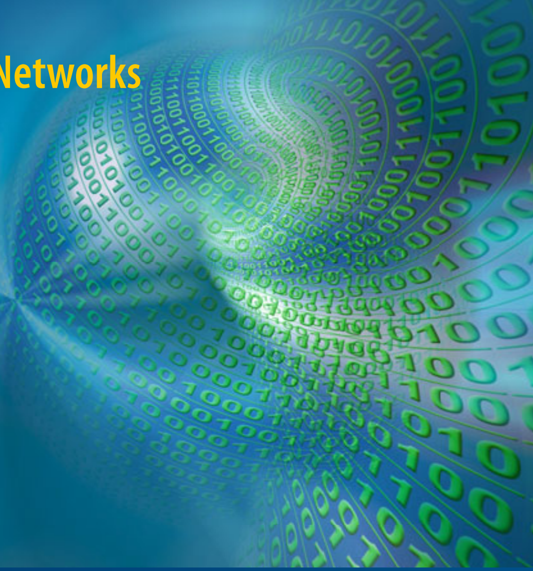
Computer Communications and Networks



Dong-Seong Kim
Hoa Tran-Dang

Industrial Sensors and Controls in Communication Networks

From Wired Technologies to Cloud Computing and the Internet of Things

Springer

Computer Communications and Networks

The **Computer Communications and Networks** series is a range of textbooks, monographs and handbooks. It sets out to provide students, researchers, and non-specialists alike with a sure grounding in current knowledge, together with comprehensible access to the latest developments in computer communications and networking.

Emphasis is placed on clear and explanatory styles that support a tutorial approach, so that even the most complex of topics is presented in a lucid and intelligible manner.

More information about this series at http://www.springer.com/series/4198

Dong-Seong Kim · Hoa Tran-Dang

Industrial Sensors and Controls in Communication Networks

From Wired Technologies to Cloud Computing and the Internet of Things

Springer

Dong-Seong Kim
Department of ICT Convergence Engineering
Kumoh National Institute of Technology
Gumi, Korea (Republic of)

Hoa Tran-Dang
Department of ICT Convergence Engineering
Kumoh National Institute of Technology
Gumi, Korea (Republic of)

ISSN 1617-7975 ISSN 2197-8433 (electronic)
Computer Communications and Networks
ISBN 978-3-030-04926-3 ISBN 978-3-030-04927-0 (eBook)
https://doi.org/10.1007/978-3-030-04927-0

Library of Congress Control Number: 2018962922

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Industrial networks have been promoted increasingly by emerging technologies such as industrial wireless communication technologies, industrial Internet of Things (IIoT), cloud computing, big data, etc. Given the increasing age of many industrial distributed systems and the dynamic industrial manufacturing market, intelligent and low-cost industrial automation systems are required to improve the productivity and efficiency of such systems. The collaborative nature of industrial wireless sensor networks (IWSNs) brings several advantages over traditional wired industrial monitoring and control systems, including self-organization, rapid deployment, flexibility, and inherent intelligent-processing capability. In this regard, IWSNs play a vital role in creating a highly reliable and self-healing industrial system that rapidly responds to real-time events with appropriate actions. At broader scale, IIoT has been recognized primarily as a solution to improve operational efficiency.

In this book, detailed reviews about the emerging and already deployed industrial sensor and control network applications and technologies are discussed and presented. In addition, technical challenges and design objectives are described. Particularly, fieldbus technologies, wireless communication technologies, network architectures, resource managements, and optimization for industrial networks are discussed. Furthermore, industrial communication standards including wired and wireless technologies and IIoT visions are presented in detail. Overall, this book covers the current state of the art in such emerging technologies and discusses future research directions in this field. The book is structured in three parts, each one grouping a number of chapters describing our state-of-the-art researches in actual domains of the technology transformation in sensing and control in future industrial networks.

Part I titled as Industrial Control Networks includes six research proposals covering the fieldbus control networks (i.e., CAN, FlexRay, Modbus). In this part, the latest fieldbus technologies are reviewed to point out the key performance and challenges of technology application in industrial domain. This challenges open potential researches to find out breakthrough solutions. One of them is described in our research proposal, which proposed to use dual fieldbus technology, CAN and

Modbus to meet the significant time delay for the distributed control system of ship engines.

Part II of the book referred as Industrial Wireless Sensor Networks includes 11 research proposals which analyze and evaluate such networks' applications in terms of wireless networking performances. Such aspect is highlighted by key points composed of medium access control (MAC) mechanisms, wireless communication standards for industrial field. In additions, applications of such networks from environmental sensing, condition monitoring, and process automation applications are specified. Designing appropriate networks are based on the specific requirements of applications. It points out the technological challenges of deploying WSNs in the industrial environment as well as proposed solutions to the issues. An extensive list of IWSN commercial solutions and service providers are provided and future trends in the field of IWSNs are summarized.

