Review of Industrial Control Systems Protocols

Alexandru Cruceru, Lars Wüstrich* and Patrick Sattler*
*Chair of Network Architectures and Services, Department of Informatics
Technical University of Munich, Germany
Email: ge54dov@mytum.de, wuestrich@net.in.tum.de, sattler@net.in.tum.de

***Abstract*—This paper provides an overview of the actual state of the art of industrial control systems protocols. ICS protocols are data transfer protocols used for the communication between devices working in an industrial control system. The protocols are classified based on two criteria: whether a protocol is vendor-specific or not and regarding the industrial sector in which the protocol is used. The paper also presents in more detail the characteristics and the design features of some popular ICS protocols.**

***Index Terms*—industrial control system (ICS), ICS protocol, process automation, building automation, power-grid automation, meter-reading automation**

1. Introduction

Industrial Control Systems (ICS) are nowadays a highly important component of large-scale producing companies and factories, from manufacturing lines and building automation to power grids, water treatment facilities, and transportation systems. Critical infrastructure, on which the comfort and wellbeing of entire cities or regions rely, is dependent on such systems which must operate with high precision and performance for keeping up to the requirements needed in such industrial fields.

ICS are in use for over forty years but have evolved and changed due to the growing requirements. The basic tasks of ICS are to gather information from remote sensors, to evaluate the collected data, to give commands to the singular components (e.g. valve, pump, turbine, burner, industrial machine) of the system, and to provide a Human-Machine Interface. As these systems grew larger and larger and as the requirements became more complex, remote access to ICS through the internet became a must. Thus, there were developed industrial systems, which work with wired and wireless connectivity using Ethernet, Routing, and IP.

The interconnectivity and communication between ICS devices are represented as an industrial network that has, in general, other performance goals than usual network systems used for Internet communication. Reliability and real-time operations are critical in such industrial networks, low bandwidth and latency have to be aimed so that data availability is a high standard. [1] Therefore, serial connection and specialized protocols focusing on specific functionality stood at the core of ICS for a long period, Ethernet being later introduced as a need to integrate ICS to the Internet. Migration towards Ethernet and IP exposed ICS design vulnerabilities. The focus on time performance pushed aside data integrity and confidentiality.

The present article discusses the ICS protocols, offering classification, and exemplification in detail. The structure of the present article is: Chapter two presents an overview of the existing ICS protocols; Chapter three focuses on a detailed description of four ICS protocols; and the last part presents the conclusion of the article.

2. Overview of the existing ICS Protocols

ICS protocols have a long history. They have been deployed starting with the first ICS devices more than over forty years ago. ICS protocols were designed to work with serial communication and with high real-time performance. Since ICS devices are used in various industrial fields, a variety of specialized ICS protocols have been developed. While certain protocols are specialized only for an industrial sector, other protocols can be implemented in more than one field.

This paper focuses on two ICS protocol classification criteria: (1) vendor-specific or widely used ICS protocols; (2) industrial sector based.

TABLE 1: ICS Protocol Classification

Protocol	Vendor-specific	Sector
Modbus	No	PA
HART-IP	No	PA
Profinet/Profibus	No	PA
FOUNDATION Fieldbus	No	PA
EtherCAT	No	PA
EtherNet/IP	No	PA
CIP	No	PA
Siemens S7	Yes	PA
Sinec H1	Yes	PA
FINS Omron	Yes	PA
DNP3	No	PA/PGA
ICCP	No	PGA
BACnet	No	BA
Niagara Tridium Fox	Yes	BA
ANSI C12.22	No	MRA
OSGP	No	MRA/PGA

PA=Process Automation
PGA=Power Grid Automaton
BA=Building Automation
MRA=Meter Reading Automation

