

## Related Work and Background

This chapter provides a general state of the art and relevant background for this work. Both wired and wireless communication systems for industrial automation have been considered with their characteristics, even though the main focus is put on wireless systems. Existing technologies and solutions are analysed with respect to the relevant application requirements as identified in Sect. 1.1. The related work for the three main components of the solution approach, i. e., medium access control, resource allocation, and the provision of a global time base is discussed at the beginning of their corresponding chapter.

### 2.1 Communication in Industrial Automation

Nowadays, three generations of field level networks exists [152]. Even though traditional field bus systems are still used in many applications, future field level networks will be based on Real-time Ethernet (RTE), because of vertical integration aspects [151]. Hence, this section is focussed on existing real-time Ethernet protocols, and their characteristics. A specific focus is put on approaches based on TDMA, because they are able to provide the lowest latencies, i. e., the most powerful real-time communication features. Due to the fact that the wired system is not a research subject of this work, the considered solutions for the wired system are based on international standards and selected real-time Ethernet standards from IEC 61784-2 [63] are analysed for the real-time communication part.

#### 2.1.1 Real-time Ethernet

Most of the existing RTE solutions are based on the IEEE 802.1 standard with switched Ethernet [65] and use the prioritization 802.1q [64]. However, depending on the required determinism, this might be not sufficient [78] and several extensions are developed which can be classified accordingly.

In general, RTE protocols can be also classified according to real-time classes (cf. Table 1.1). The classification and the differences of the protocol stack are

both shown in Fig. 2.1. The protocols are becoming more powerful from class 1 to class 3, while additional functionality on the data link layer is introduced at the same time [77]. Modbus/TCP [58] and Ethernet/IP [61] are representatives of the first category. The protocols are using Ethernet as it is, only adding an industrial-automation specific application layer on top of TCP/IP. Because of using the whole TCP/IP protocol stack, their real-time characteristics suffer, and cyclic update times of about 100 ms can be typically achieved.

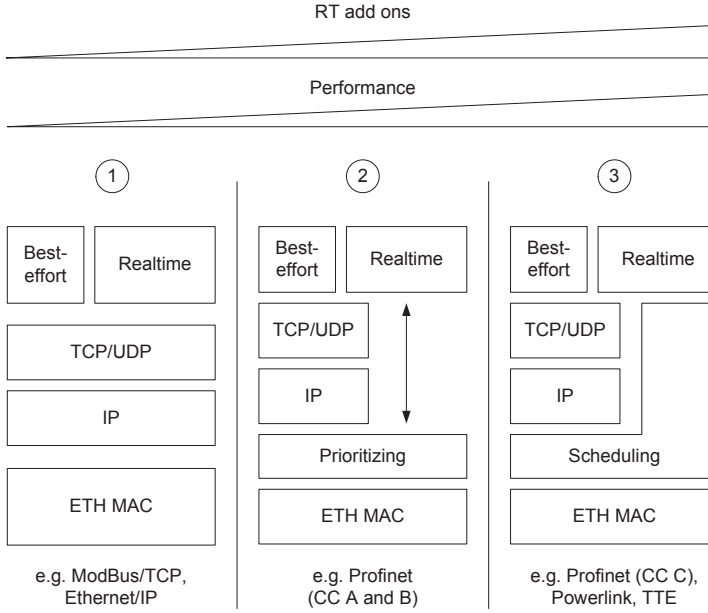


Fig. 2.1: Classification of Real-time Ethernet protocols [77]

Industrial communication systems, which use protocols of the second category, are perceived as a compromise between the native Ethernet standard and achievable real-time data transfer. An example for this category is given by Profinet (conformance class A and B) [60]. These protocols use a priority scheme at the Ethernet MAC layer. For an additional optimisation the transport and the network layer has to be bypassed for real-time data. Implementing this optimisation, cyclic update times in the range of  $\leq 10$  ms can be achieved.