Part III named as Industrial Internet of Things mentions the state-of-the-art technologies along with accompany challenges to realize such vision. Wide applications of IIoT are summarized in industrial domains. Specially, adopting such technology to the Physical Internet, an emerging logistics paradigm is described in this part.

Gumi, Korea (Republic of)

Dong-Seong Kim
Hoa Tran-Dang

Acknowledgements

We would like to express our gratitude to the publisher, Springer, for accepting this book as part of the series “Computer Communications and Networks”. In particular, we would like to thank Scientific Publishing Services (P) Ltd. in Tamil Nadu, India for their editorial and production guidance.

Our acknowledgment goes to Prof. Pactrick Charpentier and Dr. Nicolas Krommenacker at the Research Center for Automatic Control of Nancy (CRAN), University of Lorraine, France, who contributed to the content of Chap. 18. Special thank is due to our colleague, Nguyen Bach Long at University of Newcastle, Australia, who collaborated and contributed to the content of Chap. 17.

We would like to thank the Networked System Laboratory (http://nsl.kumoh.ac.kr/), Kumoh National Institute of Technology (KIT) in Gumi, Republic of Korea, which made it possible to write this book. As one of the most educational institutions in technology, we are grateful to be part of this visionary and innovative organization.

Contents

Part I Industrial Control Networks

Part II Industrial Wireless Sensor Networks

Part III Industrial Internet of Things

Part I
Industrial Control Networks

Industrial control networks play a significant role in industrial contributed control systems since it enables all the system components to be interconnected as well as monitor and control the physical equipment in industrial environments. With the development of electronic engineering, the mechanical control system has been gradually replaced by digital control systems adopting power microprocessors and digital controllers. The movement toward such digital systems requires inherently corresponding communication technologies and communication protocols to the field as well as the controllers. Basically, the core of industrial networking consists of fieldbus protocols which are defined in the IEC standard 61158 as a digital serial, multi-drop, data bus for communication with industrial control and instrumentation devices.

Part I of this book named Industrial Control Networks includes six research proposals covering the key fieldbus control networks (i.e., CAN, FlexRay, and Modbus). In this part, such fieldbus technologies are reviewed to point out the key performance and challenges when applying such communication technologies in industrial control systems. The challenges open up potential researches to find out breakthrough solutions aiming to improve the quality of services of the systems. One of them is described in our research proposal, which proposed to use dual fieldbus technology, CAN, and Modbus to meet the significant time delay for the distributed control system of ship engines.

Chapter 1
An Overview on Industrial Control Networks

1.1 Introduction

In general, the industry can be divided into two categories: process, and manufacturing sector. The process industry deals with processes involving very large material flows in both continuous, or discontinuous manner and often has strict safety requirements (e.g., power generation, cement kilns, petrochemical production), while the manufacturing industry is concerned with the production of discrete objects. Achieving the maximum throughput of produced goods is, normally, very important aspect in such industrial sectors. Practically, the industrial systems have been required to be innovated to enhance production monitoring and quality control and in the same time maintaining the operation costs as low as possible. This innovation has happened in the last few decades due to the advancement of information and communication technologies which enable the industrial systems to match up with these needs. The innovation has led to reduce significantly manual labors replaced with a faster, and more reliable automated machine, equipment in the most of industry operations. This also provides both the factories and the manufacturing plants with necessary monitoring which they both sought for better supervisory and quality control. Introducing all this number of automated unites into the factories needed an efficient method to connect them together, to communicates with each other, and to transfer the various supervisory data to the monitors. This leads to the introduction of the communication networks into the industrial sectors.

Based on the specialized functions, the industrial networks are composed of three major control components that include Programmable Logic Controllers (PLC), Supervisory Control and Data Acquisition (SCADA), and Distributed Control Systems (DCS) [1]. PLCs are nothing but digital computers that can work in hazardous industrial environments. Such processor-based systems take inputs from data generation devices like sensors and communicate them with the entire production unit and then present the output to HMI (Human–Machine Interfaces). PLCs can control the entire manufacturing process while ensuring the required quality of services

D.-S. Kim and H. Tran-Dang, *Industrial Sensors and Controls in Communication Networks*, Computer Communications and Networks,
https://doi.org/10.1007/978-3-030-04927-0_1

(QoS) and great precision control functions. SCADA systems are mainly used for the implementation of monitoring and control system of an equipment or a plant in several industries like power plants, oil and gas refining, water and waste control, telecommunications, etc. In this system, measurements are made under field or process level in a plant by number of remote terminal units and then data are transferred to the SCADA central host computer so that more complete process or manufacturing information can be provided remotely. This system displays the received data on number of HMIs and conveys back the necessary control actions to the remote terminal units in process plant. DCS consists of a large number of local controllers in various sections of plant control area and are connected via a high-speed communication network. In DCS control system, data acquisition, and control functions are carried through a number of DCS controllers which are microprocessor-based units distributed functionally and geographically over the plant and are situated near area where control or data gathering functions being performed.