2.1. Vendor-specific or widely used ICS protocols

Vendor-specific ICS protocols are designed by companies that are also ICS device manufacturers. They are designed to work only with devices produced by the same

doi: 10.2313/NET-2022-07-1_06

company or to integrate devices from multiple manufacturers. Big players in the automation device market are Tridium, Omron, Siemens, Schneider Electric, and Rockwell Automation, all being also ICS protocol developers. Protocols like Niagara Tridium Fox were developed for Tridium devices, OMRON FINS for Omron devices, Siemens S7 and Sinec H1 for Siemens devices, Foxboro for Schneider Electric devices, and CISP for Rockwell Automation. [2]

Widely used ICS protocols are non-proprietary, so they can be used on devices from different manufacturers and comply with the performance standards demanded in most of the ICS. Some of these are Modbus, BACNet, HART-IP, EtherNet/IP, EtherCAT, ProfiNet/Profibus, DNP3, and ICCP.

2.2. Industrial sector based

ICS are used in various industrial sectors having specific requirements. Therefore, each ICS protocol was developed to implement use-case-specific features and to perform data transfer operations for a distinct industrial field. This paper concentrates on a classification done previously [3], to divide the ICS protocols into specific industrial fields.

2.2.1. Process Automation. Process automation is the broadest field in which ICS are used. It concerns the use of automation devices in factories and firms so that production and administration processes are controlled and monitored using a computer infrastructure. Multiple industries use process automation, like the automotive industry, chemical industry, oil refining industry, gas industry, water industry, and wastewater industry. The main benefits of process automation are to reduce personal costs and to increase productivity. Process automation consists of the integration of multiple input and output devices in a centralized system. This system is then controlled using a computer infrastructure that comes through graphical user interfaces in contact with human administrators. The input devices are sensors that measure different production parameters (e.g., temperature, pressure, volume) and the output devices are controlled units like valves, pumps, or motors that perform different tasks. These devices are connected to programmable logic controllers (PLC) which receive the data from the sensors, processes it, and then send commands to the controlled units. The PLCs are connected with each other and also with control computers that monitor and supervise the entire production process. The control computers are accessed by human operators that can coordinate the processes from here. ICS protocols are responsible for the data transfer between all these devices. There are many protocols developed for supporting this type of ICS. Widely used protocols (Modbus, FOUNDATION Fieldbus, Profibus/Profinet, CIP - with its implementations ControlNet, DeviceNet and EtherNet/IP), EtherCAT and HART-IP) and vendor-specific protocols (FINS Omron and the Siemens protocols- Siemens S7 and Sinec H1) were developed for providing data transfer between devices that work in a Process Automation ICS. DNP3 was originally developed for power grid automation but is nowadays also used for process automation.

2.2.2. Building automation. Building automation describes the automated, centralized control of the HVAC (heating, ventilation, and air conditioning), lighting, access control, and fire detection systems of a building. Building automation systems are used in both commercial buildings as well in private homes. They consist of multiple sensors and output devices, which work together with the computer infrastructure. The sensors gather information from the environment, send it to controllers which analyze the data received and give commands to the output devices. (In general, humans can also intervene through an HMI.) An example is the fire extinction system. Smoke and temperature sensors send the data to the controllers which analyze it and determine that a fire has broken out in a specific room. The controllers then stop the elevators, isolate the area where the fire is burning by closing the doors and start the watering system. Important to note is that, in general, all these devices are built by different manufacturers and use different software. Therefore, ICS protocols deal with the integration of building automation devices into one system, providing them with a standardized data transfer format. BACnet and Niagara Tridium Fox are protocols used for Building automation.

2.2.3. Power Grid Automation. Power grid automation is used to supervise and automatically control the power system using ICS devices. The protocols specialized in this sector deal with communication between different power stations and communication within one station. An automated power system has three tasks: data acquisition (the system acquires data through measuring devices and stores it), supervision (administrators and engineers analyze the data together with the computers and check if everything works as expected), and control (the computers or the operators of the system send instructions to power-system devices). One station can also receive or send the acquired data to another remote station so that outages are better monitored. The power system automation supervises the whole process, from the generation of electrical power to the delivery of it to the consumers. [4]

Protocols specialized in this industrial sector are DNP3, ICCP, and IEC 61850 and IEC 60870-5 standards.

