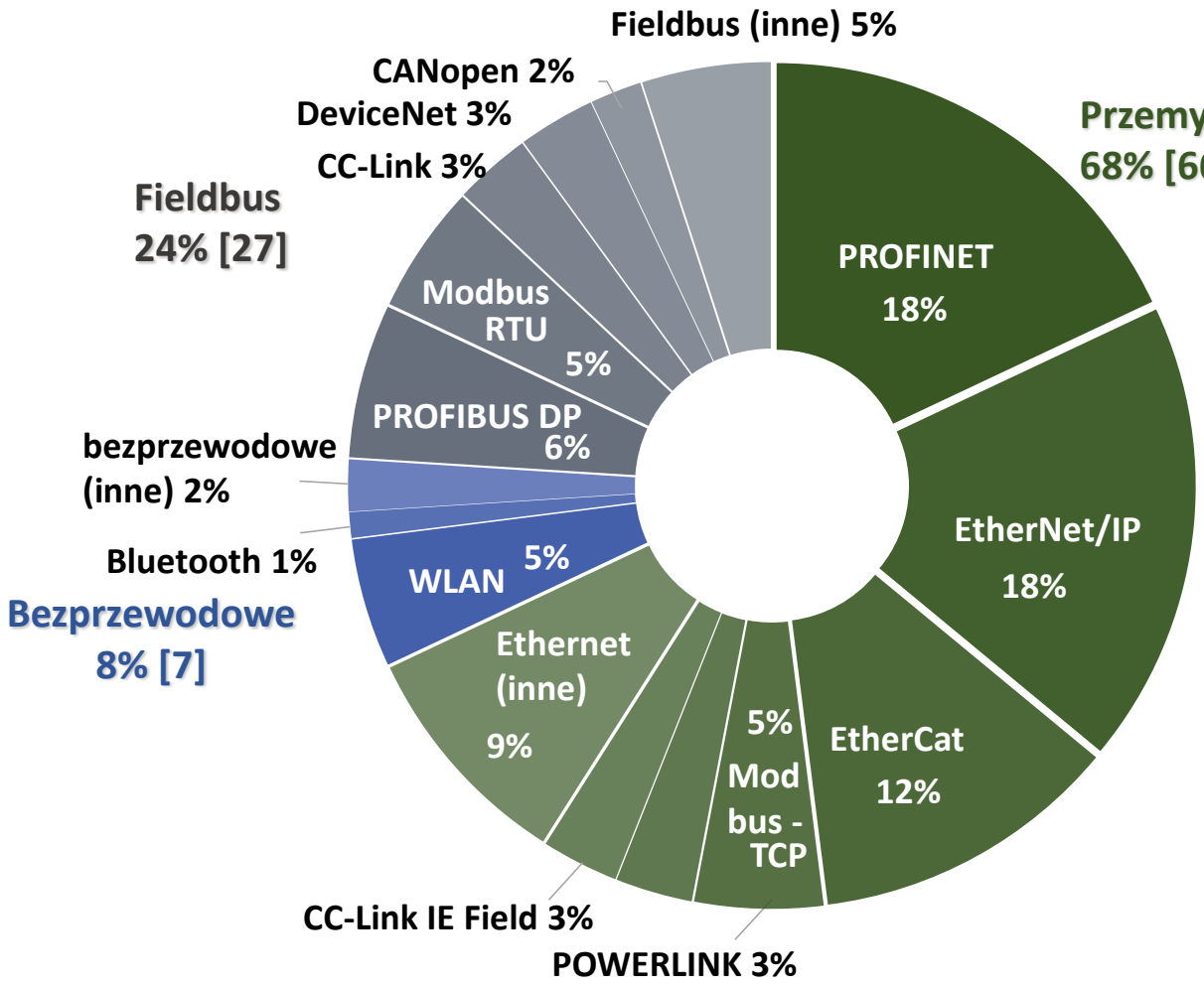
RS-485, EIA-485 (1983 r.)

korzysta z rozwiązań RS-422 (linia różnicowa); spełnia wymagania pełnej sieci wielodostępowej, obsługuje do 32 nadajników i 32 odbiorników.

EtherNet/IP

Protokoły automatyki przemysłowej

Rynek sieci przemysłowych 2023



Największy udział

Ethernet przemysłowy
(68% nowo łączonych węzłów, 66% w roku 2022)

Różnice regionalne (max)

- **Europa**
  EtherNet/IP, PROFINET, EtherCAT
- **Bliski Wschód**
  PROFIBUS, ModbusTCP
- **USA**
  EtherNet/IP, EtherCAT

HMS Networks, Industrial network market shares 2023, https://www.hms-networks.com/

Fieldbus

Fieldbus

rodzina przemysłowych cyfrowych sieci komunikacyjnych wykorzystywanych do rozproszonego sterowania w czasie rzeczywistym, opisane przez normę IEC 61784/61158.