All these three elements deals with field instruments (i.e., sensors, actuators), smart field devices, supervisory control PCs, distributed I/O controllers and HMI (Human–Machine Interface). These devices are connected and communicated by a powerful and effective communication network referred to as industrial networks. In these networks, the data or control signals are transmitted either by wired or wireless media. Cables used for wired transmission of data include twisted pair, coaxial cable or fiber optics. Meanwhile, radio waves are used to transmit data in the industrial wireless networks.

1.2 Architecture of Industrial Control Networks

Generally, the industrial control networks are constructed in hierarchical topology as illustrated in Fig. 1.1 including three basic levels: informational, control, device level [2]. Each level has unique requirements that affect which network is used for that particular level.

The device level consists of field devices such as sensors and actuators of processes and machines. The task of this level is to transfer the information between these devices and technical process elements such as PLCs. The information transfer can be digital, analog, or hybrid. The measured values may stay for longer periods or over a short period. All of the devices connect to a single cable. The cable usually has conductors for power, device signal, and a shield. There are many other field level communication networks available which are characterized by different factors such as response time, message size, etc. The messages are usually small when compared to other networks. Because of deterministic and repeatability requirements, the messages can be prioritized so that the more critical information is transmitted first [3]. Nowadays, fieldbus technology is the most sophisticated communication network used in field level as it facilitates distributed control among various smart field devices and controller. These networks support Carrier-Sense Multiple

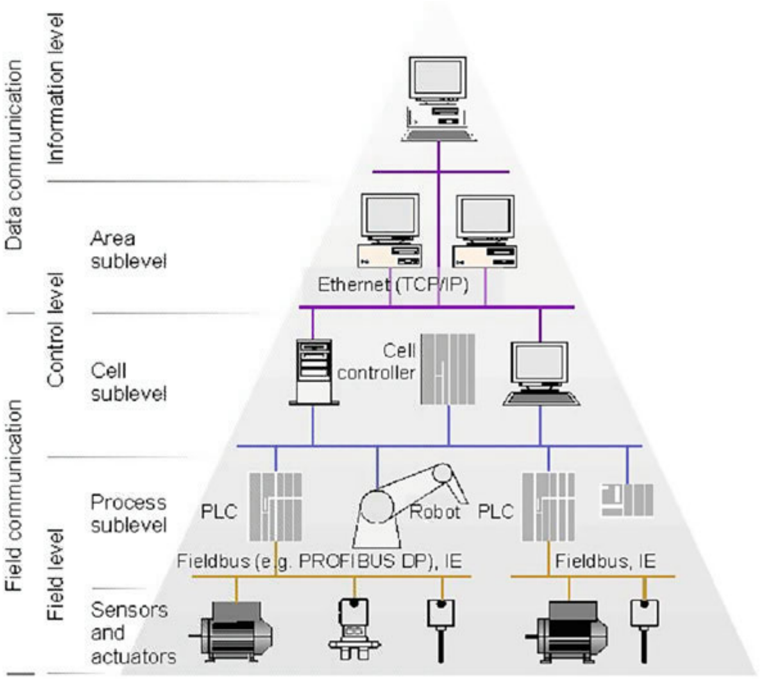


Fig. 1.1 Three-level architecture of industrial control networks

Access with Arbitration on Message Priority (CSMA/AMP) protocol for fulfilling the requirements.