Further enhancements are only possible by adapting the scheduling procedure of the MAC layer. Protocols which are changing the original MAC scheme of Ethernet are part of real-time class 3. In order to use those protocols, specific hardware or software is necessary. For example, Profinet (conformance class C) [60], Ethernet Powerlink [56], and Time-triggered Ethernet [92] belong to this category. Protocols which belong to class 3 are able to support cyclic update times in the range of  $\leq 1$  ms.

Common comparison criteria, also referred to as performance indicators, of the existing RTE communication standards are defined in [63] as communication profiles. It should be noted that all performance indicators highly dependent on the selected application scenario, i. e., payload, real-time class, chosen topology, etc. Relevant performance indicators for this work are briefly introduced in this section and summarized in a comparison table (cf. Table 2.1) followed by a description of the most relevant communication profiles.

**Physical Layer** The supported physical layers of the communication profiles are listed in the second column of Table 2.1. These can include IEEE 802.3 (Ethernet), IEEE 802.11 (wireless) and others. Ethernet is the common denominator of all communication profiles, even though always in a modified version for providing real-time.

**Real-time mechanism** The Real-time guarantee mechanism is used by a communication profile to guarantee an upper bound of the delivery time through the network. This is guaranteed in different ways. Frame prioritisation allows to send frames with a higher priority before frames with a low priority. It gives only moderate results as compared to the other two mechanisms. In the event-based/event triggered synchronization the communication partners synchronise their transmissions based on events generated by a defined master. This mechanism is usually referred to as polling. In TDMA all communication entities have a common schedule and their own time-slot for transmission. The mechanism requires synchronized distributed clocks with a high accuracy.

**Communication model** The communication model of each communication profile describes the method of organizing the communication on the application layer. The model is either a master/slave or a producer/consumer model. The *master/slave* or client/server model has at least one station which coordinates the communication by sending a request for data to its slaves, and the slaves reply accordingly. This model is considered as a confirmed service from the masters viewpoint and consists of the four service primitives request (master), indication (slave), response (slave), and confirmation (master). In the *producer/consumer* model, a producer (sender) sends data to one or more consumers (receivers). The data is sent either cyclically or event-based to the consumers. This model is considered as an unconfirmed service and consists of the two service primitives request (producer), and indication (consumer).

**Delivery time** The delivery time is the whole transmission time needed for a real-time Application Protocol Data Unit (APDU), i. e., from the sending station to the receiving station. It is measured at the application interface (cf. [63]). Therefore, a maximum delivery time or a range is given, indicating at which point the maximum value can be considered as a worst case. The delivery time depends on several factors, such as the cycle time, or the network topology (number of switches).

The delivery time can be considered as equivalent to the latency  $T_{Lat}$  defined in Sect. 4.1, which is used as a central metric for this work.

**Network topologies** Each communication profile supports a discrete set of network topologies which are star (hierarchical star), line, mesh (partial or full), and ring. Combining different topologies is also possible, for example, a tree topology is considered as a combination of a line and a star topology.

Table 2.1: Most common RTE profiles and their comparison criteria [63]

RTE Profile	Physical Layer	Real-Time mechanism	Communication model	Delivery Time	Network topologies
Ethernet/IP	IEEE 802.3	Prioritization	Producer/ Consumer	< 20,4 ms	Star Star
Profinet IO Conformance Class C	IEEE 802.3	TDMA	Producer/ Consumer	$\leq 1$ ms	Line, ring star
TTEthernet	IEEE 802.3	TDMA	–	–	Line, star
EtherCAT	IEEE 802.3, IEC 61158-2 frame	Summation	Master/ Slave	< 150 $\mu$ s	Line, star
ETHERNET Powerlink	IEEE 802.3	Polling mechanism	Master/ Slave	< 1100 $\mu$ s	Line, star

## Ethernet/IP

Ethernet/IP [61] is an application layer protocol which makes use of TCP/IP at the lower layers to transfer the information across the network. The physical layer is Ethernet and the MAC layer uses CSMA/CD for channel sensing. Because of such a channel access scheme, deterministic communication across the whole network is impossible. There are two profiles which are available for Ethernet/IP. The first profile is based on frame prioritisation and does not need special hardware on the end-stations or the switches. In this profile, the frames are prioritised and the scheduling algorithm allows a faster processing of high priority messages. In the second profile, the clocks of the devices are synchronized to each other with IEEE 1588v2 [68] and allow a scheduling of messages. Hence, the communication becomes more deterministic. The cyclic real-time frames between a producer and other consumers are tagged as *implicit* and transferred through UDP/IP.