Cechy fieldbus

- zapewnia deterministyczną komunikację, tzn. czas transmisji jest przewidywalny i kontrolowany,
- wykorzystywany głównie na poziomie bezpośredniego sterowania do połączenia urządzeń sterujących z komponentami instalacji przemysłowej,
- pozwala na wykorzystanie sieci o topologiach magistrala, gwiazda, pierścień, drzewo.

Współcześnie fieldbus jest zastępowany przez nowe rozwiązania oparte na Ethernet czasu rzeczywistego (RTE – Real-time Ethernet).

Ethernet klasyczny vs. przemysłowy

Klasyczny Ethernet

- zoptymalizowany pod kątem przesyłu dużych ilości informacji przez wiele niezależnych urządzeń jednocześnie,
- niezawodność wymiany danych osiągana poprzez powtarzanie prób transmisji,
- czas potrzebny na dotarcie informacji do odbiorcy trudny do określenia,
- wszystkie urządzenia sieciowe równorzędne pod względem praw dostępu do łącza w warstwie fizycznej.

Przemysłowy Ethernet

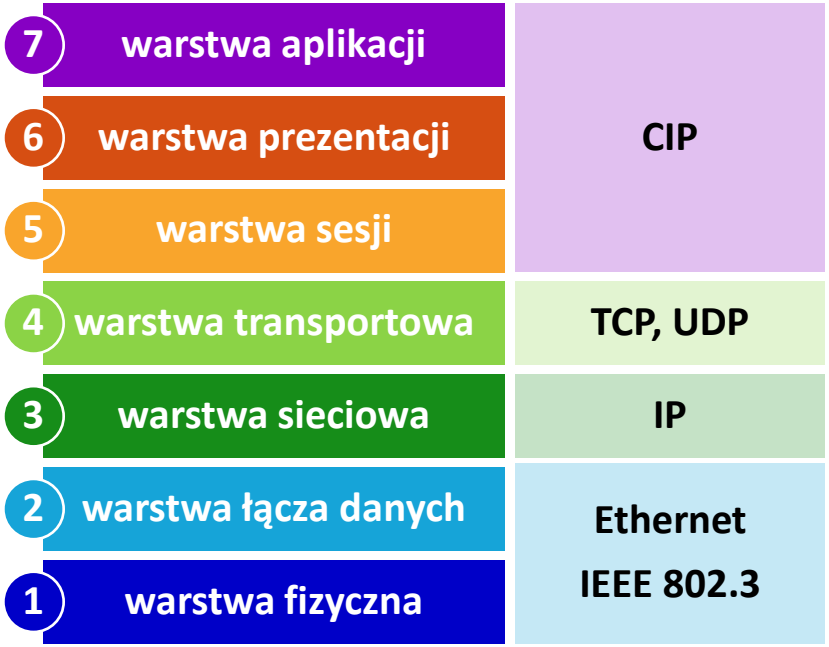
- niezawodna komunikacja pomiędzy urządzeniami przemysłowymi,
- praca w rybie rzeczywistym, szybka wymiana pakietów z kluczowymi poleceniami,
- odporność na zakłócenia i uszkodzenia sieci,
- zgodność za standardem Ethernet, urządzenia przemysłowe, czujniki, elementy wykonawcze i komputery pracują w tej samej sieci.

EtherNet/IP

EtherNet/IP (IP – Industrial Protocol)

otwarty standard dla systemów automatyki przemysłowej opracowany przez Rockwell Automation i zarządzany przez stowarzyszenie Open DeviceNet Vendors Association (ODVA); dostosowuje protokół CIP (Common Industrial Protocol) do standardowej technologii Ethernet i TCP/IP.

EtherNet/IP w modelu OSI



EtherNet/IP

Cechy EtherNet/IP

- oparty na standardzie Ethernet, pozwala na łatwą integrację urządzeń przemysłowych z istniejącą infrastrukturą sieciową opartą na kablu Ethernet,
- dwa tryby transmisji danych:
  - Explicit Messages (zwykłe pakiety i dane konfiguracyjne) przesyłane za pomocą protokołu TCP,
  - Implicit Messages (dane krytyczne czasowo) przesyłane za pomocą protokołu UDP z zapewnieniem priorytetyzacji ruchu sieciowego,
- komunikacja w czasie rzeczywistym, czasy cyklów 10-40 ms,
- stosuje standardowe komponenty sieciowe i praktyki IT,
- komunikacja (trasowanie) bez specjalnej bramy sieciowej poprzez segmenty sieciowe.

