CHEATSHEET

Communication Protocols in Industrial Control System/Operational Technology

By Shiv Kataria
https://www.linkedin.com/in/shivkataria/

ICS/OT Protocol Cheat sheet

Common ICS Protocols

Protocol	Description	Serial/Ethernet	Port Number
IEC 60870-5-101	Used for communication between electrical power systems and devices for telecontrol and tele-protection.	Serial	NA works on RS-232, RS-485, or RS-422
IEC 60870-5-104	Used for communication between electrical power systems and devices for telecontrol and tele-protection.	Ethernet (TCP)	2404
IEC 61850	Used for communication between intelligent electronic devices (IEDs) in electrical power systems.	Ethernet (TCP)	102
OPC (OLE for Process Control)	Protocol used for communication between industrial automation systems and enterprise systems.	Ethernet (TCP)	135 *(Uses DCP/RCE in Microsoft)*
CC-Link IE	Protocol used for communication between industrial devices and enterprise networks, primarily used by Mitsubishi Electric. A token-passing protocol that operates at the Ethernet data link layer (Layer 2) using the IEEE 802.3	Ethernet (UDP)	Various
ModbusTCP	Protocol used for communication between Modbus devices over TCP/IP networks	Ethernet (TCP)	502
LonWorks	Used for communication between building automation systems and devices	Serial and Ethernet (TCP/UDP)	1628 *(for TCP/UDP)*
MQTT	Used for communication between IoT devices and enterprise systems. Lightweight messaging protocol for Internet of Things (IoT) devices	Ethernet (TCP)	1883 **(non-encrypted)**, 8883 *(TLS encrypted)*
ControlNet	Used for communication between industrial control devices, including programmable logic controllers (PLCs), primarily used by Rockwell Automation. Industrial control network for real-time applications	Ethernet	2222
KNX	Used for communication between building automation systems and devices	Serial, Ethernet (TCP/UDP)	3671 *(UDP)*
EtherCAT	Real-time Industrial Ethernet protocol used for communication between industrial automation systems and devices, primarily used by Beckhoff Automation.	Ethernet	34962
CIP (Common Industrial Protocol)	Application layer protocol for industrial automation devices, used for communication between industrial	Ethernet (TCP/UDP)	44818 *(Various others as well)*

	automation systems and devices, primarily used by Rockwell Automation.		
EIP (EthernetNet/IP)	Protocol used for communication between industrial automation systems and devices, primarily used by Rockwell Automation	Ethernet (TCP/UDP)	44818 *(TCP),* 2222 *(UDP)*
BACnet/IP	Protocol used for communication between building automation systems and devices over IP networks.	Ethernet (UDP)	47808
ADS	Communication protocol for TwinCAT automation software used for communication between industrial automation systems and devices, primarily used by Beckhoff Automation.	Ethernet (TCP/UDP)	48899 *(TCP/UDP)*
Foundation Fieldbus	Digital communication protocol for process automation used for communication between industrial automation systems and field devices	Serialbus	NA
PROFIBUS	Protocol used for communication between industrial automation systems and field devices, primarily used by Siemens	Serial	NA
DNP3	Communication protocol for SCADA systems used for communication between various types of data acquisition and control equipment in Electrical Systems.	Serial and Ethernet (TCP/UDP)	20000-20002
CODESYS	Protocol used for communication between industrial automation systems and devices, primarily used by 3S-Smart Software Solutions	Ethernet (TCP/UDP)	2455, 2456 1217 (TCP/UDP)
Profinet	Protocol used for communication between industrial automation systems and field devices, primarily used by Siemens. Has 3 different modes TCP/IP with latency >10ms, Realtime(RT) with latency 1-10ms and IRT with Latency <1ms.	Ethernet	34962 , 34963 *(UDP)*, 34964 *(TCP)*
CAN bus	Communication protocol for microcontroller-based systems in automotive and industrial applications.	Serial	NA *(non IP-based)*
HART	Protocol used for communication between smart instruments and control systems	Serial	NA *(non IP-based)*
J1939	Protocol used in heavy-duty vehicles for communication between microcontrollers	Serial	N/A *(non IP-based)*
Meter-Bus	Protocol used for communication between utility meters and data collection devices	Serial and Ethernet (TCP)	10001 *(TCP)*

NMEA 0183	Communication protocol for marine electronics, such as GPS devices.	Serial	N/A *(non IP-based)*
ISO-TSAP (Transport Service Access Point)	A protocol used for communication between systems using the OSI model. ISO-TSAP provides a layer of abstraction between the application layer and the lower layers, allowing different application-layer protocols to be used with different lower-layer protocols. ISO-TSAP is used as the transport layer for S7Comm and ICCP.	Ethernet (TCP)	TCP: 102, 104
S7Comm	Communication protocol for Siemens S7 PLCs (Programmable Logic Controllers) based on ISO-TSAP.	Ethernet	102 *(TCP)* 161 *(UDP)*
ICCP (Inter-Control Center Communications Protocol)	A protocol used for communication between control centers in electrical power grids. ICCP is based on the OSI model and includes multiple layers, including a transport layer based on TCP or TP4.	Ethernet	102, 410 *(TCP)*
OPC (OLE for Process Control)	A set of standards for communication between devices in industrial automation systems, such as sensors, PLCs, and human-machine interfaces. OPC includes multiple protocols, including OPC DA (Data Access), OPC AE (Alarms and Events), and OPC UA (Unified Architecture). OPC UA is the latest and most secure version, supporting encryption and authentication. OPC uses various transport protocols, including ISO-TSAP, TCP, and HTTP.	Ethernet (TCP)	OPC DA: 135, 137, 138, 139, 445, 4840-4843; OPC AE: 135, 137, 138, 139, 445; OPC UA: 4840-4843 *(TCP)*