2.2.4. Meter Reading Automation. Meter reading automation consists of automated transfer and centralized storage of data from metering devices that measure utility consumption of households, businesses, and institutions. Automated utility meters measure the use of resources and store it. They then use an ICS protocol to send the data through a network within regular time intervals to the data center of the utility provider. This data is then analyzed to check if the meter works fine and to calculate the consumption of the customer. In many situations, the customers are also provided with access to the data through the internet. The automation of meter reading has multiple benefits for both providers and consumers. The providers can reduce their personnel costs and monitor the devices remotely, and the customers can manage their consumption by having access to the consumption information. The most important protocol used for this purpose is ANSI C12.22. OSGP (Open Smart Grid Protocol) is another protocol that operates in both Meter Reading and

Power Grid automation and it is used in the deployment of electrical smart meters. [5]

3. Characteristics and Design of the most used ICS Protocols

This section includes a detailed presentation of the design and features of the frequently used ICS protocols: Modbus, ICCP, BACnet, and DNP3. The first three protocols are each representative of a different industrial sector. DNP3 is used in both process automation and power grid automation.

3.1. Modicon Communication Layer

Modicon Communication Layer (Modbus) [6] is an application layer protocol designed by Modicon (later bought by Schneider Electrics), first deployed in 1979. Modbus operates by using a master-slave architecture. There are two cases: either a Human Machine Interface (HMI) that acts as a master and multiple Programmable Logic Controllers (PLC) acting as slaves, or a PLC acting as a master having other devices, like sensors, motors, or other PLCs as slaves. Master devices can be, at the same time, slaves of other devices. The master/slave architecture is based on a request/reply methodology, where a master sends a request to the slaves and the slaves send a reply to that request. Masters can send either broadcast messages that address all slaves or individual messages that address an individual slave. The slaves cannot send a message unless they received a request that was addressed to them. [1] Modbus uses 3 distinct Protocol Data Units (PDU) for communication: Modbus Request, Modbus Response, and Modbus Exception Response. The master sends a Modbus Request at the slave including a Request PDU. The slave receives the request and responds to it either with a Data Response in the PDU if there is no error occurred, or with a Modbus Exception Response if an error occurred during the transmission. [1]

Being an Application Layer protocol, Modbus can be easily adapted to either serial or routable network protocols. RS-232 and RS-485 are used on the physical layer for serial communication. Ethernet is used on the physical layer for networked communication while IP and TCP are used as protocols for the Link and Transport Layer. In time, different variants of Modbus were developed, three of which are Modbus RTU, Modbus ASCII, and Modbus TCP. Modbus RTU and ASCII are used in asynchronous serial communication while Modbus TCP is used for routable communication. Modbus TCP has two solutions for integrating a Modbus message to the routed Internet. It either adds a Modbus Application Protocol header, which includes Link and Transport layer information to the existing serial frame keeping the original address information and error check, or it removes the original address information and error check, keeping the Modbus PDU and attaching the Modbus Application Protocol header to it. The first solution is commonly implemented in legacy devices. The second one is preferred in the implementation of modern devices. [1]

Since Modbus was designed for serial communication and time performance, it lacks some features that are important when using the Internet. Modbus has no authentication procedure and uses no encryption. It also allows, in some cases, the serial networks to be flooded with messages due to no broadcast suppression. [1]

3.2. Inter-Control Center Communication Protocol

The Inter-Control Communication Protocol (ICCP) [7] was developed by a working group founded in 1991, tasked by the International Electrotechnical Commission to create a standardized real-time data exchange protocol, which should facilitate the communication between electric power utility stations. ICCP is an application layer protocol. It was designed to support a set of data transfer operations between electric control centers. These operations are: establishing a connection with other control centers, reading and sending information from and to remote centers, configuring and controlling remote devices, and controlling programs on remote centers. [1]

The ICCP is based on a client-server architecture. The server center contains data and functions which are accessed by the client center via a request. Most of the implementations of the ICCP allow nowadays that a device is both a server and a client.

