SY486K MICS Lecture 8

Other ICS Protocols

CDR Brien Croteau, USNA Cyber Science Department, March 2023

Outline

- Modbus TCP
- CIP
- EtherNet/IP
- DNP3
- HART
- BACNet
- OPC
- Profinet

Distributed Network Protocol

Modbus TCP

Modbus was originally developed to send data over serial lines.

It was later adapted to work over TCP-based devices.

It still uses the same quad address space layout and Function Codes.

Since Modbus TCP is based on reliable connection service, the CRC check code in RTU protocol is no longer needed, so there is no CRC check code in Modbus TCP protocol.

Object type	Access	Size	Address Space
Coil	Read-write	1 bit	00001 – 09999
Discrete input	Read-only	1 bit	10001 – 19999
Input register	Read-only	16 bits	30001 – 39999
Holding register	Read-write	16 bits	40001 – 49999

Modbus TCP frame format

Primarily used on Ethernet networks.

Name	Length (bytes)	Function
Transaction identifier	2	For synchronization between messages of server and client
Protocol identifier	2	0 for Modbus/TCP
Length field	2	Number of remaining bytes in this frame
Unit identifier	1	Server address (255 if not used)
Function code	1	Function codes as in other variants
Data bytes	*n*	Data as response or commands

Function type			Function name	Function code
Data Access	Bit access	Physical Discrete Inputs	**Read Discrete Inputs**	2
		Internal Bits or Physical Coils	**Read Coils**	1
			Write Single Coil	5
			Write Multiple Coils	15
	16-bit access	Physical Input Registers	**Read Input Registers**	4
		Internal Registers or Physical Output Registers	**Read Multiple Holding Registers**	3
			Write Single Holding Register	6
			Write Multiple Holding Registers	16
			Read/Write Multiple Registers	23
			Mask Write Register	22
			Read FIFO Queue	24
	File Record Access		Read File Record	20
			Write File Record	21

Common Industrial Protocol (CIP)

CIP is a comprehensive suite of messages and services for industrial automation applications. CIP provides a unified communication architecture throughout the manufacturing enterprise.

Was previously known as Control and Information Protocol.

- EtherNet/IP
- DeviceNet
- CompoNet
- ControlNet

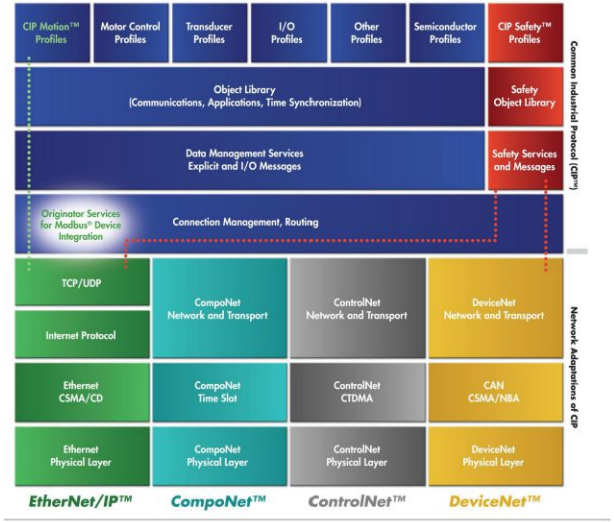
Founded in 1995, ODVA is a global association whose members comprise the world's leading automation companies. ODVA's mission is to advance open, interoperable information and communication technologies in industrial automation. ODVA recognizes its media independent network protocol, the Common Industrial Protocol or "CIP" and the network adaptations of CIP as its core technology and the primary common interest of its membership.

https://www.odva.org/wp-content/uploads/2020/06/PUB00123R1_Common-Industrial_Protocol_and_Family_of_CIP_Networks.pdf

The Common Industrial Protocol (CIP™) and the Family of CIP Networks

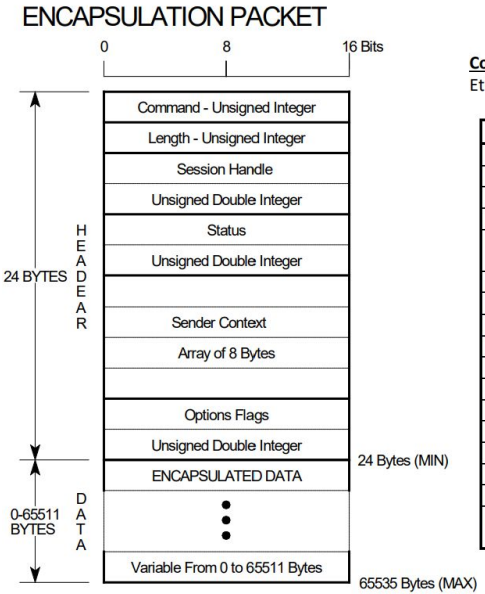
Publication Number: PUB00123R1

ODVA, Inc.
Ann Arbor, MI, USA
TEL 1-734-975-8840
FAX 1-734-922-0027
WEB www.odva.org



