Connecting the Industrial Internet of Things
A QoS Model based Approach

Master-Arbeit
Dominik Schneider
KOM-M-0581

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Fachbereich Elektrotechnik
und Informationstechnik
Fachbereich Informatik (Zweitmitglied)

Fachgebiet Multimedia Kommunikation
Prof. Dr.-Ing. Ralf Steinmetz

Connecting the Industrial
Internet of Things
A QoS Model based Approach
Master-Arbeit
KOM-M-0581

Eingereicht von Dominik Schneider
Tag der Einreichung: 28. Februar 2017

Gutachter: Prof. Dr.-Ing. Ralf Steinmetz
Betreuer: The An Binh Nguyen
Externe Betreuer: Benjamin Kirchner, Daniel Goldfuss

Technische Universität Darmstadt
Fachbereich Elektrotechnik und Informationstechnik
Fachbereich Informatik (Zweitmitglied)

Fachgebiet Multimedia Kommunikation (KOM)
Prof. Dr.-Ing. Ralf Steinmetz

Ehrenwörtliche Erklärung

Hiermit versichere ich, die vorliegende Master-Arbeit ohne Hilfe Dritter und nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die aus den Quellen entnommen wurden, sind als solche kenntlich gemacht worden. Diese Arbeit hat in dieser oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen. Die schriftliche Fassung stimmt mit der elektronischen Fassung überein.

Darmstadt, den 28. Februar 2017 Dominik Schneider

Contents

List of Figures

List of Tables

Abstract

Driven by the Internet of Things (IoT), the integration of smart physical objects into the information network, the world around us becomes increasingly digitalized and connected. Also the industrial space seeks to introduce IoT systems, termed Industrial IoT (IIoT), to reap the potential benefits in efficiency and effectiveness of operations through real-time insights, big data analytics and saved costs from wireless instead of wired connections of devices. In general, wireless network technologies play a major role in the spread of IoT and IIoT. However, research about the traffic characteristics and the required quality of service (QoS) of the network in Industrial IoT networks is still very limited. At the same time, the number of connectivity options increases, especially with the advent of Low Power Wide Area Network (LPWAN) technologies, such as LoRaWAN.

All of this makes it challenging to pick the right wireless network technology for an Industrial IoT use case. Therefore, this research study aims to shed light on the broad wireless connectivity landscape and the selection of the right wireless network technology for Industrial IoT use cases. It will do so, by following a quality of service model based approach, that will be explained in the following. After giving background knowledge on Industrial IoT and connectivity technologies as well as reviewing and discussing related work to this thesis, a new QoS model for Industrial IoT is introduced. The developed model consists of QoS parameters, ten QoS classes and a taxonomy, that allows the easy classification of IIoT use cases. For the classification, the knowledge about required coverage and surrounding conditions, reliability, delay tolerance and message size is enough to classify a use case into one of the service classes. The classes are distinguished in those for global and local coverage and are numbered according to their criticality.

Next, a scoring model-based technology selection process was developed. For each of the defined QoS classes, a subset of technologies that meet the minimum requirements are preselected. The developed scoring model is able to calculate a score for each wireless technology in the subset. It also allows to include preferences, such as that the technology is provider operated (e.g. by a cellular service provider). The technology with the highest score is finally the proposed pick for the intended IIoT use case.

As a last part of this thesis, the quality of service of two popular wireless technologies, LTE and LoRaWAN, was experimentally evaluated in a real-world industrial setting. The QoS parameters coverage, reliability and supported message size were measured at eleven points on the production site of a large science and technology company. LTE achieved 100% coverage and proved to be an energy intensive and costly, but also reliable and universal connectivity option that could be used to connect applications across several QoS classes. On the other hand, LoRaWAN was only able to successfully connect in nine out of eleven measurement points and showed several shortcomings in terms of reliability, allowed message size and permitted duty cycle that limited it's use only to applications in the QoS class with the lowest message size and criticality.

To the knowledge of the author, this is the first research study that developed an end-to-end framework for the QoS based wireless technology selection for Industrial IoT use cases. Also the documented experimental evaluation of LTE and especially LoRaWAN in a real-world industrial environment was the first of it's kind. The results of this research study are valuable to research scholars and practitioners alike. The research community gains knowledge in the fields of traffic characteristics, QoS models and network selection procedures for Industrial IoT. Also the literature on LPWAN technologies is extended through the results on LoRaWAN performance in an industrial environment. Practitioners from the industrial world can use the models developed in this thesis as a starting point for their network planning process for IIoT solutions. Additionally, the experimental evaluation allows them to make more informed decisions about the choice of potential connectivity and LPWAN technologies.

1 Introduction

The world we're living in becomes increasingly digitalized and connected. A major driver behind this trend is the spread of the Internet of Things (IoT) - the integration of smart physical objects into the information network, to bridge the gap between the physical world and its digital twin in information systems [3]. The reader of this research study might already know consumer IoT systems such as smart light bulbs like Phillips Hue or intelligent heater controllers like the Nest thermostat, that can be monitored and controlled via smartphones. The next step is to bring such intelligent IoT systems also in the industrial space, then called Industrial IoT (IIoT), to reap the potential benefits in efficiency and effectiveness of operations. According to a study from Gartner, a total of 26 billion devices will be connected by 2020 [4]. IIoT systems are thereby expected to generate three types of return on investment (ROI) [5]. While the first two types are stemming from increased efficiencies due to real-time insights and big data analytics, the third potential ROI comes from saved capital and operational expenditures through wireless, instead of wired networks.

In their highly cited papers, also Atzori et al. [6], Gubbi et al. [7] and Xu et al. [8] see open wireless technologies as a driving force in the spread of the internet of things. At the same time, the landscape of available wireless connectivity technologies has broadened tremendously [9]. Short-range wireless networks as Bluetooth Low Energy or IEEE 802.15.4 based systems, new WiFi standards as IEEE 802.11ah as well as energy sensitive cellular connectivity technologies like NB IoT are only some examples. The advent of Low Power Wide Area Network (LPWAN) technologies created an entire class of new connectivity options, with LoRaWAN as one of the currently most widespread ones [10].

But which of the available and upcoming wireless network technologies is the best pick for a specific Industrial IoT system, also in consideration of the increased demand on reliability, scalability and security in harsh industrial environments? The answer to this question has not directly been addressed in the literature so far. It is however tied to the type of network traffic that the IIoT system generates and to the demands of the IIoT system on the quality of the network service, also termed solely quality of service (QoS). While QoS has been extensively researched for networks of human-to-machine communication (H2M, e.g. web-browsing or video-streaming), the field of machine-to-machine (M2M) communication, that is dominant in the IoT field, is still underresearched. As such, Gubbi et al. [7], Rawat et al. [11] and Ray et al. [12] see QoS in IoT systems and Industrial IoT systems in particular as an open challenge. Also Xu et al. [8] stress the heterogeneous QoS demands of IoT on the network and their importance for the flawless operation of the IoT system. Likewise, Atzori et al. [6] demand for more research on traffic characterization in IoT networks, as the characteristics of traffic that flows through IoT is rather unknown, but very important for an adequate network planning. In the industrial space of IIoT, this is even more the case.

Therefore, this research study aims to shed light on the broad wireless connectivity landscape and the selection of the right wireless network technology for Industrial IoT use cases. It will do so, by following a quality of service model based approach, that builds on a set of QoS parameters and specifies ten QoS classes. The overall objective of this thesis is twofold. The first one is to develop an end-to-end framework that guides through the entire technology selection process, which is achieved by the development of a QoS model, including a QoS taxonomy, and a scoring model for wireless technologies. The second objective is to provide real-world evidence on the capabilities of currently trending technologies to adhere to the specified QoS classes, which is done by an experimental evaluation of LTE and LoRaWAN in an industrial environment.

The remainder of this thesis is as follows. Next on, chapter 2 introduces relevant background knowledge, by presenting an overview of the Industrial Internet of Things, an IIoT architecture and potential use cases for Industrial IoT. Also detailed information on basics, constraints and technologies for wireless networks, relevant to IIoT, are given. After that, the four major parts of this research study

follow. First, chapter 3 provides a thorough overview about related work on constraints on quality of service in Industrial IoT environments and about previous QoS models. Also, the related work is reviewed and discussed. Chapter 4 introduces the developed QoS model, that specifies ten service classes and incorporates a taxonomy to allow the easy selection of the correct service class for a use case. In chapter 5, a scoring model based wireless technology selection process is developed, that enables to pick the best connectivity technology for a certain service class. To study the performance of currently upcoming technologies relevant for IIoT, chapter 6 presents an experimental evaluation in a real-world industrial setting of LTE and LoRaWAN, as a major LPWAN technology. The results of the measurements of important QoS parameters and their suitability for the specified QoS classes is stated as well. Finally, chapter 7 presents limitations, contribution and conclusion of this research study. As a last step, an overview of potential future work and an outlook of future technologies is given.