The transfer procedure of the ICCP uses a bilateral table which takes the role of an access control list. The bilateral table has the purpose of checking the access rights of the client that requests access to data or control. Therefore, it strictly defines what information is accessible to which control center. To ensure that the access rights are agreed upon by both centers, the bilateral table entry must match on both server and client. [1]

ICCP is a wide-area network protocol. Since it operates at the application layer, it can work with different transport and link-layer protocols and use different physical media. ISO transport on port 102/TCP over Ethernet is mostly used for the implementations of this protocol. [1]

Like other ICS protocols, ICCP also lacks authentication and encryption, leaving this in the hand of lower layer protocols. ICCP is highly accessible as it operates on wide-area networks, therefore it is susceptible to denial of service attacks. [1]

3.3. Building Automation and Control Networks

BACnet [8] stands for Building Automation and Control Networks, and it was first presented by the American Society for Heating, Refrigerating, and Air-Conditioning Engineers in 1987. Buildings have nowadays a lot of facilities offered by HVAC, access control, lighting control, elevator, and fire alarm devices. All these devices are produced by multiple manufacturers and thus use different operating programs and protocols. BACnet was developed for integrating all these devices into a single control system so that building owners do not have to be dependent on one manufacturer or do not have to use a different management system for every device.

BACnet uses an object-oriented model for data transfer between system devices. The Information shared between the devices is represented as a logical object. These objects are abstract constructs that are characterized by a set of

properties. They describe physical inputs, outputs, or non-physical components like software. An example for such an object would be a logical representation of a temperature measuring device which has as property the value of the measured temperature. The use of objects organizes the information and standardizes the data formats that can be transmitted. BACnet defines a set of 25 standardized object types that offer usage in a wide area of applications. It also allows the vendors to customize these objects by adding specific properties to them or to create entirely new objects. [9]

Besides the objects used for data representation, BACnet also provides standardized services. They are responsible for the interaction within the system, describing actions that can be performed by a device. BACnet provides a wide functionality through these services, grouped into the following categories: object access, alarm and event management, scheduling, trending, file configuration and transfer, and device management. [9]

BACnet offers support for a variety of network implementations. The most used ones are BACnet/Ip (which uses Ethernet and IP) and a low-cost implementation called MS/TP (Master-Slave Token Protocol) (which uses RS-485 together with twisted pair cable). MS/TP networks are used to couple devices that transmit a low volume of data, and which do not require high transfer speeds. BACnet/Ip is used for high-speed transmission of larger data blocks, providing also interface for data that has to be routed outside the current Local Area Network segment using IP. Specialized BACnet controllers and routers are responsible for organizing and controlling the infrastructure of a BACnet network.

3.4. Distributed Network Protocol

The Distributed Network Protocol (DNP3) [10] was developed by Westronic in 1990. It was designed for communication within the electric power industry, in environments with high electromagnetic interference but implemented in other industries as well. [1]

DNP3 is based on a master-slave architecture similar to Modbus. In contrast to Modbus, it allows bidirectional communication: master–slave, slave-master. In addition, DNP3 puts a high accent on reliability. To ensure reliability DNP3 uses many cyclic redundancy checks (CRC), one for the link-layer header and one for every 16 payload data bytes. If errors are identified by the receiver when checking the CRC, the message is retransmitted. Besides this, DNP3 provides an acknowledgment mechanism to prevent the loss of frames due to physical layer errors. The sender of the message requests the receiver to send a confirmation that the message was received. If no such confirmation is received by the sender, it sends the message again. These two safety mechanisms provide high reliability but also a higher overhead, a fact that represents a problem in some real-time environments. [1]