## Profinet IO

Profinet IO [60] is currently the most important view for Profinet. It is allowing real-time communication and addresses decentralized field devices. Profinet IO has three conformance classes supporting different real-time requirements. Conformance class C, formerly referred to as Profinet IRT (Isochronous RT), is specifically designed for

NCS, and supports real-time constraints. In Profinet the standard MAC of Ethernet is modified and the medium access is based on TDMA. The whole real-time data traffic is scheduled a priori based on different requirements of the application. The nodes share a common notion of time which is obtained by the precision time control protocol (PTCP), a modification of IEEE 1588v2 PTP [68].

### **Time-triggered Ethernet**

The TTEthernet system [92] uses the same infrastructure for real-time communication and best-effort traffic by adding a TDMA scheme to a switched Ethernet system. All TTEthernet share a common schedule which is provided by a global scheduler and transferred to all TTEthernet nodes and switches. The clock synchronization for the global time is based on IEEE 1588v2 [68]. The protocol supports time-triggered traffic as well as rate constraint traffic and best-effort traffic. Rate constraint traffic is used for applications with reduced real-time requirements.

### **Ethercat**

Ethercat [55] is a master/slave based system and uses a summation frame for transmitting real-time critical process data. The network is segmented into Ethercat segments. The Ethercat master sends cyclic frames to its slaves. Each slave processes the received frame on-the-fly and forwards it to the next slave. Ethernet frames are transmitted through all slaves on the segment, in sequence, from the first slave device (the owner of the MAC address of the segment, or the segment address slave) to the last slave device. No intermediate switches between master and slave are used in Ethercat, since every slave is a 2-port switch. However, the slaves require special hardware to support the on-the-fly frame processing. The profiles of Ethercat are based on an event-based synchronization and a clock synchronization scheme, the second one allowing for real-time communication.

### **Ethernet Powerlink**

Ethernet Powerlink [56] is based on a master/slave communication model on a shared Ethernet segment. The master, which is also called managing node, coordinates the communication with every slave and ensures deterministic real-time communication. Four phases are forming a cycle, start, cyclic, asynchronous, and idle. In the start phase the master multicasts the start of cycle (SoC) message to start the cyclic phase. In this phase the master polls each slave separately and gets a reply from the slaves. After polling the active nodes, there are some slots reserved for asynchronous communication where non real-time traffic is sent followed by the idle phase until the next cycle. There are no restrictions on which topologies Ethernet Powerlink when using hubs. Even though switched Ethernet can also be used, it is not recommended. Switches will cause an additional jitter and path delay which reduces the achievable performance of the protocol.

### 2.1.2 Engineering Aspects and Flexibility

The commissioning of today's Real-time Ethernet (RTE) systems requires a time consuming and error-prone manual system configuration process. The corresponding common engineering cycle is always based on a static offline configuration phase as discussed in [33]. This is due to the need to maintain a high level of determinism for the production process and avoiding costly production interruptions. It consists of three steps, (i) the control application is implemented in an engineering tool, (ii) the physical structure of the automation system, including all devices, is added to the engineering tool and configured accordingly, and (iii) The logical variables of the control software are mapped to the physical sensor and actuator data. Only the second step is further considered here.

The procedure for the second step is as follows. The device information of all IOD of the system, referred to as Device Description (DD) files, is transferred offline to an engineering tool. The DD file is then used to create a project with configuration and parameterisation as required by the application. In this step the parameters and the communication schedule is calculated for all devices of the system, even the ones that are inactive. Afterwards, it is passed from the engineering to the PLC which configures all available IO Devices (IODs) in the start-up phase of the system.