2 Background

In this chapter, an overview of the Industrial Internet of Things (IIoT) and wireless network technology is presented, to provide the contextual foundation of this research study. The chapter starts with a definition of Industrial Internet of Things, goes on with possible use cases for Industrial IoT and presents an IIoT architecture. Finally, basics and constraints of wireless networking options are presented, along with an overview of relevant wireless network technologies for the Industrial Internet of Things.

2.1 Overview of Industrial Internet of Things

The Internet of Things (IoT) in general can be seen as a far-reaching vision that has technological as well as societal implications [13]. In the highly cited paper of Gubbi et al. [7], it is defined as the interconnection of sensing and actuating devices that provide the ability to share information across platforms and thereby enable innovative applications. According to them, this is achieved by large scale sensing, combined with data analytics and information representation by leveraging the power of ubiquitous sensing and cloud computing.

The term Internet of Things was originally coined at the MIT Auto-ID Center in 1999 with the vision to tag every object in the physical world with a globally unique ID, that can be sensed by the means of RFID (Radio Frequency Identification) [3]. Since then, the meaning of IoT has been broadened dramatically, thanks to the increasing number of sophisticated hardware and software combinations.

Atzori et al. [6] divide IoT into three perspectives. The first is the *Internet* based perspective, that views IoT as as a world-wide network that is based on standard communication protocols. The second perspective is *things* based and has an emphasis on specific enabling technologies like sensor and actuator devices and the technical details associated with them. Finally, there is the *semantics* oriented perspective, that embodies the data analytics part such as reasoning over data [6]. The connectivity of sensing and actuating devices, also termed Machine to Machine (M2M) communication, is located on the overlap of the Internet and the things based perspective, meaning that both perspectives are relevant for this thesis (Figure 2.1). As the focus is on the connectivity part, the semantics and data-analytics perspective will not be covered in this research study.

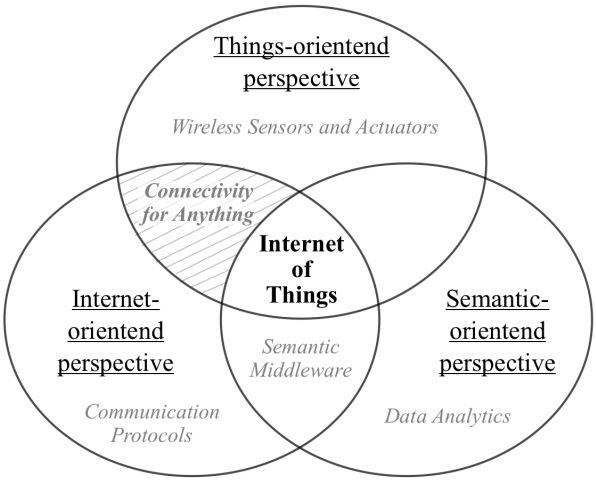

Figure 2.1.: Three Perspectives on the Internet of Things [6].

The *Industrial* Internet of Things (IIoT) is the convergence of the Internet of Things with industrial applications and enterprise systems. While IoT is a very broad term, that spans use cases from the

smart home over smart museums to assisted driving [6], Industrial IoT is more focused on business use cases in industrial ecosystems and therefore has greater demands on reliability, scalability, availability and security of the IoT system. In Germany, the term "Industry 4.0" was introduced at the Hannover Messe in 2011, which covers the field of cyberphysical production systems. After the first three industrial revolutions driven by steam engines, electrification and the first steps towards digital programming of automated manufacturing systems, Industry 4.0 is announced as the fourth industrial revolution, that brings internet technology in the industry [14]. As such, it is closely related to Industrial IoT.

Global spending on IIoT is expected to reach $500 billion by 2020, making it a major market in the ICT landscape, and optimistic predictions assume that it can create value of around $15 trillion of global GDP by 2030 [15]. The Return-on-Investment stems from improved efficiencies due to real-time information, deeper insights from big data analytics and saved costs from less cable installations and maintenance efforts [5]. Enterprises in the industries of manufacturing, mining, agriculture, oil and gas, and utilities are affected, as well as service providers for healthcare, logistics and transportation [15]. In this thesis, the focus will be on manufacturing industries, as these are the industries with the highest export rates in Germany [16]. The manufacturing industry domain can be split in companies that conduct process manufacturing versus discrete manufacturing. In *process manufacturing*, the production process takes place in a continuous manner and materials are chosen according to a formulae or recipe. Examples are oil and gas, steel, chemicals and pharmaceuticals. In *discrete manufacturing*, the products are assembled in discrete steps by using a bill of materials. Examples are the automotive, furniture or consumer electronics industries and the assembly usually depends on robotics and conveyor belts [17][18]. Although there are overlaps in the use cases and requirements in these segments considering IoT solutions, they are usually examined separately. An overview of use cases will be presented in section 2.3.

After introducing the general concept of Industrial Internet of Things, the next section will give an overview of the architecture and components of these systems.

2.2 Industrial IoT Architecture

In terms of the basic components required for operations, Industrial IoT systems are comparable to consumer grade IoT systems, such as smart home equipment or digital assistants as Amazon Echo. Porter and Heppelmann [19] provide a good overview of the required building blocks (Figure 2.2). Other architectural overviews of IoT are provided by Atzori et al. [6], Al-Fuqaha et al. [20] or Gubbi et al. [7]. However the framework of Porter and Heppelmann [19] is chosen here, because it provides the most complete overview of the various components and it was also chosen by other IoT researchers, such as e.g. Wortmann and Flüchter [21].

As illustrated in figure 2.2, the Internet of Things consist of three main layers: the thing or device layer (where the data is generated by sensors), the connectivity layer, that provides the connection of the thing to the IoT platform, and the IoT cloud and platform layer, where the sensed data is stored and processed and commands are sent down to the device. As shown, the identity and security functions are important across all layers and play a major role in the IoT area. On the other side, also the integration of the generated data from sensors with data from business systems (such as SAP ERP system) or other external sources (such as e.g. weather data) are important, to generate additional insights and improve the decision making. Relevant for this thesis are especially the connectivity and things layers, that connect the sensor or actuator devices to a cloud service. For a discussion of other layers, surveys are provided by Gubbi et al. [7] and Al-Fuqaha et al. [20].

Though the term "Internet of Things" is rather new, the transfer of sensor values via wireless networks has already concerned ample of researchers in the field of Wireless Sensor Networks (WSN). Today, WSNs can be seen as a major part of IoT, as also reflected in the highly cited paper of Gubbi et al. [7]. WSNs are covered by the connectivity and things layer in the architecture of Porter and Heppelmann (Figure 2.2). They are composed of several field devices ("nodes") that are equipped with sensors and