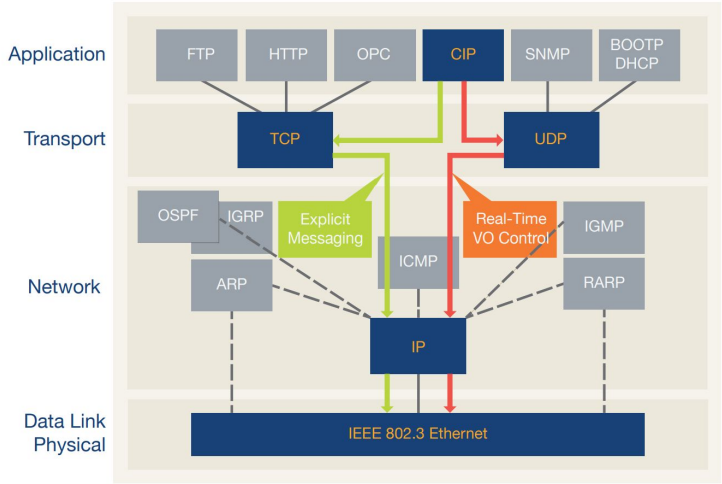
EtherNet/IP (IP = Industrial Protocol)

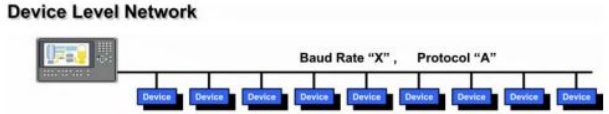
An industrial network protocol that adapts the Common Industrial Protocol (CIP) to standard Ethernet.

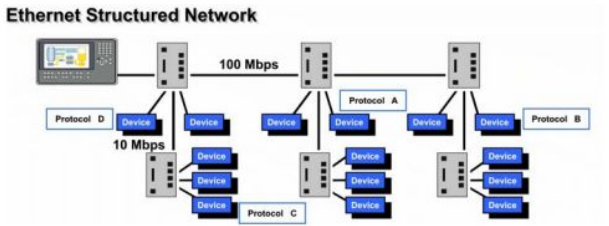


Command (2 Bytes) – This is the encapsulation command code (refer to the EtherNet/IP Specification for detailed information on commands):

CODE (HEX)	DESCRIPTION
0000H	NOP (No operation) – Sent only via TCP.
0001..0003H	*Reserved for legacy*
0004H	List_Services - May be sent via TCP or UDP
0005H	*Reserved for legacy*
0006..0062H	*Reserved for future expansion – compliant products may not use command codes in this range.*
0063H	List_Identity – May be sent via TCP or UDP.
0064H	List_Interfaces (optional) - May be sent via TCP or UDP.
0065H	Register_Session – Sent only via TCP.
0066H	UnRegister_Session – Sent only via TCP.
0067..006EH	*Reserved for legacy*
006FH	SendRRData – Sent only via TCP.
0070H	SendUnitData – Sent only via TCP.
0071H	*Reserved for legacy*
0072H	Indicate_Status (optional) – Sent only via TCP.
0073H	Cancel (optional) – Sent only via TCP.
0074..00C7H	*Reserved for legacy*
00C8..FFFFH	*Reserved for future expansion – compliant products may not use command codes in this range.*



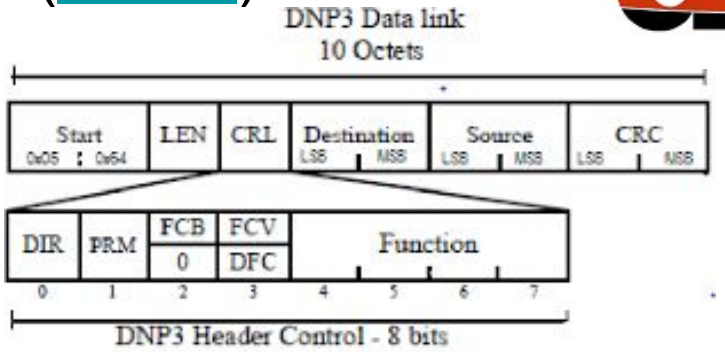


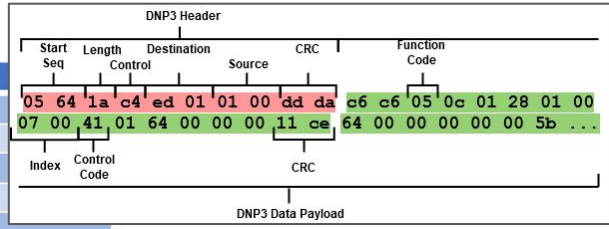


Distributed Network Protocol 3 (DNP3)

A set of communications protocols used between components in process automation systems. It is primarily used for between a master station and RTUs or IEDs in Power Grid applications.