The control level involves networking machines, work cells, and work areas. This is the level where Supervisory Control and Data Acquisition (SCADA) is implemented. If an automotive assembly plant is used as an example, this network level is where the individual control systems will be given information on the make, model, and options that are to be included on a vehicle so that the controllers can run the appropriate programs to assemble the vehicle correctly. Data such as cycle times, temperatures, pressures, volumes, etc., are also collected at this level [4]. The tasks of this level include configuring automation devices, loading of program data and process variables data, adjusting set variables, supervising control, displaying variables data on HMIs, historical archiving, etc. The control level of the network must achieve the predefined requirements such as deterministic, repeatable, short response time, high-speed transmission, short data lengths, machine synchronization, and constant use of critical data. Determinism is the ability to accurately predict when data will be delivered, and repeatability is the ability to ensure that transmit times are consistent and unaffected by devices connecting to the network. Because of the deterministic and repeatability constraints, medium access control protocol by CSMA/CD (Carrier-Sense Multiple Access with Collision Detection) in traditional Ethernet network is inadequate, so a different type of network access is required. Local Area Networks

(LANs) are widely used as communication networks in this level to achieve desired characteristics. The Ethernet with TCP/IP protocol is mostly used as a control level network to connect control units with computers. In addition, this network acts as a control bus to coordinate and synchronize between various controller units. Some fieldbuses are also used in this level as control buses such as PROFIBUS and ControlNet. In such networks, Concurrent Time Domain Multiple Access (CTDMA) protocol is used based on a time-slice algorithm that regulates each node's opportunity to transmit in a network interval. Adjustment of the amount of time for a network interval gives a consistent, predictable time for data transmission [3].

The informational level is the top level of the industrial system which gathers the information from the lower level, i.e., control level. It deals with large volumes of data that are neither in constant use or time critical. Large-scale networks exist in this level. So Ethernet WANs are commonly used as information level networks for factory planning and management information exchange. Sometimes these networks may connect to other industrial networks via gateways.

1.3 Requirements of Industrial Control Networks

The industrial control networks operate along two different paradigms: time-triggered and event-triggered [5]. In the time-triggered applications, the systems work periodically. They first wait for the beginning of the period (or some offset from the beginning), sample their inputs, and compute some algorithm according to the inputs and some set point data received from computers higher in the hierarchy. They then make the results available at the outputs. Inputs and outputs correspond to sensors and actuators at the lowest level in the hierarchy. At higher levels, inputs correspond to status and completion reports from the next lower level. Outputs are set points or commands to the lower level. Acquisition and distribution applications are special cases. Acquisition applications have no outputs to the process but store the output results internally. Distribution applications have no input and compute the algorithms from stored information.

Periodicity is not mandatory but often assumed because it simplifies the algorithms. For instance, most digital control theory assumes periodicity. Furthermore, it assumes limited jitter on the period and bounded latency from input instant to output instant. Acquisition and distribution applications have similar requirements in terms of periodicity and jitter.

Meanwhile, in event-triggered applications, the system is activated upon the occurrence of events. An event may be the arrival of a message with a new command or a completion status or the change of an input detected by some circuitry. When an event is received, the application computes some algorithm to determine the appropriate answer. The answer is then sent as an event to another application locally or remotely. The time elapsed between the generation of the input event and the reception of the corresponding answer must be bounded. Its value is part of the requirements on the application and also the communication system if the events have to be transported through some network. Furthermore, applications should be able to assess some order in the event occurrences. This is usually not a problem when the event is detected and processed on the same computer. It becomes a problem when the events are detected at different locations linked by a network which may introduce some variable delay.

Because large amounts of data may be passed through these control networks and message lengths tend to be longer, data transmission rates tend to be faster than with fieldbus networks. However, since they can be used to pass time-critical data between controllers, control networks must also be deterministic and meet the time-dependent (usually called real time) needs of their intended applications. Determinism in a network context is defined as: there is a specified worst-case delay between the sensing of a data item and its delivery to the controlling device. Real time in this context is defined as "sufficiently rapid to achieve the objectives of the application," and is measured as latency time. Determinism and latency are separate but complementary requirements. Both determinism and a specific latency are required to achieve synchronization. If the same control network is used to exchange both real-time data between controllers and business information between controllers and business systems, clearly there must be some way to prevent business information from interfering with real-time deterministic response. Many complex protocols have been constructed for this purpose, but most control networks rely only on the underlying nature of the chosen network protocol. Usually, determinism is achieved by preventing message collisions and limiting the maximum message length. Low latency is achieved by using high-speed media and minimizing the number of times a signal must be rebroadcast, such as in a mesh network.