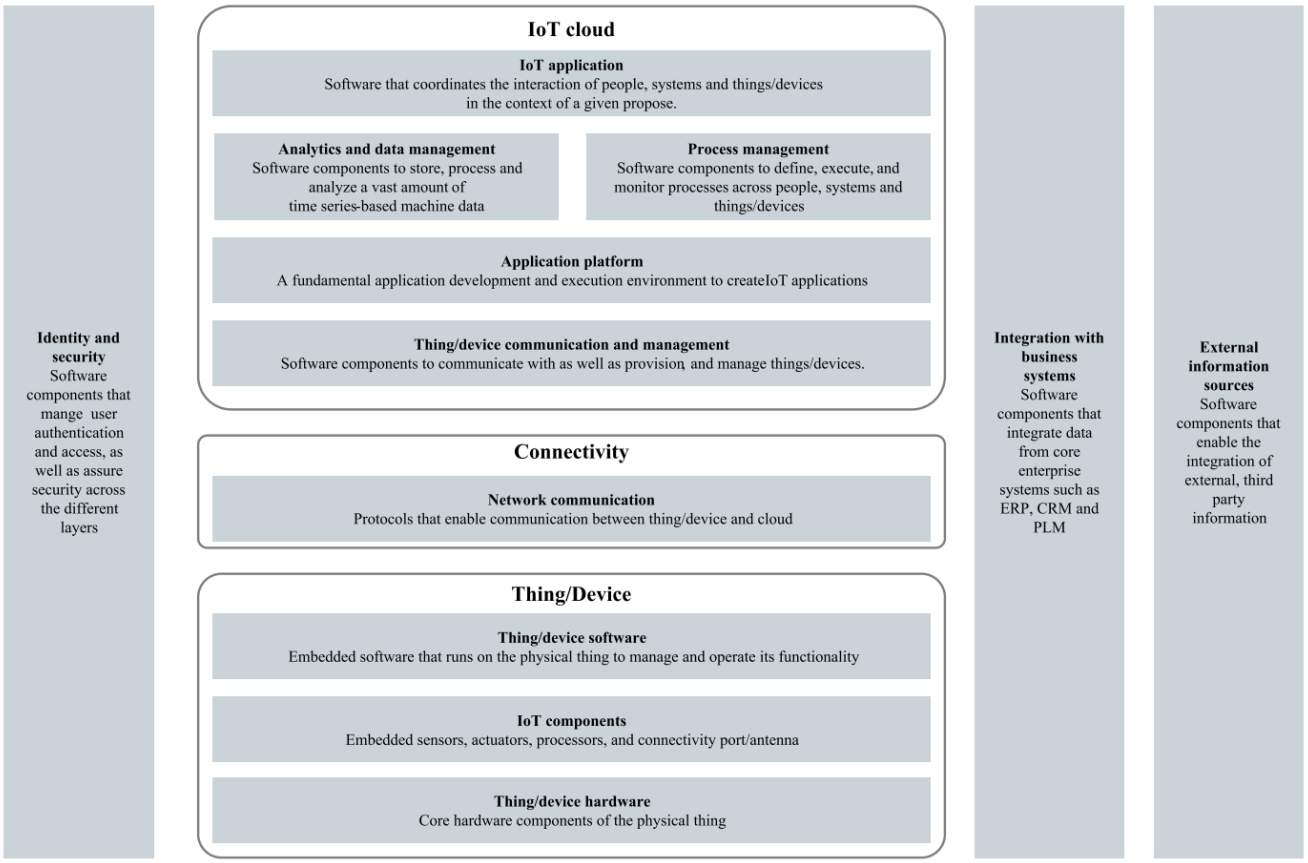

Figure 2.2.: IoT Architecture Components [19].

are wirelessly connected to a gateway, that is the intermediary to a backend service, such as a cloud platform in the Internet (Figure 2.3). The wireless connectivity thereby has a number of advantages over a wired connection, such as greater mobility, better scalability and less maintenance work with broken cable links. A detailed discussion of wireless networks will be given in section 2.4. Though the gateway in the network was originally mainly a network bridge between the nodes and a cloud service, a current trend is to bring more intelligence to the edges of the network and leverage the gateway as a kind of intermediate cloud, that provides local capabilities for processing and decision making. This greatly improves the delay performance of applications and is also known as fog computing [20].

In Industrial Internet of Things systems, the nodes in the field might also have the ability to carry out actions, like closing a valve or power up an engine. These nodes are then called actuator devices and the whole network is called Wireless Sensor and Actuator Network (WSAN). WSANs are a subclass of Industrial Wireless Sensor Networks (IWSN) [22]. Especially here, fog computing is of interest, as control applications are very delay sensitive and require timely responses of the actuator nodes.

The connection between the gateway and a cloud platform is usually achieved by an IPv4 or IPv6 based backhaul network, that relies on proven network technologies as cable based Ethernet, WiFi or LTE [10]. On the other hand, a growing number of options are developed to connect the network nodes in form of IIoT devices and a gateway (which can also be a gateway operated by a mobile service provider for cellular services as 3G/LTE). The emphasis in this thesis is therefore on the wireless connection between the gateway and the nodes, to gain greater understanding of the different traffic and network types that are relevant here. Before a review of existing wireless connectivity technologies follows in section 2.4, the next section gives an overview of use cases and scenarios for IIoT and Industrial WSN. These scenarios will later form the baseline of the Quality of Service models developed in this thesis.

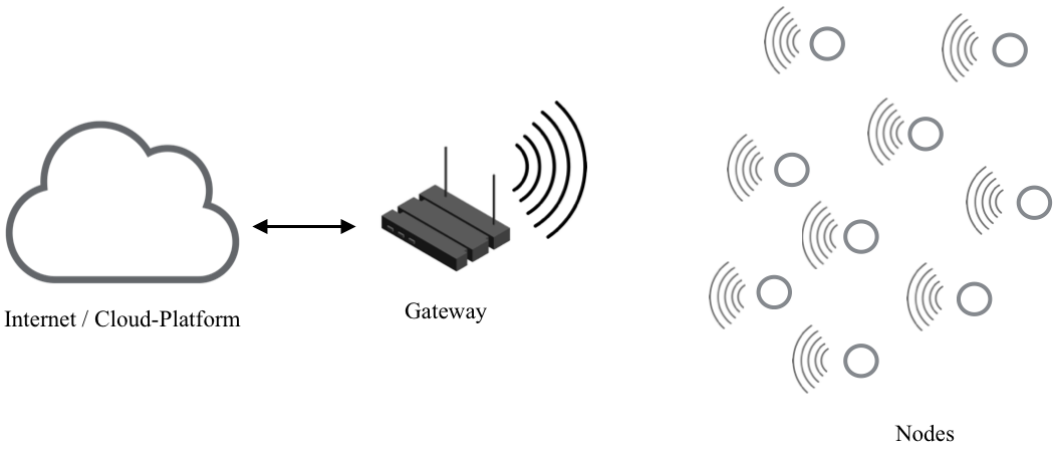

Figure 2.3.: Components of Wireless Sensor Networks as Connectivity Layer in Industrial IoT Systems (Adapted from [23]).

2.3 Industrial IoT Use Cases

Use cases in the field of Industrial IoT can fall into two categories. The first one is the inclusion of IoT capabilities in the product. This means, that the goods that are produced by a company include sensors or actuator functionalities and are connected to a cloud or fog platform. The second category is the usage of IoT in the production process, for example by connecting the machinery that is used in production or by tracking the assets along the route to the customer. Detailed use cases will be presented in the following. An identifier will be assigned to each use case (UC), based on whether they fall into the product (UCPd) or process category (UcPc). The identifier will later be used to reference the use cases that form the basis of the developed IIoT QoS model in section 4.

2.3.1 IoT in the Product

Although ample of currently available products incorporate IoT functionalities, not all of them belong to the class of Industrial IoT. A lot of them are consumer devices like wearables, smart home equipment and entertainment accessory. Examples are the Amazon Echo smart assistant, Phillips Hue light bulbs or the Apple Watch. Usually these consumer IoT devices are sold in small quantities to individuals or families. On the other hand, IIoT products are targeted towards institutions and companies and are usually sold in larger batches to cover the demand of the entire organization. For companies in the *discrete manufacturing* industries, one possibility is to sell products with integrated sensors in a field where monitoring is the main driver of business value, such as medical devices (UCPd01) [19]. In other fields, the sensors can be used to see how the product is used (UCPd02), to deliver predictive maintenance (UCPd03) and to improve the customer support (UCPd04) by having the information about faulty parts directly at hand [19] [24]. As an example, General Electric connects their wind turbines with their Predix IoT platform, to adjust the blades for maximizing the gained wind power and to provide diagnostic reports [25]. Additionally the manufacturer gains the possibility to implement pay-as-you-go pricing models for their products (UCPd05), as Rolls Royce did for their jet engines with a "TotalCare" program. Their jet engines are connected to the Microsoft Azure IoT platform to submit data about the runtime and health of the engines, to provide add-on services like fixing broken engines and insights like fuel-efficiency [26].

In the *process manufacturing* industries, a direct inclusion of IoT in the product itself is (currently) not possible. One option here is to include sensor devices in the packaging (UCPd06), to track the conditions and the consumption of the product. Examples are chemicals or oil packaging solutions.

The entire class of IIoT products, that target industrial use cases and are not sold to consumers, but to professionals or companies, is also called *commercial IoT* [27].

2.3.2 IoT in the Process

Additional to the inclusion of IoT capabilities in the final product, enterprises also have the possibility to leverage the power of IoT already in the manufacturing process and in the previous and following process steps. This can help to increase efficiencies and effectiveness of the production process and the operations of the company.