A part of IEC 60870-6.
DNP3 is used between central master stations and distributed remote units.
DNP3 is based on an object model and uses 27 basic function codes.





Function Code	Function Code Description
0x00	Confirm Function Code
0x01	Read Function Code
0x02	Write Function Code
0x03	Select Function Code
0x04	Operate Function Code
0x05	Direct Operate Function Code
0x0d	Cold Restart Function Code
0x0e	Warm Restart Function Code
0x12	Stop Application Function Code
0x1b	Delete File Function Code
0x81	Response Function Code
0x82	Unsolicited Response Function Code

HART (Highway Addressable Remote Transducer)

A hybrid analog+digital industrial automation open protocol. Its most notable advantage is that it can communicate over legacy 4–20 mA analog instrumentation current loops, sharing the pair of wires used by the analog-only host systems.

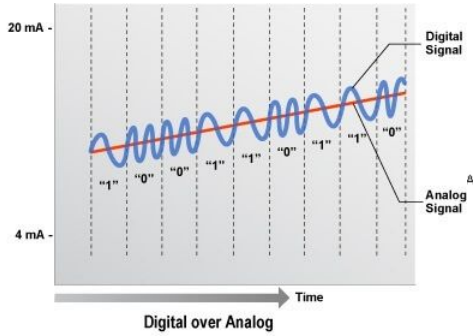
There are two main operational modes of HART instruments:

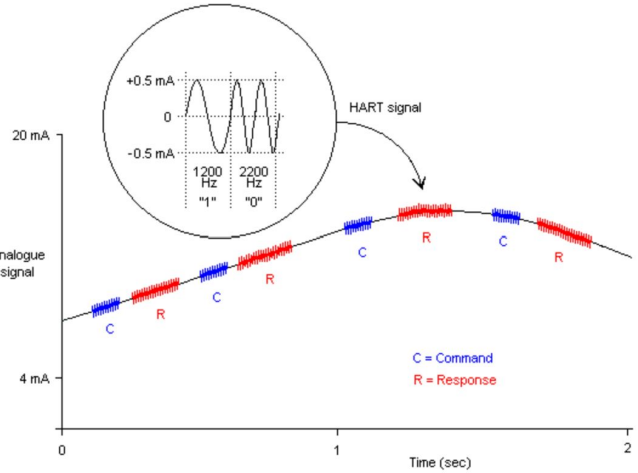
- point-to-point mode
- multi-drop mode.

Packet structure [edit]

The request HART packet has the following structure:

Field Name	Length (in bytes)	Purpose
Preamble	5–20	Synchronization and Carrier Detect
Start byte	1	Specifies Master Number
Address	1–5	Specifies slave, Specifies Master and Indicates Burst Mode
Expansion	0–3	This field is 0–3 bytes long and its length is indicated in the Delimiter (Start byte)
Command	1	Numerical Value for the command to be executed
Number of data bytes	1	Indicates the size of the Data Field
Data	0–255	Data associated with the command. BACK and ACK must contain at least two data bytes.
Checksum	1	XOR of all bytes from Start Byte to Last Byte of Data



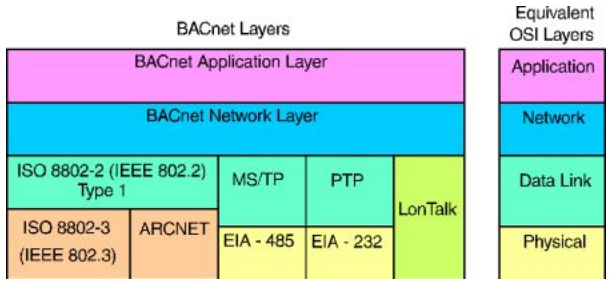


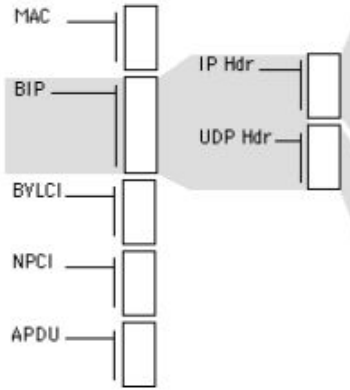
BACnet

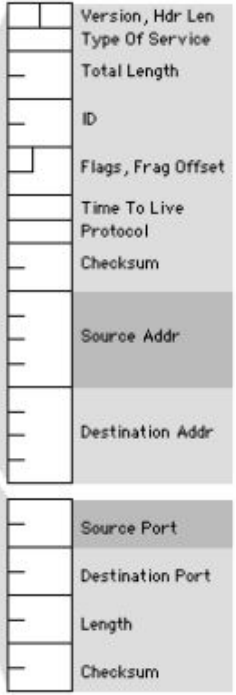
BACnet is a communication protocol for building automation and control (BAC) networks that use the ASHRAE, ANSI, and ISO 16484-5 standards protocol.