The benefit of using a standard network protocol such as Transport Control Protocol/Internet Protocol (TCP/IP) over an Ethernet network is a lower cost. By simply selecting standard Ethernet cabling and using full-duplex Ethernet switches instead of passive hubs, a control network built on this commodity technology can guarantee that there will be no network collisions, making such networks deterministic. Using high speed such as 100 or 1000 Mbps and the standard Ethernet maximum packet length of 1500 bytes achieves low latency and means that other applications cannot "hog the wire," preventing time-critical data transfers. However, you still must do the math! Remember that the definition of real time and determinism requires that the network must make its bandwidth available for time-critical data transfers in less than the maximum time period allowed for the control system. For example, if a business application were to transfer a maximum size Ethernet message (1500 bytes) at 100 Mbps, the network would be blocked for a maximum time of about 150 μs. Normally this magnitude of delay is perfectly acceptable for both process control and factory automation needs, but it may not be acceptable for motion control or machine control. It would be nice if control networks and fieldbus networks could not be used for the same applications, but they can. It would also be nice if control networks were always confined to a business or control room environment, but increasingly they are being extended to the field and shop floor. In some cases, control networks are being used in applications normally requiring a fieldbus. In fact, all of the control networks were developed from one or more of the fieldbus networks and use the same application layer and user layer protocols. Since control networks are related to fieldbuses, there will continue to be a very loose dividing line between them.

1.4 Communication Technologies for Industrial Control Networks

In order to carry out the assigned tasks of networks, it is essential for the devices to communicate. Traditional wired communication technologies have played a crucial role in industrial monitoring and control networks. Accordingly, this communication was performed over point-to-point wired systems. Such systems, however, involved a huge amount of wiring which in turn introduced a large number of physical points of failure, such as connectors and wire harnesses, resulting in a highly unreliable system. These drawbacks resulted in the replacement of point-to-point systems using advanced industrial communication technologies. This section aims to highlight the major technologies deployed in the industrial control networks.

1.4.1 Fieldbuses

Traditionally, control systems in factories and plants were analog in nature. They used direct connections from controller to actuator or transducer to controller and were based on a 4- to 20-mA control signal. As the system became more complex and as networking technologies evolved, eventually a change from the analog system to a digital system came about. Fieldbuses were developed to tie all these digital components together. Over the past few decades, the industry has developed a myriad of fieldbus protocols (e.g., Foundation Fieldbus H1, ControlNet, PROFIBUS, CAN, etc.). Compared to traditional point-to-point systems, fieldbuses allow higher reliability and visibility and also enable capabilities, such as distributed control, diagnostics, safety, and device interoperability [6].

Fieldbuses are digital networks and protocols that are designed to replace the analog systems. They are essentially industrial LANs that network all of the computers, controllers, sensors, actuators, and other devices so they can interact with one another. A single network cable replaced the dozens or even hundreds of individual analog cables in the older systems. Protocols allowed operators to easily monitor, control, troubleshoot, diagnose, and manage all devices from a central location. While these fieldbuses reduced the wiring and improved the reliability and flexibility of the system, another issue was created: multiple proprietary systems, with incompatibility and a lack of interoperability between the various components. Devices made to work with one fieldbus and protocol could not work with another.

Many fieldbuses have been developed. Some attempts at building a common standard were made but no one system or standard ever emerged. ControlNet, DeviceNet, Foundation Fieldbus H1, HART, Modbus, PROFIBUS PA, and CAN/ CAN open are the most commonly used fieldbuses.

1.4.1.1 ControlNet

ControlNet is an industrial network and protocol supported by the Open DeviceNet Vendors Association (ODVA) [7]. It is based on the Common Industrial Protocol (CIP), which defines messages and services to be used in manufacturing automation. ControlNet uses RG-6 coax cable with Bayonet Neill-Concelman (BNC) connectors for the physical layer (PHY) and is capable of speeds to 5 Mbits/s using Manchester coding. The topology is a bus with a maximum of 99 drops possible. Its timing permits a form of determinism in the application.

1.4.1.2 DeviceNet

DeviceNet is another ODVA-supported fieldbus. It uses the well-known controller area network (CAN) technology for the PHY that was originally developed by Bosch for automotive applications. The DeviceNet protocol is similar to that of ControlNet and also uses the Common Industrial Protocol (CIP) at the upper layers. Layers 1 and 2 are CAN bus. The medium is an unshielded twisted pair (UTP) using a single-ended non-return-to-zero (NRZ) format with logic levels of 0 V and +5 V. The topology is a bus with up to 64 nodes allowed. Data rate depends on bus length and can be as high as 1 Mbit/s at 25 m to 125 kbits/s at 500 m.

1.4.1.3 Foundation Fieldbus H1

Originally developed by the International Society of Automation (ISA) standards group as Foundation Fieldbus, SP50 was one of the earlier digital fieldbuses for replacing 4- to 20-mA loops. The protocol is designated H1, which uses the IEC 61158-2 standard for the PHY and features twisted-pair cabling with basic data rate of 31.25 kbits/s. The transmission frames are synchronous with start and stop delimiters. Coding is Manchester.