Beginning with the *supply chain*, it's possible for a manufacturer to ensure the physical integrity and quality of the transported goods along the transportation route (UCPc01), as well as the integrity of the route itself (UCPc02). Also the compliance to legal regulations, internal policies and service level agreements can be assured (UCPc03)[3]. This can be done, by a global tracking of assets and transportation vehicles, e.g. through GPS or indoor-location systems (UCPc04).

Furthermore there are several usage scenarios that affect discrete manufacturing and process industries alike. IIoT can be used for *process and equipment monitoring*, by deploying a wireless sensor network (WSN) that senses temperature, pressure, vibrations or power usage of machinery equipment [28] [29]. For example, Intel monitors the condition of their semiconductor fabrication equipment, GM observes their conveyor belts and machinery and Honeywell tracks the furnace temperature of their steel mills [28] [30]. With the deployment of WSNs, faulty parts that are due for a repair can be detected more easily, e.g. by analyzing their vibration "signature". Potential problems can be forwarded to the plant personnel, to carry out predictive maintenance tasks before the plant efficiency drops or the entire production has to be halted unexpectedly (UCPc05) [31] [32].

Also the general *monitoring of the environment* is possible. Here, the monitoring of the indoor (UCPc06) or outdoor (UCPc07) environment is possible [31]. For indoor monitoring, a further breakdown in systems that provide emergency services (UCPc08), like systems for fire safety, and general monitoring and information gathering systems (UCPc09) is possible [22].

As Hou and Bergmann [33] state, industries could *reduce energy consumption* of motor system by up to 18%, by using condition monitoring for induction motors that measure temperature and vibration signals. Potter et al. [29] see possibilities in this direction as well, by leveraging smart metering (UCPc10), smart power control systems (UCPc11) and efficient use of utilities (UCPc12).

On an aggregated level, the generated data can be used to *maintain statistics* on the expected production rates, quality parameters and volumes of a production plant (UCPc13). Like this, the logistics coordination inside the plant (UCPc14) and an automation of the plant processes becomes possible (UCPc15). Also a more detailed business oriented *model of the plant operations* can be generated to forecast expenditure, expansions (UCPc16) and get insights on the effects of other changes (UCPc17) [29].

Next to the possibility to generate data by deploying a pure WSN, the usage of wireless sensors and actuator networks, that also serve *control purposes* is one of the main scenarios for Industrial IoT [22] [34]. In the process manufacturing industries, closed loop control (UCPc18) and control by interlocks (UCPc19) can be distinguished. In closed loop control, the intent is to stabilize a normally unstable process (such as in the production of chemicals), while control by interlocks is used to issue start, stop and safety stop commands to machines [17]. In discrete manufacturing, also the coordination and control of fixed or mobile robots can be achieved (UCPc20), next to the control of conveyor belts, machinery and other manufacturing equipment (UCPc21) [28] [34].

An improved *inventory management* is an additional use case. Locality and quantity information of items (UCPc22) can be achieved through radio frequency identification (RFID) or bar code scanners. This enables an efficient localization and tracking of unfinished parts or containerized raw materials (UCPc23) [34] [31].

To sum up, several usage scenarios for the Internet of Things are possible in the industrial domain. IoT in the product, also termed commercial IoT, enables to track the usage and consumption, deliver predictive maintenance and additional support to customers, as well as implementing new business models. With IoT in the process, equipment and process monitoring, measuring of environment conditions, improved inventory and supply chain management are possible. This can lead to reduced energy consumption and enables to maintain plant statistics and models. With the deployment of actuator devices in the field, a manufacturing process control can be implemented, which leads to realizing the vision of the autonomous smart factory [35].

2.4 Wireless Networks for Industrial IoT

After reviewing potential IIoT use cases, this section is concerned with the wireless network technology than can be used to connect the devices in the field.

The first question to be asked should be, why it could be advantageous to have wireless connectivity at all, instead of a wired connection of sensor and actuator devices?

A major driver of wireless solutions are the high costs, that come with the installation (capital expenditure) and maintenance (operational expenditure) of wires in an industrial environment [17] [36]. One meter of wire for new a green field installation costs about $200 in an average production plant. In highly regulated or harsh environments, these costs can exceed $3000 per meter, accumulating to up to 80% of total system costs [17] [36] [37]. These high installation costs lead to a limited scalability of the number of deployed sensor and actuator nodes. If one has to deploy cables to every single sensor, large scale deployments are not feasible. On the other hand, the deployment of additional WSAN nodes is comparably easy and cost efficient, as the placement of the sensor node is more flexible with the wireless connection channel. The primary source of high maintenance costs for wired connections are broken connectors that link different wires together. Additionally, corrosion, burned cabling and other issues occur so that inspections, testing and troubleshooting becomes necessary [17] [36] [38] [37].

Next to costs, the constraints that are caused by the wire itself are tackled. Installation of sensors on rotating equipment and in sealed containers becomes possible. Also the mobility of nodes is feasible, allowing for example the tracking of assets, the easy reconfiguration of assembly lines or the temporary measurement of certain process values [17] [36] [38] [37].

The remainder of the section is as following. First, basics of wireless networking will be presented, to understand the impact of implementation decisions of various wireless connectivity technologies. Next, constraints of wireless networks in the industrial environment will be reviewed, after listing the drawbacks of wired connections above. Finally, popular and upcoming wireless technologies that are relevant for IIoT are introduced.

2.4.1 Basics

Network technologies are composed of different protocols, that define the format and order of exchanged messages and that serve dedicated functions. These protocols can be organized into layers, forming a protocol stack (Table 2.1). Each protocol performs its functions within the layer and uses the functions of the layer below it [39]. The following overview of the network protocol stack only covers the most important techniques that are relevant for this thesis. The interested reader can find more detailed information in the books of Akyildiz and Vuran [23] and Kurose and Ross [39].

At the lowest level of the protocol stack is the *physical layer*. It is responsible for moving the individual bits from one node to another, by converting them so that they can be transferred via electromagnetic signals on the radio frequency (RF) bands. The RF bands span from 3Hz to 300GHz, with dedicated ISM (Industrial, Scientific, Medical) bands that are internationally or locally reserved and free to use without licensing costs. Other bands are reserved, e.g. for mobile communication providers like Deutsche Telekom or Vodafone. Different classes of modulation techniques exist to transform the digital bits into analog signals, usually in a waveform. The three most important classes are narrowband (NB), ultra-wideband (UWB) and spread-spectrum technologies. While NB networks employ a bandwidth of usually less than 200kHZ in a dedicated frequency band to transmit the data, UWB networks spread the information over a larger bandwidth of more than 500 MHz. Spread spectrum technologies combine both techniques, by spreading a narrowband signal over a larger frequency band. This can be done by a random hopping of the NB signal in the frequency band, as in Frequency Hopping Spread Spectrum (FHSS), or by actually "spreading out" the signal over the whole band by using a spreading code, as in Direct Sequence Spread Spectrum (DSSS). These spread spectrum techniques are considered as more

Layer	Function	Transmit Unit
Application Layer	Main application functionalities, APIs	Data
Transport Layer	Congestion control, Reliable transport	Segment (TCP) / Datagram (UDP)
Network Layer	Routing	Packet
Link Layer	Medium Access Control, Reliable delivery, Error correction	Frame
Physical Layer	Frequency selection, Modulation, Data encryption	Bit

Table 2.1.: Network Protocol Stack [39].

prone to interference with other RF signals and harder to attack by eavesdropping or jamming [23] [39] [40].

As soon as the signal is in the air, multiple nodes might compete for sending their data over the same wireless channel (same frequency and same bandwidth). To coordinate the broadcasting of the wireless signals and avoid collisions of bit-frames by different senders, the *link layer* provides protocols for Medium Access Control (MAC). Three classes of MAC protocols exist, namely channel partitioning protocols, random access protocols and taking-turn protocols. Channel partitioning protocols divide the resources appropriately among the sensor nodes and examples are Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA). FDMA techniques are not appropriate for WSNs and do not provide high efficiencies, due to the limited channel bandwidth for each node. Contrary to the procedure with fixed channel partitioning, where each node has a reserved channel, nodes in networks with random access protocols immediately transmit their data into the channel at full rate and sense for possible collisions. Examples are ALOHA and Carriers Sense Multiple Access (CSMA). However, CSMA becomes less effective in networks with a larger number of nodes and is therefore less suited for the use in WSNs. In taking-turn MAC protocols, each node knows exactly when it is its turn to send, either by a polling mechanism of a master node or by a token that is passed to the node. Hybrid schemes, that combine various approaches, are also possible [23] [22] [39] [40].