Hence, the existing systems are very static and flexibility as required for the first application category of RMS must be engineered a priori. Interesting solution approaches are discussed by Dürkop et al. in [32] for the configuration and by Wisniewski et al. in [183] for scheduling, but not further considered in this work.

## 2.2 Industrial Wireless Communication

Typical application areas for industrial wireless networks can be found in the Process Automation (PA) as well as in the Factory Automation (FA) domains. Building automation is also relevant, but not further considered in the context of this work. Both domains have different requirements [172]. Wireless systems in the PA domain are mainly used for monitoring, process control and asset management. The wireless technology has to span distances of more than 1 km, but with moderate latencies. Whereas applications in the FA domain might even deal with control loops, i. e., stationary and mobile sensors, and monitoring. In many applications of FA you have to cover a limited range (e. g., one single manufacturing cell), but the temporal requirements are in the range of real-time class 2 and very challenging. This section provides an analysis of existing industrial wireless solutions and their characteristics based on the identified requirements of the application categories (cf. Table 1.2).

The existing wireless solutions for industrial automation are based on COTS technologies, due to economical reasons and a wider market acceptance [39]. In FA existing IEEE 802.11 and IEEE 802.15.1 conform components are typically used with a few proprietary protocol extensions. For instance, the iWLAN system of Siemens [157] or the Wireless Interface for Sensors and Actuators (WISA) system of

ABB [153]. Another solution is the Wireless Sensor and Actuator Network (WSAN) for factory automation [94], which is specified by the Profibus and Profinet user organization (PNO). Its fundamental concepts are based on WISA, but it has been extended with a few modifications.

In the PA domain, system based on IEEE 802.15.4 are used due to their low energy consumption. Based on this, the standards WirelessHART and ISA 100.11a are developed by the HART communication foundation and the international society of automation (ISA), respectively.

### 2.2.1 Systems Based on IEEE 802.15.1

The IEEE 802.15.1 standard [66] specifies the Physical Layer (PHY) and the Medium Access Control Sublayer (MAC) of the well-known Bluetooth (BT) technology and it operates in the 2,4 GHz-ISM-Band. A typical application for the 802.15.1 would be for instance a connection between a cell-phone and a headset or a headphone and an audio device. However, the system is also attractive for the use in industry applications [181], since its medium access method allows a deterministic data delivery.

According to 802.15.1 every physical channel used, is called a piconet consisting of one master, and up to seven slaves. The master device within a piconet coordinates the traffic within a piconet and starts the connection setup procedure. Furthermore, the wired and the wireless network are connected via the master device. The other devices are called slave devices. These are only able to directly communicate with their master. Slave devices within a piconet are either in an active or inactive operation mode. An active slave device communicates with the master device, inactive devices are in an energy saving state and only start a communication upon a wake up call by the master device.

Piconet traffic is based on TDMA with a duplex scheme, allowing the master to communicate in odd-numbered time slot. The slaves are only permitted to reply in time slots which are even-numbered and after they have been polled by the master. The channel access is divided into slots, each of 625  $\mu$ s length. A data transmission may occupy the channel for 1, 3 or 5 consecutive slots. A frequency hopping spread spectrum (FHSS) modulation with 79 different 1 MHz channels is used to deal with the ISM-Band requirements. In order to avoid problems with the coexistence to other technologies, an adaptive FH (AFH) can be used to render occupied frequencies.

The Data Link Layer protocol is mainly divided into asynchronous connectionless (ACL) and Synchronous Connection Oriented (SCO) frames. The SCO transmission is attractive for industrial usage. The SCO transport mechanism reserves time slots on the physical channel. It is therefore able to provide QoS guarantees. The transmission of an SCO packet takes 366  $\mu$ s and typically transmits data with a rate of 64kb/s [181]. This is done by reserving periodic slots for a specific communication between the master and a slave device. An extension to the SCO data transmission is the eSCO data transmission. It also uses reserved time slots and has the advantage that it can deal with different, but still static, transmission rates and

is able to transport non voice data [66]. Nonetheless, in most cases, it is necessary to have more than one piconet, because of the existing slave limitation to seven.