1.4.1.4 HART

HART standing for Highway Addressable Remote Transducer is a two-way communications path over twisted pair. It retains the popular 4–20 mA analog functionality but adds digital signals. The digital signal is in the form of a frequency shift keying

(FSK) modulated carrier that uses the old Bell 202 modem frequencies of 2200 Hz for a 0 and 1200 Hz for a 1.

The data rate is 1200 bits/s. The FSK signal is phase continuous and does not affect the analog signal level because it is ac. Also, the FSK signal is a 1-mA variation around the dc level. The protocol uses OSI layers 1 through 4 and 7. The digital part of the communications is primarily used for commands, provisioning, and diagnostics.

The HART fieldbus is popular as it is compatible with older 4- to 20-mA equipment while adding the digital networking capability. It is still widely used. Typical HART field instruments such as the Analog Devices ADμCM360 consist of an embedded controller and the I/O for the sensors such as a pressure transducer and real-time data (RTD) temperature sensor. The on-board 24-bit sigma-delta analog-to-digital converters (ADCs) digitize the sensor information and then send it to the AD5421, a digital-to-analog converter (DAC) and 4- to 20-mA current source for connection to the cable. Digital information is also sent to the AD5700 HART FSK modem.

1.4.1.5 Modbus

Modbus is a popular industrial protocol normally used for communications with PLCs. It is simple and the standard is open so that any users can use it. Basically, Modbus works with RS-232 interfaces. The basic format comprises asynchronous characters sent and received with a UART. Modbus can be carried over a variety of PHYs and is often encapsulated in Transmission Control Protocol/IP (TCP/IP) and transmitted over Ethernet. It is also compatible with a wireless link.

1.4.1.6 PROFIBUS

PROFIBUS, another widely used fieldbus, was developed in Germany and is popular worldwide. There are versions for decentralized peripherals (DP) and process automation (PA). The protocol is synchronous and operates in OSI layers 1, 2, 4, and 7. Using RS-485, bit rates can range from 9.6 kbits/s to 12 Mbits/s. With a bus up to 1900 m long, the data rate is 31.25 kbits/s.

1.4.1.7 CAN/ CANopen

The use of Controller Area Network (CAN) is still dominated by its vast use in the automobile industry. Another stronghold is the use as a physical layer for the SAE J1939 protocol, and CAN will remain the most cost-sensitive fieldbus solution for small, embedded systems. In summary, the use of CAN will continue in:

- Automobiles and Trucks
- Aerospace (e.g., satellites)
- SAE J1939

- Small Embedded Solutions
- Legacy Applications

CANopen is basically a software add-on to provide network management function to CAN. The side effect is a reduced CAN bandwidth. These CANopen legacy applications are motion control and Industrial Machine Control.

CAN and CANopen, used as fieldbus systems for embedded solutions. The advantages of such networks include

- Extreme Reliability and Robustness
- No Message Collision
- Very low resource requirements
- Low-cost implementation
- Designed for real-time applications
- Very short error recovery time
- Support of device profiles (CANopen only)

However, there are some disadvantages of using CAN and CANopen, the biggest being the limited network length (~120 ft at a 1 Mbit/s baud rate). The disadvantages include limited network length (depending on baud rate), the limited baud rate of 1 Mbit/s, and limited bandwidth.

1.4.2 Industrial Ethernet

For many years, Controller Area Network (CAN) and CANopen, a higher layer protocol based on CAN, has been proved to be the best solution for low-cost industrial embedded networking. However, the most obvious shortcomings of these technologies include limited baud rate and limited network length. Industrial Ethernet technologies are currently the most formidable challenge to CANopen as the low-cost industrial networking technology of choice for business and enterprise for decades. It is by far the most successful and widely used networking technology in the world. It is affordable and reliable and is backed up by a strong series of IEEE 802.3 standards that keep it current. Over the past 10 years or so, Ethernet has found its way into the industrial setting for I/O and networking. It is gradually replacing the multiple fieldbuses and proprietary networks or working with them.

Some of the benefits of moving to Ethernet are

- Fewer smaller networks: Most fieldbuses can connect up to 20–40 devices. But beyond that, a separate fieldbus network is required for more devices and for connecting the two networks, if that is even possible. With Ethernet, you can connect up to 1000 devices on the same network. This arrangement improves the efficiency and decreases the complexity of the network.
- Lower cost: With many Ethernet vendors, equipment prices are competitive and the overall cost of building a network is typically lower than building a fieldbus network.