Another function that is provided by the link layer is the control for bit-level errors by using error detection bits in the frame. The ability to detect and correct errors is known as forward error correction (FEC) and enables the correct recovery of the message without retransmission. Nevertheless, the error detection bits add overhead to the frame. Next to FEC, Automatic Repeat Request (ARP) is another technique for error control, that relies on feedback from the receiver (acknowledgements) and the retransmission of corrupted frames. Usually, a cyclic redundancy check (CRC) is performed to check if the frame is delivered correctly or not. Due to the necessary retransmissions in case of errors, additional latency reduces the real-time capabilities of ARP compared to FEC techniques [23] [32] [39] [34].

Now that a successful transmission between two entities in the network is accomplished, the *network layer* is responsible for routing the message to the correct destination. Two criteria impact the routing of the network packages: whether one or multiple wireless hops have to be crossed to reach the destination and whether there is infrastructure, such as a base station, in the network. For infrastructure-less technologies, especially the single-hop networks are of interest, as multi-hop networks induce additional complexity and latency in the network [10]. Although no base station is

present in the single-hop networks, one (master) node may coordinate the transmission with several other nodes, as it's the case with Bluetooth. On the other hand, infrastructure based technologies include a base station that is connected to a larger network, such as the Internet. In single hop networks, a direct connection of a node to a base station is given. This is know as star network topology. In multi-hop networks, nodes have to relay their communication through other nodes to deliver the message to the base station. This is also called mesh network topology. Hybrid approaches such as tree or star-of-star network topologies are possible [39] [37] .

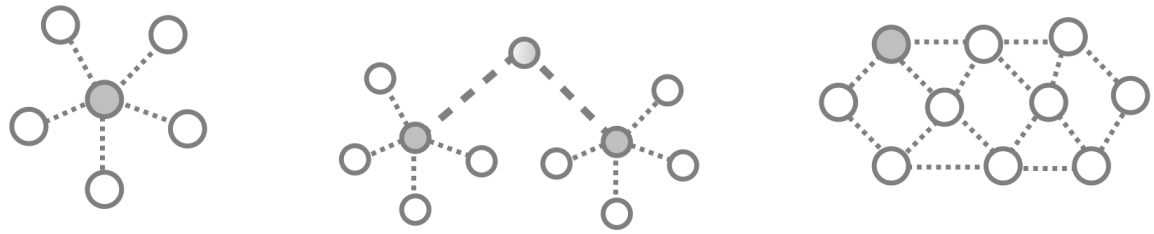

Figure 2.4.: Network Topologies (Adapted from [37]).

White circles: nodes; Grey circles: base stations/gateways.

The consideration of topology is important, as it directly affects scalability, energy efficiency, reliability and latency. Although star topologies are prone to a single point of failure and are less reliable than mesh networks, they have serious advantages in terms of energy efficiency and latency. Also deployment of devices is easier and costs for a huge number of geographically distributed devices is much lower for star topologies. The star-of-star networks combines the advantages of both approaches, which results in better scalability of the network [38] [40] [41] [37].

Energy efficiency is an important criteria for battery powered IoT devices in the field. Though actuator nodes usually have access to the power supply of the actuator, sensor nodes are battery powered in most of the cases. As the transceiver of the wireless signal is the most energy-demanding unit of the device, decisions regarding the wireless technology have a huge impact on the node's battery lifetime. Next to the already discussed star topologies and lightweight medium access mechanisms, duty cycle strategies are another way to bring down the power consumption. Radio duty cycling allows to turn off the transceiver when it is not required. Although it allows to save energy, legislative rules in certain regions that force duty cycling can also limit the applicability for some use cases [38] [40].

After reviewing the basics of wireless networking, covering the network stack, network topologies and energy efficiency, several constraints in the field of industrial wireless networking will be explained.

2.4.2 Constraints

Compared to wired networks, a number of constraints have to be taken into account when wireless connectivity technologies are used. First, the natural decrease in signal strength, the path loss, is much higher in wireless networks and interferences from other sources have a further impact. Additional blurring of the obtained signal occurs at the receiver through multipath propagation, when the radio signal reaches the receiver antenna by more than one path due to the signal reflection at objects. One example of interference by other nodes is when node A and node C can't detect each others signal due to a physical obstacle, but both signals interfere at node B. This is called the hidden terminal problem. The case when node A and node C can't sense each others signal because of low signal strength at their location, but both signals interfere at a node B between them, is called fading. All mentioned problems lead to bit-errors that need to be recovered to ensure a proper communication [39].

Industrial IoT is a highly sensitive field, where security is of utmost importance. As the wireless signal propagates through the air in every direction and doesn't stop at plant boundaries, wireless networking makes additional security considerations necessary. Possible attacks on the wireless link can be distinguished in passive and active attacks. In passive attacks, an attacker continuously collects information from the network by eavesdropping the passing traffic. While those attacks can corrupt the confidentiality of information such as data and routing information, they can not be detected due to their passive nature. By using the captured data for traffic analysis, the attacker can infer information about the location of a base station and the network topology [42] [43] [44].

By using active attacks, an attacker can damage the system in more severe ways. Most common are denial of service (DoS) attacks, where the capacity of the network to perform the desired function is diminished or eliminated completely. On the physical layer, this can be done by jamming: causing a lot of interference on the wireless channel through the transmission of radio signals. One layer up, the communication protocol on the link layer can be violated by generating collisions that require retransmissions. The routing layer, e.g. in a mesh network, can be affected by simply refusing to route messages or by routing them to incorrect nodes. Further attacks on upper layers are possible. Next to DoS, Man-in-the-Middle attacks, replay attacks of transmitted messages and sybil attacks, where a node uses multiple identities, are further threats. Although the impact of such active attacks is more severe, a detection of them and the launch of countermeasures is possible for attacks on the link layer and up. Attacks on the physical layer, as jamming on a broad spectrum, are impossible to prevent and hard to tackle. Even in only sporadic attacks, they can cause severe damage in time-critical environments, such as factory automation systems [42] [43] [44].

Next to security issues, the harsh conditions in the industrial domain have to be taken into consideration. Additional to possible variations in temperature, pressure and humidity or the impact of vibrations and noise, the above average rate of interference causes big problems for the wireless connectivity. Sources of interference can be of broadband or narrowband nature. Broadband interference signals cover all frequencies with high energy and can stem from motors, welding equipment, voltage regulators or pulse generators. Contrary, narrowband interference has lower energy and originates from UPS (uninterruptible power supply) systems, signal generators or strong power-lines, but can cause signal corruption nevertheless. As already said, spread spectrum modulation techniques, especially FHSS, is to some extend resistant against interference sources [28] [34].

From the previous section, we know that certain regulations in some regions of the world exist regarding the allowed duty cycle in unlicensed ISM frequency bands. This is done to assure that the shared license-free frequency channel can also be used by other devices. Additionally, limits on the effective radiated power (erp) of the antenna can apply. In Europe, the ETSI EN 300 220-x standard (in version 3.1.1 as of December 2016), determines the channel access and transmit power for devices that operate in the range of 20 to 1000 MHz. For the popular 868.0-868.6 MHz ISM band, a 1% duty cycle rule applies, meaning that a device can only transmit data for 1% (or 36 seconds) of an hour. Alternatively listen-before-talk techniques for "polite spectrum access" have to be used. Also the maximum erp transmission power is 25 mW and the originally use case for this band was the transmission of alarm signals. On the other hand, for the 2.4 GHz ISM band, no duty cycle rules are given [45] [46] [47].

Also the scalability of wireless networks is limited. Though no constraints due to the costly installation of cables arise, only a limited number of nodes can share a wireless channel. Therefore, the spectrum efficiency, as the relation of throughput and channel bandwidth, and the used channel access mechanism of the wireless technology are critical [48].

2.4.3 Technologies

Finally, different wireless connectivity technologies that are relevant for the Industrial Internet of Things are presented. Later on, appropriate technologies for the different QoS classes are selected based on the following overview of wireless connectivity options.

Based on Raza et al. [40], wireless networks for IoT are classified into Short-Range Wireless Networks, Wireless Local Area Networks, Low Power Wide Area Networks and Cellular Networks.