### **Wireless Interface for Sensors and Actuators**

The WISA system [153, 90] has been developed by ABB and is targeted at typical factory automation applications. It has been designed to cover wireless communication as well as wireless power supply. This enables truly wireless connected sensors and actuators without having the need for a separate power supply.

The wireless communication WISA COM is based on IEEE 802.15.1 physical layer. In a system that needs to achieve the delivery of messages with a very high probability of success and high number of devices, the medium access is important. The medium access in WISA is time division multiple access with frequency division duplex and frequency hopping (TDMA/FDD/FH). The WISA frequency hopping scheme guarantees that the frequencies used in successive frames are widely spread. The downlink transmission from the base station to the wireless devices is always active, for the purpose of establishing frame and slot synchronization for the devices, but also to send acknowledgements and data.

In order to save power, uplink transmissions from a sensor only occur when it has data to send. The requirement of wireless real-time communication combined with a need for a high number and high density of devices, makes efficient use of the available bandwidth very important. A number of input modules (base stations) can be distributed in the plant, with short-range communication to local sensors/actuators. The input modules (base stations) are connected to the control network via any field bus and communicate with the local wireless devices. A sophisticated input module (base station) ensures that the complexity resides in the input module rather than in the wireless sensors or actuators. One input module can handle up to 120 devices (sensors) or 13 wireless sensor input/output pads. Since in typical applications only sensor and actuator devices are targeted the capacity of the system is very limited. It is possible to exchange only a few bytes of payload.

### **Wireless Sensor and Actuator Network for Factory Automation**

The WSA for factory automation is developed by the Profibus User Organization and is partly based on the previously introduced WISA system. It also uses the PHY layer of IEEE 802.15.1 and provides a frequency hopping multiple access, i. e., a combination of frequency hopping and TDMA. The whole system is specifically designed for the sensors and actuators on the field level. WSA is able to address up to 120 wireless nodes in the system, targeting applications of real-time class 2. The reliability is achieved by allowing up to four retransmissions on different frequencies. In this case the update time must be decreased. Moreover, a blacklisting of certain channels is provided to minimise interference with other system. However, the capacity of the system is limited due to the same reason as for WISA.



### 2.2.2 Systems Based on IEEE 802.15.4

The IEEE 802.15.4 standard [69] has become a communication standard for low data rate, low power consumption and low cost Wireless Personal Area Network (LR-WPAN). The protocol focuses on very low cost communication, which requires very little or no underlying infrastructure. The basic framework supports a communication range of  $\leq 10$  m. The capacity of the system varies depending on the selected data rate of 20, 40, 100, and 250 kbps. The protocol provides flexibility for a wide variety of applications by effectively modifying its parameters. It also provides real-time guarantees by using a Guaranteed Time Slot (GTS) mechanism for time sensitive applications. Hence, two kinds of network configuration modes are provided in [69]. The beacon enabled mode, where a PAN Coordinator periodically generates beacon frames after every Beacon Interval (BI). In the non beacon enabled mode, all nodes can send their data by using an unslotted CSMA/CA mechanism which does not provide any time guarantees to deliver data frames.

The Physical Layer (PHY) is responsible for transmission and reception of data using a selected radio channel according to the defined modulation and spreading techniques. The spreading in all frequency bands is based on Direct Sequence Spread Spectrum (DSSS). The different modulation schemes are Binary Phase Shift Keying (BPSK), Amplitude Phase Shift Keying (ASK) and Offset Quaternary Phase Shift Keying (QPSK). The choice of a modulation scheme depends on the desired data rate.