Vendor specific Protocols

Protocol	Vendor	Description	Port Number
ADS	Beckhoff Automation	Protocol used for communication between industrial automation systems and devices	48898
CC-Link IE	Mitsubishi Electric	Protocol used for communication between industrial devices and enterprise networks	304
CIP	Rockwell Automation	Protocol used for communication between industrial automation systems and devices	44818
CODESYS	3S-Smart Software Solutions	Protocol used for communication between industrial automation systems and devices	2455, 2456

ControlNet	Rockwell Automation	Protocol used for communication between industrial control devices, including programmable logic controllers (PLCs)	2222
EtherCAT	Beckhoff Automation	Protocol used for communication between industrial automation systems and devices	34962
EtherNet/IP	Rockwell Automation	Protocol used for communication between industrial devices and enterprise networks	44818
PROFIBUS	Siemens	Protocol used for communication between industrial automation systems and field devices	102, 161
Profinet	Siemens	Protocol used for communication between industrial automation systems and field devices	34962, 18534
Protocol Name	**Vendor**	**Description**	**Port Number**

Data Historian Specific Protocols

Protocol	Description	Port Number
OPC	Commonly used in industrial automation to allow devices and systems to communicate with each other using a standard interface	TCP 135 and dynamic ports
SQL	Standard language used to manage relational databases, commonly used in data historians to query and store historical data	TCP 1433 or other port configured by the SQL server
ODBC	Standard interface used to access various types of databases, including SQL-based databases	N/A (uses TCP/IP and dynamic ports)
JDBC	Java-based interface used to access various types of databases, including SQL-based databases	N/A (uses TCP/IP and dynamic ports)
Modbus	Serial communications protocol commonly used in industrial automation and data acquisition systems to transmit signals from instrumentation and control devices	TCP 502 or other port configured by the Modbus server
DNP3	Protocol used in the utility industry to communicate between different types of equipment, including data historians	TCP 20000 or other port configured by the DNP3 server
Protocol	**Description**	**Port Number**
OPC	Commonly used in industrial automation to allow devices and systems to communicate with each other using a standard interface	TCP 135 and dynamic ports
SQL	Standard language used to manage relational databases, commonly used in data historians to query and store historical data	TCP 1433 or other port configured by the SQL server

Database Protocols used in ICS

Database Protocol	Default Port
Microsoft SQL Server	1433
Oracle Database	1521
MySQL	3306
PostgreSQL	5432
Redis	6379
Cassandra	9042

IT Protocols used in ICS

Protocol	Super Short Description	Default Port Number
DHCP	Automatically assigns IP addresses to devices on a network	67, 68
DHCP	Dynamic Host Configuration Protocol - Used to assign IP addresses and other network configuration information to devices on a network.	UDP 67, 68
DNS	Translates domain names to IP addresses	53
FTP	File transfer protocol	21
HTTP	Web browsing protocol	80
HTTPS	Secure web browsing protocol	443
ICMP	Diagnostic protocol, also known as ping	N/A
IEEE 1588	Precise time synchronization protocol used in industrial automation systems and process control	N/A (not IP-based)
IMAP	Receives email over the network	143
JDBC	Protocol used for accessing databases, similar to ODBC but for Java-based applications	N/A
Kerberos	Secure authentication protocol	88
LDAP	Accesses and maintains distributed directory information services	389
LLDP	Link Layer Discovery Protocol - Used to advertise and discover network devices and their capabilities.	Ethernet
LLMNR	Link-Local Multicast Name Resolution - Used for name resolution on local networks when DNS is not available.	UDP 5355
NTP	Synchronizes clocks between devices	123
ODBC	Protocol used for accessing databases	N/A

OPC UA	Protocol used for communication between industrial automation systems and enterprise systems, including for data acquisition and database synchronization	4840
POP3	Receives email over the network	110
PTP	Precise time synchronization protocol used in industrial automation systems and process control	N/A (not IP-based)
RDP	Remote desktop access protocol	3389
SFTP	Secure file transfer protocol	22
SMB	File and printer sharing protocol	139, 445
SMTP	Sends email over the network	25
SNMP	Simple Network Management Protocol - Used to manage and monitor network devices, including routers, switches, and servers.	UDP 161, 162
SNTP	Protocol used for time synchronization in networked environments	123
SSH	Secure remote access protocol	22
SSL/TLS	Secure communication protocol used for encrypting data transmitted via HTTP, SMTP, FTP, and other protocols	N/A
TCP/IP	Network communication protocol	N/A
DHCP	Automatically assigns IP addresses to devices on a network	67, 68
DHCP	Dynamic Host Configuration Protocol - Used to assign IP addresses and other network configuration information to devices on a network.	UDP 67, 68
DNS	Translates domain names to IP addresses	53
FTP	File transfer protocol	21