Short-Range Wireless Networks

Technologies that (originally) have limited coverage and may cover the direct workspace of a person or the room the person is in, fall into the category of short-range wireless networks.

Bluetooth is a popular short-range networking technology, as it is already included in a lot of devices such as smartphones, tablet computers and notebooks. It operates in the 2.4 GHz ISM band, uses FHSS channel hopping modulation and TDMA for channel access. From version 4.0 on, it can operate in an Basic Rate/Enhanced Data Rate or in a Low Energy (LE) mode, of which the last one is most interesting in the IoT domain. Both, Forward Error Correction and Automatic Repeat Requests are used to ensure the correct data transmission. A single-hop star-topology, called piconet, with one master-device and up to seven active slave devices is the default network topology, although a Smart Mesh working group was formed by the Bluetooth Special Interest Group in 2015. Since version 4.2 the security has been enhanced, by introducing Elliptical Curve Diffie-Hellman(ECDH) key exchange, data signing and 128 bit AES-CCM encryption. The throughput of 1 Mb/s, very low latency and ranges up to 200 meter make Bluetooth LE a very interesting connectivity option for some use cases. In fact, it is expected to become the de facto standard for short-range IoT devices, that may be the core of commercial IoT products [49] [5] [11] [39].

The class of short-range technologies that are based on the *IEEE 802.15.4* physical and MAC layer specifications are relevant as well. Available standarts here are ZigBee, WirelessHART and ISA100.11a. While ZigBee focuses more on the consumer IoT side, WirelessHART and ISA100.11a are two standards that directly target the industrial domain. While WirelessHART was designed specifically for the process industry, ISA100.11a is more general. Both are defined in the 2.4 GHz band, use a combination of DSSS and FHSS modulation and TDMA for channel access. The default topology is a multi-hop mesh network that consist of up to several thousand nodes, one or more gateways at the edges of the network, a network management service and a security management service. The ISA 100.11a standard additionally requires backbone routers and a system time source. The throughput for both standards is 250 kb/s with a coverage range of up to 100 m per node. As both are targeted towards the industrial environment, they were designed for robust and reliable communication and come with security mechanisms such as 128-bit AES-CCM encryption, message authentication and key management. Despite the high reliability of both standards, several factors limit their applicability in the industrial domain. Due to the shared use of the 2.4 GHz ISM band with other technologies such as cordless telephones, Bluetooth or WiFi, and limited transmission power it can be expected that the message delivery over a large and congested distance can be challenging. Additionally, the mesh topology is problematic with the real-time requirements of industrial automation use cases, where the required roundtrip latency is usually in the range of 10ms [50]. Although ISA100.11a has a low latency of only 10ms per hop, this can frequently add up when several hops are necessary to reach the destination. As the network grows, further problems such as management complexity, interference issues and routing overhead become evident [51] [11] [41] [52].

Wireless Local Area Networks

The class of wireless LAN technology is defined by the IEEE 802.11 standard set and is also known as WiFi. It operates in the 2.4 GHz or 5 GHz ISM band, uses DSSS modulation and CSMA with Collision Avoidance (CSMA/CA) for channel access. By using a star topology, it was originally designed to provide high throughput to deliver multimedia content to a limited number of indoor devices such as notebooks and computers. Therefore, the current IEEE 802.11n standard supports up to 600 Mb/s and 802.11ac even up to 6933 Mb/s in the 5 GHz band. Next to the fact that such high data rates are not necessary in most IoT use cases, where message sizes are comparably small, they come at the price of large energy consumption. With the current work on the IEEE 802.11ah standard, this could change. IEEE 802.11ah is a low-power WiFi that is based on the physical and MAC layer design of 802.11n & ac, but operates in a sub-1GHz ISM band (863-868 MHz in Europe) to cover a wider range of up to 1 km. Data rates of at least 100 kB/s and a better scalability are targeted, to support a larger number of connected devices (up to 8191) than it was possible before. IP based communication will work out-of-the-box and device and network authentication based on the Extensible Authentication Protocol (EAP) as well as AES encryption of traffic will be available. As the sub-1GHz band is also used by other techniques, duty cycle regulations and other limitations apply, that limit the transmission frequency and applicability. While the standard is still in draft, with a deadline of December 2016, no commercially available hardware is on the market as of early 2017 [9] [39] [5] [53].

Low Power Wide Area Networks

Previously, mesh networks, based on the IEEE 802.15.4 specification, have been the primary option to connect a larger field of distributed sensor and actuator nodes. With the advent of Low Power Wide Area Networks (LPWAN), this is going to change. LPWAN technologies allow the energy efficient, low cost connection of several thousands of nodes, thousands of meters away from the base station. As the LPWAN market is rather new, several technologies exist that compete against each other.

Among the most popular of them is the *LoRa*® standard (abbreviation for Long Range), that is patented and licensed out by SemTech. LoRa® defines the physical layer of the network stack, operates in the 868 MHz ISM band in Europe and uses a proprietary chirp spread spectrum (CSS) technique. Multiple spreading factors are offered to provide a tradeoff between data rate and range, resulting in a throughput of up to 37.5 kB/s and up to 5 km coverage in an urban environment. In rural areas, up to 25 km could be achieved under certain conditions. Due to the used ISM band, duty cycle regulations of 1% per channel have to be met when no listen-before-talk mechanisms are used. However, as LoRa® supports multiple channels, the engagement in longer data exchange procedures is possible [54] [55] [40]. Other standards sit on top of the LoRa physical layer, to implement further layers of the protocol stack.

The first of them is *LoRaWAN*™, governed by the LoRa Alliance™, that defines the Link and Application Layer in the network. The channel access occurs at random, by using the unslotted ALOHA MAC protocol and FEC is used for error correction. A star-of-stars topology is applied, consisting of the wireless gateways and a central network server that is connected to the application servers. In LoRaWAN, the end-devices don't join a single base station, but rather a network that is defined by the network server. Three different classes of end-devices are possible (class A/B/C), that make tradeoffs in terms of battery lifetime and downlink latency. While class A devices (e.g. sensor nodes) only listen for downlink messages after an uplink transmission, class C devices (e.g. actuator nodes) are continuously listening. Class B is a mixture of both, where the device gets active at prescheduled times to receive data. However, to date, only class A devices are supported by most network backend services and hardware modules. For security purposes, 128 bit AES end-to-end encryption is used and authentication of the device, the network and the application is required. Furthermore features to

support localization of devices are on the roadmap. LoRaWAN is well received in the market and has a growing community [54] [40] [10].

Another technology that builds on the LoRa® physical layer is *Symphony Link™* from Link Labs. Targeted specifically towards industrial use cases, it employs a more deterministic TDMA channel access scheme with 100% acknowledgment of all messages to overcome packet errors. Furthermore it uses listen-before-talk mechanism for polite spectrum access and like this avoids the duty cycle limit in the 868 MHz ISM band in Europe. Instead of using pre-shared keys, it uses a PKI based Diffie-Hellmann key exchange mechanism and AES encryption. Regarding device management, Link Labs claims that over-the-air updates of the firmware will be possible [56]. As of early 2017, the technology is only available for operation in the US, with the announcement of a soon availability of EU compliant hardware.

Weightless-P, specified by the Weightless Special Interest Group, is an open LPWAN standard that is also targeted towards the industrial sector. It uses a narrowband modulation scheme and also operates in the European 868 MHz ISM band. As the standard is open, a proprietary chipset is not required. A combination of FDMA and TDMA is used for channel access and the data rate is adaptive up to 100 kB/s. Furthermore the listen-before-talk technique is used to avoid the duty cycle regulation. FEC and ARQ are used to provide a 100% acknowledged message transmission rate. The range is specified with up to 2km in an urban environment and the operation in a licensed spectrum is possible. Furthermore, Weightless-P provides device and network authentication, 128/256 bit AES encryption and over-the-air firmware updates [40] [10] [57]. While the hardware was not available at the end of this thesis (February 2017), it is scheduled for a public presentation by mid of March.