The IEEE 802.15.4 MAC layer provides features like: beacon management, channel access, GTS management, frame validation, acknowledgment frame delivery, association, and disassociation. In the beacon enabled mode, the PAN Coordinator uses a superframe structure in order to manage the communication between its associated nodes. The superframe structure is defined by means of two parameters: *Beacon Order (BO)* and *Superframe Order (SO)*. The active period (superframe duration (SD)) is divided into 16 equally sized time slots for data transmission. Within the active period two medium access coordination functions are defined in IEEE 802.15.4: a mandatory Carrier Sense Multiple Access (CSMA) mechanism for the contention access period and an optional GTS mechanism for the Contention-free Period (CFP). The contention access phase shall start immediately after the beacon and complete before the beginning of the CFP on a superframe slot boundary. The CFP shall start on a slot boundary immediately after the CAP and it shall complete before the end of the active period of the superframe. The CFP can be activated by a request sent from a node to the PAN Coordinator.

1. *CSMA*: Two versions of CSMA/CA are defined, the unslotted for the non beacon-enabled mode and the slotted CSMA/CA for the beacon-enabled mode. For both versions it is based on backoff periods.
2. *GTS*: GTS provides real time guarantees for time sensitive applications. GTS can be activated by the request sent from a node to the PAN Coordinator. At the reception of this request, the PAN Coordinator checks whether there are sufficient resources available for the requested node in order to allocate requested time slot. Maximum of 7 GTSs can be allocated in one superframe.

Existing industrial solutions are described in the next two subsections. They are based on IEEE 802.15.4 and mainly targeting applications of the process automation domain and building automation, because during designing the IEEE 802.15.4 standard the focus was put on a very low power consumption of the nodes rather than on their real-time capabilities [93, 51].

### **WirelessHART and ISA 100.11a**

WirelessHART and ISA 100.11a are quite similar with only a few differences which are not relevant for this work (cf. [140]). Therefore, only Wireless HART is introduced here, since it is accepted as international standard IEC 62591 [59] since 2010 and gains a wider acceptance at the moment. WirelessHART [59] can be considered as the wireless extension of the Highway Addressable Remote Transducer (HART) protocol extensively deployed in process automation. The system is based on the 802.15.4 standard with several modifications of the MAC layer, a network layer, a transport layer and the HART application layer. The MAC is a combination of TDMA with a synchronized frequency hopping called time synchronized mesh protocol (TSMP). It defines time slots of 10 ms which are grouped into periodic superframes. The system is deployed in a mesh topology and gateways provide the access to the plant backbone network. The scheduling assigns different receive and transmit timeslots to individual devices and along certain routes in the network. The scheduling is done by a centralized network manager which is the core component of the wireless system and also responsible for a continuous monitoring and adaptation if necessary. Unfortunately, for both systems the network manager is not part of the standard and depends on proprietary implementations. The minimum achievable latency for both systems is approx. 100 ms but depends on the application [140].

### **Time Synchronized Channel Hopping and 6TiSCH**

Recently, the IEEE 802.15.4e [71] standard was introduced as an amendment of IEEE 802.15.4 which is targeting industrial applications. Its main features are the time synchronized channel hopping (TSCH) to increase the reliability of transmissions, being similar to TSMP, and reduce the energy consumption of nodes. TSCH is based on time slots which are typically 10 ms and grouped into one slot frame. The slotframe is periodically repeated. The mechanism requires that all nodes in the network are synchronized and adhere to a schedule which defines the time of transmission, time of reception, sleep time, etc. for each time slot. The mechanism also defines a channel offset for each slot which is used to calculate different transmission frequencies for consecutive slotframes resulting in a channel hopping. Due to the mesh topology of the network, the achievable latency is in the order of  $\geq 100$  ms [125]. The required accuracy of the clocks is in the range of 1 ms [159].

In this context the 6TiSCH activities within a new Internet Engineering Task Force (IETF) working group must be considered [134]. 6TiSCH is working on an architecture to use IPv6 in 802.15.4e based networks using an operation sublayer

<http://www.springer.com/978-3-662-49157-7>

Isochronous Wireless Network for Real-time  
Communication in Industrial Automation

Trsek, H.

2016, XIX, 170 p. 82 illus., 24 illus. in color., Softcover

ISBN: 978-3-662-49157-7