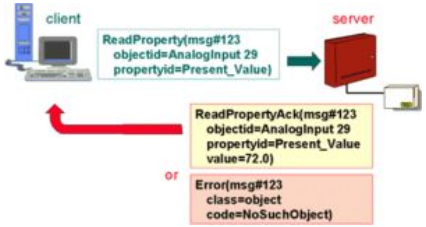
The BACnet protocol defines a number of services that are used to communicate between building devices. The protocol services include: Who-Is, I-Am, Who-Has, I-Have, which are used for Device and Object discovery. Services such as Read-Property and Write-Property are used for data sharing.

ANSI/ASHRAE 135-2016 specifies 60 standard object types





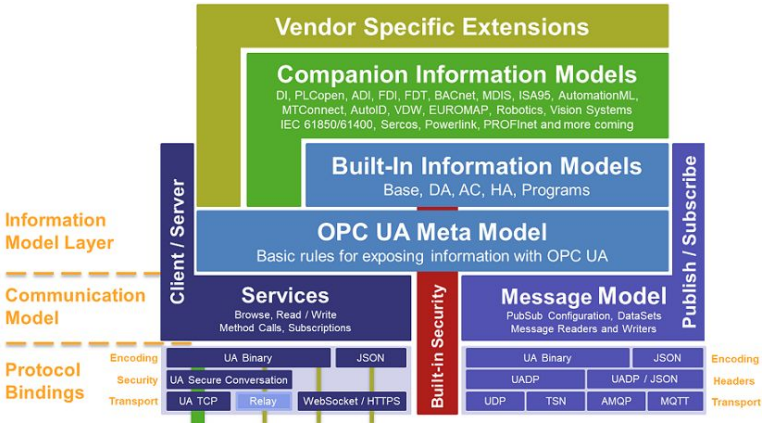


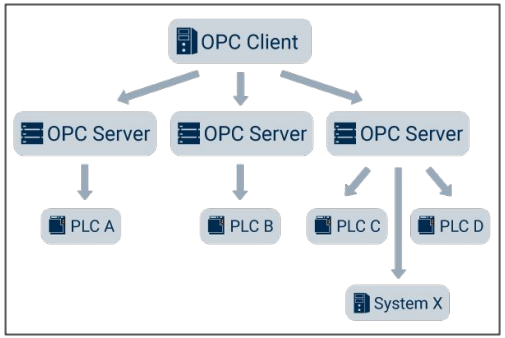


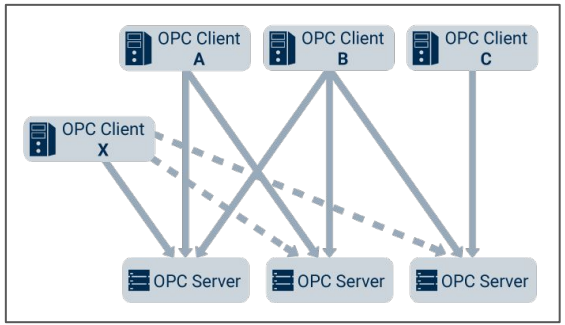
Open Platform Communications (OPC)

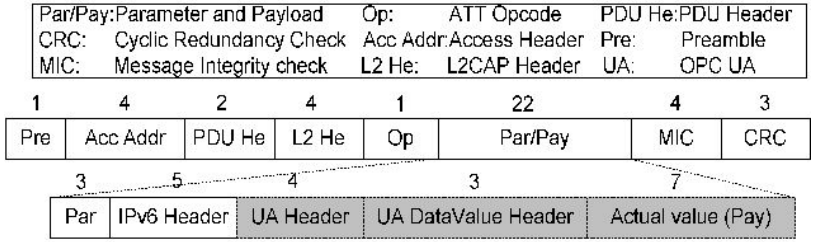
Open Platform Communications (OPC) is a series of standards and specifications for industrial telecommunication. They are based on Object Linking and Embedding (OLE) for process control. OPC specifies the communication of real-time plant data between control devices from different manufacturers.

Once an OPC Server is written for a particular device, it can be reused by any application that is able to act as an OPC client.









PROFINET

PROFINET (a portmanteau for Process Field Network) is an industry technical standard for data communication over Industrial Ethernet, designed for collecting data from, and controlling equipment in industrial systems, with a particular strength in delivering data under tight time constraints. The standard is maintained and supported by Profibus and Profinet International, an umbrella organization headquartered in Karlsruhe, Germany.