Other interesting LPWAN technologies are WAVIoT NB-Fi, Ingenu RPMA and SigFox. While WAVIoT is self operated, as the technologies presented above, Ingenu and SigFox employ a subscription based pricing model, where only the node needs to be purchased and the network access is provided for a monthly or yearly fee. Although all of them have interesting features, they come with a number of drawbacks. In the case of WAVIoT, the website is currently out of order and it is unclear whether the company still exists. Ingenu RPMA sends in the 2.4 GHz ISM band, together with WiFi and Bluetooth networks. It was originally developed to connect oil fields in the southern United States over a large distance. As these areas are usually less congested with other signals on the 2.4 GHz frequency, this is different in more crowded urban areas as it is most likely the case in the stated IIoT scenarios. SigFox, on the other hand, only allows to send unencrypted unidirectional uplink messages and is therefore less suited for IIoT, with a strong need for security and bidirectional communication for configuration management. Additionally, the network operator model induces risks in terms of lifetime of the network (startups can become bankrupt) and total costs of ownership (so far, only limited pricing information are available) for Ingenu RPMA and SigFox. More detailed information about NB-Fi, RPMA and SigFox can be found at Centenaro et al. [54] and WAVIoT [58].

Cellular Networks

Today's mobile cellular networks are mostly composed of 3G and Long Term Evolution (LTE) technology, with a transition to full LTE coverage. The standard LTE networks are designed towards the transmission of voice, video and high-speed data transmission and usually have a high power consumption. Therefore, the 3GPP standards commission, the governing body behind the LTE standard, included three new energy-sensitive LPWAN technologies in their latest LTE Release 13 specification. The first two are Enhanced Coverage GSM-IoT (EC-GSM-IoT), targeting traditional GSM bands, and LTE Machine Type Communication M1 (MTC Cat M1/eMTC), that can be operated on normal LTE base stations via a software update. The third and most interesting one in terms of energy efficiency and device costs is Narrowband IoT (NB-IoT). NB-IoT can be operated within the licensed LTE band in an in-band or guard-band mode, but also in standalone mode, by utilising a band in the legacy GSM spectrum. It can be expected, that operation in Germany will take place in the 800 MHz LTE band or

the 900 MHz E-GSM band. As it's name implies, it uses a small bandwidth in combination with FDMA techniques for channel access. It is expected to offer a throughput of up to 250 kB/s and is targeted towards massive MTC, where very low latency and very high reliability and availability are less crucial. Security features like authentication of the device and the network, end-to-end encryption at application level, integrity protection and key management mechanisms are already included. The next 3GPP release (14) is likely to add support for multicast downlink transmissions (e.g. for software updates) and for location tracking. In Germany, probably Vodafone and Deutsche Telekom will be among the carriers where NB IoT will be available. Nationwide public operation is expected to start in early 2017 and the first transceiver modules for nodes in the field are already available. As with SigFox and RPMA, the pricing structure is not published yet [5] [40] [59] [60].

To sum up, wireless networks have several advantages over wired solutions, like cost savings, but also come with constraints, such as signal interference and security issues which may be not possible to prevent (e.g. jamming the signal on a broad frequency range). Wireless connectivity options are short-range networks like Bluetooth Low Energy or IEEE 802.15.4 based networks, WiFi networks, LPWAN networks such as LoRaWAN, Symphony Link or Weightless-P and cellular networks like NB-IoT. Tables 2.2 and 2.3 provide an overview of the presented connectivity options, along with their technical details.

After having established the background knowledge in terms of Industrial IoT and wireless connectivity options, the next chapter will go on with related work to this research study.

	Short-Range Wireless Networks		*Wireless Local Area Networks*		*Cellular Networks*	
	BLE	**WirelessHART / ISA100.11a**	**802.11ac**	**IEEE 802.11ah**	**LTE**	**NB IoT**
Frequency (Europe)	2.4 GHz	2.4 GHz	2.4 GHz/5GHz	868 MHz	800 MHz, 2600 MHz	700/800/900 MHz
Modulation	FHSS (GFSK)	DSSS + FHSS	DSSS (OFDM)	DSSS (OFDM)	OFDMA	OFDMA
Bandwidth	2 MHz	2 MHz	20/40/80/160 MHz	1/2/4/8/16 MHz	5/20 MHz	180/200 kHz
Duty Cycle Regulation	n	n	n	y (2.8%)	n	n
Range	200m	100m	200m (outdoor) 70m (indoor)	1km (outdoor) 700m (indoor)	nationwide	nationwide
MAC	TDMA	TDMA	CSMA/CA	CSMA/CA	OFDMA	OFDMA
Reliability	FEC, ARQ	FEC, ARQ	FEC, ARQ	FEC, ARQ	FEC, ARQ	FEC, ARQ
Topology	Star	Mesh	Star	Star	Star	Star
Throughput (max)	1 MB/s	250kb/s	6933 Mb/s (5 GHz)	100kb/s	150 Mb/s	250kb/s
Security	128 bit AES-CCM encryption, ECDH key exchange	128-bit AES-CCM encryption, message auth. and key management	Extensible auth. Protocol (EAP); AES encryption	Extensible auth. Protocol (EAP); AES encryption	AES 128/256 bit encryption, device authentication	integrity protection, mutual authentication, AES cipher suite

Table 2.2.: Overview of Wireless IIoT Connectivity Options (1/2).

	Low Power Wide Area Networks					
	LoRaWAN	**Symphony Link**	**Weightless-P**	**WAVIoT NB-Fi**	**RPMA Ingenu**	**SigFox**
Frequency (Europe)	868 MHz	868 MHz	868 MHz	868 MHz	2.4 GHz	868 MHz
Modulation	Chirp Spread Spectrum (CSS)	Chirp Spread Spectrum (CSS)	OQPSK	DBPSK	RPMA-DSSS(UL), CDMA(DL)	UNB DBPSK(UL), GFSK(DL)
Bandwidth	125kHz	125kHz	12.5 kHz	100Hz	1MHz	100Hz
Duty Cycle Regulation	y (1%)	n (Listen Before Talk)	n (Listen Before Talk)	y (1%)	n	y (1%)
Range	5km (urban)	5km (urban)	2km (urban)	16km (urban)	4km (urban)	9km (urban)
MAC	unslotted ALOHA	TDMA	FDMA + TDMA	?	CDMA-like	unslotted ALOHA
Reliability	FEC	FEC, ARQ	FEC, ARQ	?	FEC	/
Topology	Star of Stars	Star	Star	Star	Star	Star
Throughput (max)	37.5 kb/s	37.5 kb/s	100 kb/s		78 kb/s	100b/s
Security	128 bit AES end-to-end encryption, network and device auth. with pre-shared keys	Diffie-Hellmann key exchange mechanism; AES encryption; over-the-air firmware updates	device and network auth.; 128/256 bit AES encryption; over-the-air firmware updates	XTEA 256 bit encryption	AES 128 bit encryption	no encryption

Table 2.3.: Overview of Wireless IIoT Connectivity Options (2/2).

3 Related Work

Several research studies exist, that are related to the core of this thesis. In the first part of this chapter, general work and a definition of Quality of Service (QoS) in networking will be presented, followed by an overview of previous approaches to define QoS models in the IoT domain. The consideration of the quality of service in the field of Industrial IoT networks allows the abstraction of the network traffic and operation and permits to make informed decisions about the best suited wireless network technology.

3.1 Quality of Service

As defined by the International Telecommunication Union (ITU), the *Quality of Service* (QoS) is the totality of characteristics of a telecommunications service that determine its ability to satisfy stated and implied needs of the user of the service. As such, QoS is influenced by the performance of the (network) service and the expectation of the service user. All in all, QoS consist of criteria regarding network performance and non-network performance parameters and is usually examined end-to-end (Fig. 3.1) [61].

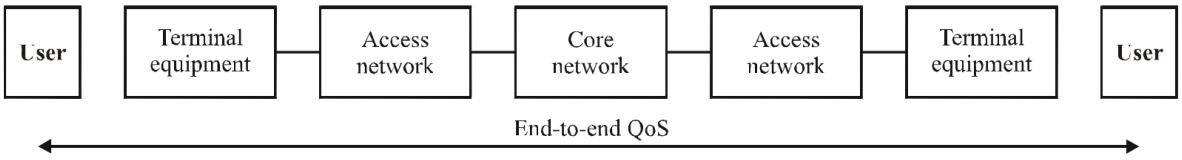

Figure 3.1.: End-to-end Quality of Service [61].

Traditionally, QoS mechanisms were carried out to maximize end-to-end throughput and minimize delay between users in wired networks, such as the telephone network or the Internet. Predominant traffic types were multimedia traffic such as voice or video and data traffic for web browsing or file transfers. While data traffic was delay insensitive, voice and (sometimes) video packages had to be delivered in real-time, with latency of not more than 150ms and a package loss of less than 1% [62].