- Higher speeds: Ethernet has much higher speed capability than most fieldbuses. While that speed is not always needed, it is a benefit and the network grows in size and as faster devices are connected. While 10/100-Mbits Ethernet is the most common, some industrial facilities have already upgraded to 1-Gbit/s Ethernet.
- Connection to the factory or plant IT network: The industrial networks are traditionally kept separate from the business network, but companies are finding that advantages occur when the two networks can be interconnected. Data can be collected and used to optimize the manufacturing process or make improvements or decisions not previously possible.
- Connection to the Internet: This may not be desirable, but if it is, Ethernet provides a very convenient way to send and receive data over an Internet connection.

There are two main disadvantages of using Ethernet in the industrial setting. First, the hardware was not designed for the demanding environment in factories and process plants. Excessive temperatures, environmental hazards, chemicals, dust, mechanical stresses, and moisture make traditional equipment less reliable. Yet over the years, manufacturers have repackaged Ethernet gear to bear up under such conditions by adding industrial-grade housings and tougher electronics. Another hazard is excessive noise caused by motors, power switching, and other sources. Ethernet's differential wiring is essentially noise-resistant. It can be made noise-free with shielded cable. Most industrial wiring is simply standard, but higher grade CAT5 or CAT6 cable usually suffices. On the other hand, the RJ-45 connectors are a source of problems, especially in dirty and high-moisture environments. Special RJ-45 connectors have been developed to solve this problem. These connectors add a dirt- and moisture-sealed cover to an upgraded RJ-45 connector. These connectors meet the rigid IP67 environmental standards for hazardous environments.

A second disadvantage is Ethernet's inherent non-deterministic nature. Many industrial networks rely on timing conditions that must occur within a specific time frame. Many need a real-time connection or something close to it. Determinism means that a device or system can respond within a minimum time interval. It can respond in less time but no more than a specified time. If a device is deterministic to 10 ms, then anything less is okay. The response does not usually have to be repeatable, but that depends on the application.

Ethernet determinism is widely variable. It is a function of the carrier-sense multiple access with collision detection (CSMA/CD) access method, cable lengths, number of nodes, and the combinations of hubs, repeaters, bridges, switches, and routers used in the system. To improve the deterministic response, designers of industrial Ethernet systems must keep cables short and minimize the number of nodes, hubs, and bridges. Switches can be added to larger networks to isolate different segments, and that reduces the number of collisions and interactions.

Determinism can also be implemented or improved in some cases by using the IEEE 1588 Precision Time Protocol (PTP). The PTP permits systems with clocks to achieve synchronization among all connected devices, allowing precise timing information transfer within a network. Time stamping and near real-time performance can occur in some applications.

Another feature of Ethernet finding acceptance is Power over Ethernet (PoE). Defined by IEEE standards 802.3af and 802.3at, it allows the transmission of dc power over the Ethernet cables to power remote devices. This is a major benefit in many industrial settings and eliminates the need to install a power source near some remote sensor or other device. The standard defines power levels up to 15.4 or 25.5 W, but higher power versions up to 51 W are becoming available.

Finally, several enhanced or modified versions of Ethernet have been developed to overcome the timing issues of standard Ethernet or simply make it more compatible with existing equipment and systems. These include EtherCAT, EtherNet/IP, Profinet, Foundation Fieldbus HSE (high-speed Ethernet), and Modbus/TCP. Some use special protocols while others use TCP/IP.

EtherNet/IP is an application layer protocol using CIP, which defines all devices as objects and specifies the messages, services, and transfer methods. CIP is then encapsulated in a TCP or User Datagram Protocol (UDP) packet for transfer over Ethernet.

Profinet is another protocol that uses TCP/IP over Ethernet. It is not PROFIBUS over Ethernet. Instead, it uses two different protocols: one called Profinet CBA for component-based systems and Profinet IO for real-time I/O operations. Profinet CBA can provide determinism in the 100-ms range. It also can deliver determinism to 10 ms. A version of Profinet IO called IRT for isochronous real time can have a determinism of less than 1 ms.

Foundation Fieldbus HSE uses the H1 protocol over TCP/IP. It also uses a special scheduler that helps to guarantee messages in known times to ensure determinism at some desired level.

EtherCAT gets rid of the CSMA/CD mechanism and replaces it with a new “telegram” message packet that can be updated on the fly. Networked devices are connected in a ring or a daisy chain format that emulates a ring. As data is passed around the ring, message data can be stripped off or inserted by the addressed node while the data is streaming. The one or more EtherCAT telegrams are transported directly by the Ethernet frame or encapsulated into UDP/IP datagrams. Determinism of 30 μs and less can be achieved with up to 1000 nodes.

Modbus/TCP is the popular Modbus fieldbus protocol packaged in a TCP/IP packet. The Modbus checksum is replaced by TCP/IPs 32-bit checksum. Then the TCP/IP packets are carried over standard Ethernet.