PROFINET

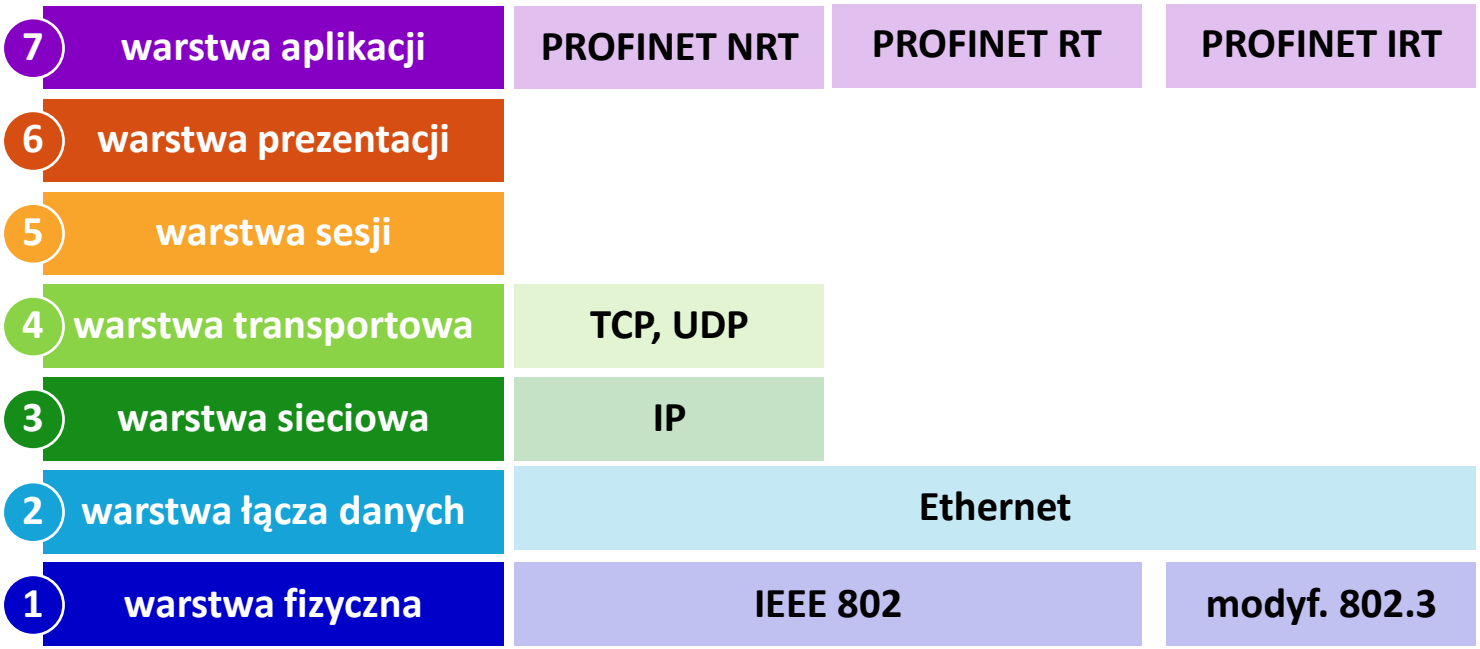
PROFINET (ang. Process Field Net)

technologia przemysłowa służąca do wymiany danych pomiędzy sterownikami i urządzeniami, opracowana przez konsorcjum Profibus International, bazująca na standardzie Profibus DP, zaprojektowana pod kątem szybkości działania.

Cechy PROFINET

- kompatybilny ze standardem IEEE 802.3 Ethernet, urządzenia PROFINET i kontrolery mogą współistnieć z urządzeniami Ethernet w tym samym segmencie sieci,
- pozwala na współistnienie komunikacji zwykłej NRT (ang. Non-Real Time) z komunikacją w czasie rzeczywistym RT (ang. Real Time) i komunikacją izochroniczną w czasie rzeczywistymi IRT (ang. Isochronous Real Time),
- pozwala na automatyczne wykrywanie topologii sieci.

PROFINET w modelu OSI



PROFINET NRT

zastosowanie: aplikacje niekrytyczne czasowo (transmisja danych do konfiguracji, monitorowania i diagnostyki), czasy cyklu < 100ms

PROFINET RT

zastosowanie: transfer danych dla aplikacji, w których czas jest krytyczny (dane procesowe), czasy cyklu < 10ms

PROFINET IRT

zastosowanie: transfer danych dla aplikacji wymagających bardzo krótkich czasów aktualizacji (kontrola ruchów), niezbędne są dedykowane urządzenia IRT, czasy cyklu < 1ms

Modbus

Modbus

otwarty protokół transmisji danych typu klient/server działający w warstwie aplikacji, opublikowany w roku 1970 przez Modicon (obecnie Schneider Electric) do komunikacji z programowalnymi sterownikami logicznymi (PLC); obecnie otwarty i wolny od opłat licencyjnych standard, rozwijany przez stowarzyszenie branżowe Modbus Organization Inc.