DNP3 supports multiple data types: files, counters, analog, and binary data, and other types of data objects. The data is structured into multiple data classes. Class 0 stands for static data. This data type is used for representing the current values that the supervised objects gathered, providing the master with a real-time view of the monitored system. Classes 1 to 3 stand for event data. Event data is time-stamped and prioritized, class 1 having the highest priority and class 3 the lowest. Event data represents old data stored in the buffer of a remote terminal unit (RTU). Through the time-stamp, event data offers a historical view of the system. Unsolicited reporting is another feature that DNP3 has. In contrast to Modbus, DNP3 allows slave-stations to send messages without getting a request from their masters. This feature allows slaves to send messages immediately as an event occurs and they do not have to wait for the master to request their data. Unsolicited reporting makes the system more efficient but adds overhead to the message frames. As slaves initiate communication and the master acknowledges receiving the message, the frames have to include both source and destination address. [1]

DNP3 was integrated into Internet communication by adding an IP and TCP or UDP header to the DNP3 frame. For a more secure Internet connection, Secure DNP3 was developed. This version of the protocol provides an authentication mechanism. Authentication is initiated by the receiving device. When the sender tries to access data from the receiver, the receiver requests identification of the sender before giving him access to the data. [1]

4. Conclusion

ICS and ICS protocols represent a major topic in the domain of distributed systems. Automation is an important tool in the present-day industry. Due to high product demand, productivity and efficiency become a must. Infrastructure is continuously growing and becomes more complex in order to satisfy people's needs. Without automation, the productivity of such complex systems would be low, control and monitoring nearly impossible. ICS protocols are essential components of automation, being responsible for the transfer of information between industrial devices.

ICS protocols are designed for various industries, as such a variety of such protocols exists. They can be either developed by ICS device manufacturers (to serve the devices these manufacturers build) or can be designed for the general use of any ICS devices specialized in a certain industry. The four industrial fields that use ICS protocols are Process Automation, Building Automation, Power Grid Automation, and Meter Reading Automation. Because every industry has different performance standards, protocols must be adapted to the special needs of every industry. Therefore, ICS protocols are, in general, specialized for an industrial sector, with few exceptions.

As seen in the third chapter, the design of ICS protocols differs from one protocol to another. Client-Server architecture, Master-Slave architecture, or an object-oriented methodology are three examples of design choices. In general, these protocols operate on the application layer of the ISO/OSI model and therefore are compatible with many implementations on lower layers. Ethernet and TCP/IP were added to the ICS protocols as a need to integrate the ICS devices into the Internet.

References

[1] E. Knapp and J. Langill, *Industrial Network Sekurity, 2nd Edition*. Syngress, 2014.

doi: 10.2313/NET-2022-07-1_06

[2] Dragos, "ICS & IT PROTOCL SUPORT," https://www.dragos.com/wp-content/uploads/Dragos-Supported-Protocols.pdf, 2021.

[3] A. Mirian, Z. Ma, D. Adrian, M. Tischer, T. Chuenchujit, T. Yardley, R. Berthier, J. Mason, Z. Durumeric, J. A. Halderman, and M. Bailey, "An internet-wide view of ics devices," in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, 2016, pp. 96–103.

[4] Wikimedia Foundation, "Power-system automation — Wikipedia," https://en.wikipedia.org/wiki/Power-system_automation, 20 September 2021, online, accessed on 19 December 2021.

[5] ——, "Smart meter — Wikipedia," https://en.wikipedia.org/wiki/Smart_meter, 22 November 2021, online, accessed on 19 December 2021.

[6] Modbus Org., "The Modbus Organization," https://modbus.org/, online, accessed on 19 December 2021.

[7] "Telecontrol equipment and systems - Part 6-503: Telecontrol protocols compatible with ISO standards and ITU-T recommendations - TASE.2 Services and protocol," International Electrotechnical Commission, Standard, Jul. 2014.

[8] ASHRAE, "BACnet Website," http://www.bacnet.org/index.html, online, accessed on 19 December 2021.

[9] D. Fisher and PolarSoft, "How BACnet is Changing Building Automation Networking," *The Extension. A Technical Supplement to Control Network*, vol. 8, 2007.

[10] DNP Org., "DNP.org," https://www.dnp.org/, online, accessed on 19 December 2021.

doi: 10.2313/NET-2022-07-1_06