Obviously, all of these systems are not interoperable with one another. But they can all coexist on the same Ethernet LAN since they all conform to the Ethernet Layer 1 PHY standard. Those using TCP/IP could be made interoperable with the appropriate software modifications.

Table 1.1 provides an overview of the various industrial Ethernet protocols [1].

Table 1.1 Comparison of various industrial ethernet networks

	EtherCAT	Ethetnet/IP	Powerlink	Modbus/TCP
Vendor Organization	EtherCAT Technology Group	Open DeviceNet Vendor Organization	Ethernet Powerlink Specification Group	Modbus-IDA Group
Homepage	www.ethercat.org	www.odva.org	www.ethernet-powerlink.org	www.modbus-ida.org
Availability of specification	Members signing an NDA	Free	Members	Free
Availability of technology	Example Code, ASIC, FPGA	Example Code	Standard Ethernet Chips	Example Code
Products available since	2003	2000	2001	1999
Interaction structure	Master/Slave	Client/Server	Master/Slave	Client/Server
Communication method	One frame for all communication partners	Message oriented	Message oriented	Message oriented
Ether data transfer rate	100 Mbit/s	100/10 Mbit/s	100 Mbit/s	100/10 Mbit/s
Physical topology	Line, Daisy, Chain, Tree	Star	Star	Star, Tree
Logical topology	Open Ring Bus	Bus	Ring	Bus
Infrastructure components	Switches between different segments	Switches (hubs are possible, but not efficient)	Hubs, no switches	Hubs, switches
Device profiles	CANopen, SERCOS	DeviceNet, ControlNet	CANopen	None

1.5 Trends and Issues

The industrial field generally lags behind other sectors of electrics simply because its technological needs do not follow the consumer or enterprise market trends. But overall, industrial sectors do follow the general trends in communication technologies. Key trends and issues include followings

- Continued use of fieldbus technology: The fieldbus technologies are the digital LAB of the industry. They connect the sensors, controllers, and actuators of most factory automation and process control facilities. Despite the ongoing movement to Ethernet connectivity and wireless, there continues to be the growth of several percents per year in the fieldbus market.
- A strong movement to Ethernet: Ethernet has been the local area network (LAN) of choice for enterprise and even consumer networking for decades, and it dominates. The industry was slow to adopt it but has now embraced it completely. Most new

industrial networking efforts use some form of Ethernet. Its proven reliability, low cost, and high availability have made it particularly popular. Special industrial versions of Ethernet have emerged to enhance it for industrial use.

- Significant growth in wireless connectivity: Industry was slow to adopt wireless despite its many benefits. Industrial users assumed it was unreliable and insecure but have learned otherwise since. New and improved wireless standards and equipment have made wireless a key component in most modern industrial settings.
- Fewer proprietary standards and equipment: For decades, industrial communications needs were met with many high-cost proprietary fieldbuses, interfaces, and equipment, which are still entrenched in many systems. However, the trend today is to open standards and Ethernet.
- Rapid adoption of the Internet protocol (IP) model: The goal is to give the most industrial equipment an IP address so devices and equipment can communicate over Ethernet and the Internet. With the availability of IPv6, that is now possible.
- Increased use of video surveillance: security has become an issue at many plants and facilities, and video is useful. Video also enables improved monitoring that simple sensors cannot provide.
- Industrial Standardization for Interoperability: Most factories, process control plants, and facilities are a real mixed bag of old and new, analog and digital, and proprietary and open standards. A big issue has been the incompatibility and interoperability of different equipment such as all devices and system can work together seamlessly. Such challenges lead to new standards, equipment, and software gradually developed to address those problems.

1.6 Conclusions

Technology is continuously and rapidly transforming industrial processes. It is sometimes hard for businesses to integrate a new technology into an existing system. It requires professional expertise and training to run a newly introduced system. However, with the growing demand for sophisticated and high-quality products, businesses have to quickly adapt and utilize the power of emerging automation systems.

Looking to the future, the most notable trend appearing in the industry is the move to industrial wireless networks at all levels [8–10]. Wireless networks further reduce the volume of wiring needed (although oftentimes power is still required), enable the placement of sensors in difficult locations, and better enable the placement of sensors on moving parts such as on tooltips that rotate at several thousand revolutions per minute. Issues with the migration to wireless include interference between multiple wireless networks, security, and reliability and determinism of data transmission. The anticipated benefit in a number of domains (including many outside of manufacturing) is driving innovation that manufacturing, in general, can leverage. It is not inconceivable that wireless will make significant in-roads into networked control and even safety over the next 5–10 years