https://modbus.org/

Implementacje protokołu Modbus

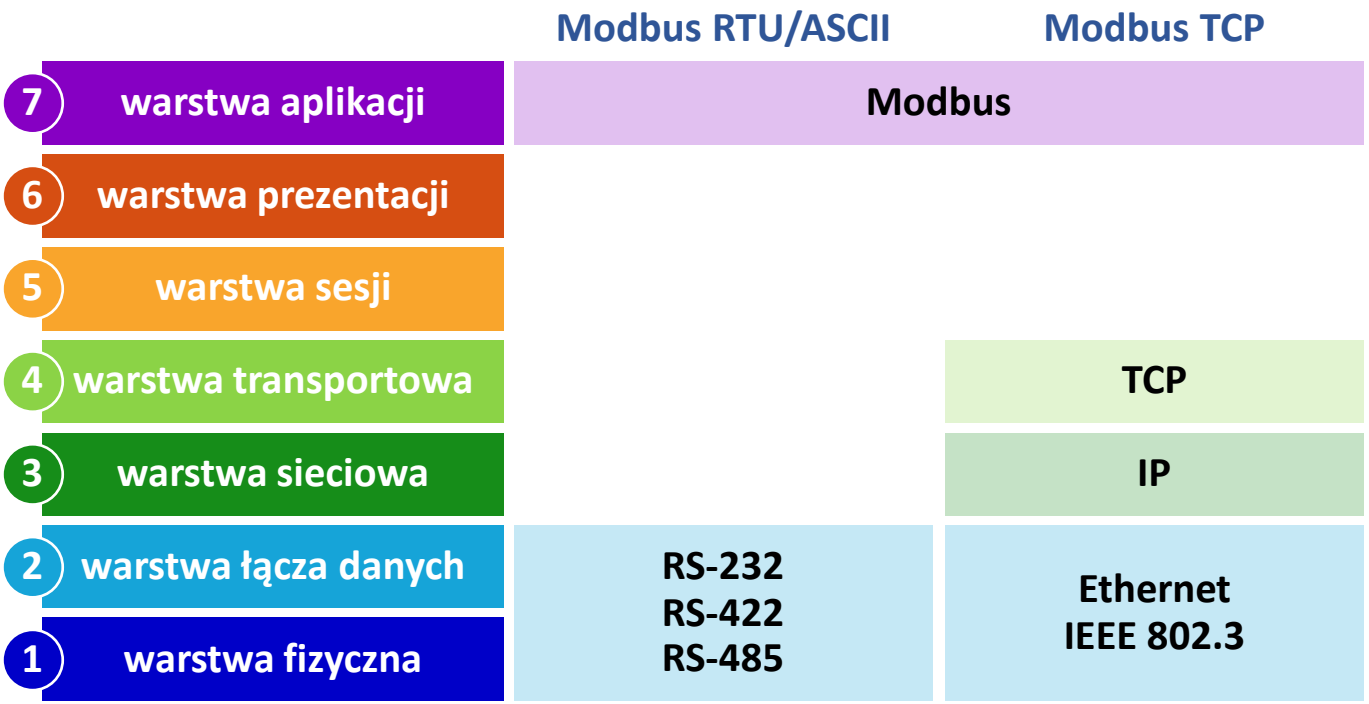
- Modbus z transmisją szeregową (RS-232, RS-422, RS-483,…)

  protokół typu master-slave, obsługuje jedno urządzenie typu master (pełni rolę klienta) i wiele urządzeń slave (pełnią rolę serwerów), obejmuje:

  - Modbus RTU – wykorzystuje binarną reprezentację danych,
  - Modbus ASCII – dane reprezentowane przez kody ASCII przesyłane jako dwubitowe wartości szesnastkowe,

- Modbus TCP – wykorzystuje sieci TCP/IP jako warstwę transportową.

Modbus w modelu OSI



Modbus

Ograniczenia Modbus

- dostępne typy danych ograniczone do używanych przez PLC w latach 70-tych,
- brak mechanizmu obsługi zdarzeń (klient musi odpytywać każde urządzenie i szukać zmian w danych – pochłania przepustowość i czas sieci), nie dotyczy TCP/IP,
- może zaadresować maksymalnie 247 urządzeń slave, nie dotyczy TCP/IP,
- nie zapewnia zabezpieczeń (przejęcie , nieautoryzowane połączenie).

Cechy Modbus TCP

- spełnia podstawowe wymogi transferu w czasie rzeczywistym (czasy ok.100 ms),
- wykorzystuje standardowe komponenty sieciowe i praktyki IT,
- radzi sobie z opóźnieniem występującymi w połączeniach modemowych lub sieciach bezprzewodowych (cecha wyróżniająca),
- umożliwia niezawodne sterowanie i monitorowanie urządzeń oraz rejestrację danych w trybie zdalnym.