In general, QoS support in wired networks can be achieved by over-provisioning of resources and/or traffic engineering. While the over-provisioning of bandwidth or other resources is easy to realize, it is possible that the service becomes unpredictable during traffic peaks, as all users are served in the same service class. Contrary, the method of traffic engineering classifies the data stream of users into service classes with a dedicated priority, so that important data (e.g. real-time audio traffic) is delivered with a higher priority than less sensitive data (e.g. a file transfer) [63].

However, Industrial IoT, with wireless links and machine-to-machine (M2M) communication face different challenges than these legacy network, such as resource constraints, greater network dynamics and more diverse traffic types. A more detailed explanation about the changed constraints will be presented in section 3.2. Before that, a review of conceptual models about Quality of Service is given.

On a formal basis, different granularities of a QoS system can be distinguished. In the following, two conceptual models by Chen and Varshney [63] and Burkhard Schmitt [64] are presented.

A simple QoS model by Chen and Varshney [63] is depicted in figure 3.2. This model is meant to specify the architecture of the QoS system, in terms of the requirements regarding the service quality and the QoS support mechanisms, that are provided by the network. The users or applications at the top of the model form the baseline for the requirements, that are posed on the network. The network at the bottom of the model has to achieve these requirements. Therefore it is necessary that the minimum requirements are met by the network out of the box, if e.g. only a single user uses the network. When the network gets more congested, the QoS support comes into play. The QoS mechanisms then manage

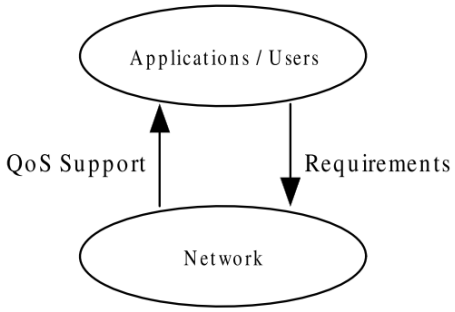

Figure 3.2.: A simple QoS Model [63].

the network traffic, so that the network meets the requirements of more critical applications, while discriminating less important ones [63]. The emphasis of this thesis is on the requirements part, rather than the QoS support mechanisms, as the requirements on the network imposed by M2M systems are fundamentally different from traditional end-user networks, which will be explained in the next section. Though the model allows to explain the major mechanisms of QoS, it lacks the detailed explanation of what exactly the QoS system should consist of and how the different components interact.

A more elaborated QoS system was introduced by Burkhard Schmitt [64]. The system is shown in figure 3.3 and consists of the QoS architecture and the QoS strategy. While the QoS architecture describes the technical details and mechanisms, the strategy consists of a formal policy that determines how the technical features are used to provide the required service levels. The architecture is based on a QoS model, that makes certain assumptions about traffic and control in the final system.

The traffic model describes the presumed traffic mix, based on the intended application use cases that use the network, and is therefore an important design criterion for the final architecture. It anticipates the different kinds of traffic that will flow through the network and what their relative importance will be. Of course the model can only be an estimation of the final traffic mix, but it is nevertheless the main source of requirements that determines the QoS architecture. Extreme assumptions regarding the traffic model are e.g. that only asynchronous data-applications, as e-mail, will use the network or that it will be only used for real-time voice traffic from Voice over IP services. However, a mix of different traffic types is likely and there is an uncertainty for the best QoS architecture for a given traffic mix, besides that the underlying network has to support at least the minimum requirements, when only one traffic type flows through the network. Previously defined traffic models will be introduced in section 3.3. The control model, on the other hand, makes decisions about where the intelligence of the QoS architecture is placed - on the edges or in intermediary nodes [64].

Based on the QoS model, an architecture can be designed that meets the requirements articulated by the traffic and control models. The architecture consists of QoS declarations and procedures. QoS declarations form the static part of the architecture expressed by parameters and service classes [64].

Parameters describe a certain property of the service and can represent the network performance, but also other attributes of the service. Network performance parameters usually come with a specification unit, so that the interpretation and measurement of the parameters is more clear. Example parameters of network performance are *throughput*, *delay* and *packet loss*, with the units *bit/s* (throughput), *seconds* (delay) and *percentage* (package loss) [64] [61]. More parameters, that are relevant for this thesis, will be presented in section 3.3.

The other QoS declaration that forms the static part of a QoS system are service classes. They represent a set of traffic, derived from the traffic model, that requires specific characteristics from the network. These shared characteristics are defined by the parameters mentioned above. While some service classes require the specification of all parameters, others might only need a subset of the parameters to be defined. Furthermore, service classes may also specify the QoS mechanisms that are taken to ensure the

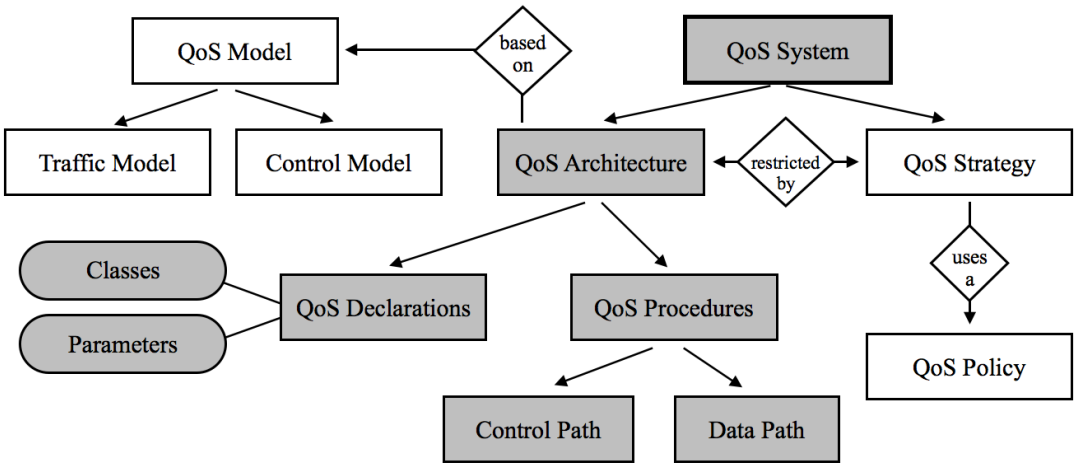

Figure 3.3.: A conceptual QoS System (Adapted from [64]).

right level of quality. Usually the service classes are ordered according to criticality of the network traffic and strength of assurance of the required level of quality. Examples of service classes are best-effort service, like in the Internet, or statistical guaranteed delivery for more critical applications [64] [1]. Previous work already defined certain traffic classes that are related to this research study. These will be presented in section 3.3.

Next to QoS declarations, QoS procedures form the second part of architecture components. The procedures are in accordance with the control part of the QoS model. Here, procedures on a control path and a data path are separated. Approaches affecting the control path usually are more long-term in nature and control the way data is transferred over a network. This includes network design and engineering, but also traffic engineering and admission control in more short-term time scales. Procedures on the data operate on individual packets and are of very short-term nature. Packet classification, scheduling and buffer management fall into this category [64]. In this thesis, the focus is on the wireless technology that is necessary in the network design to support the QoS requirements of Industrial IoT use cases, that were described in section 2.3.

In sum, both, the simple and the detailed conceptual model, show the building blocks of a QoS system. Nevertheless, in this thesis, the more detailed and elaborate model of Burkhard Schmitt [64] will be used to relate to further previous work regarding QoS traffic models, parameters and service classes for Industrial IoT systems.

3.2 Constraints on QoS in Industrial IoT

As already said, previous assumptions about QoS in legacy networks are not true any longer in modern IoT environments.

The assumptions were for example, that the target of the communication is an end-user that induces a traffic mix of data, audio and video content on the network, resulting in huge requirements in bandwidth. Contrary, in IoT systems, the network-endpoints are nodes in form of hardware-devices, instead of human users, and mainly small data-messages are sent over the network. However the nature of these data-messages can be fundamentally different from use-case to use-case. Therefore, the traffic mix is not entirely clear anymore.

Also the medium, that the network is based on, is rather different. In traditional QoS system, wired networks, like telephone networks or the Internet, were dominant. At most, high-bandwidth WiFi or cellular networks were the target of considerations. As already presented in section 2.4 about wireless networks for IIoT, the new connectivity landscape has broadened tremendously.

Due to the fact that the assumptions in legacy networks were quite stable and QoS declarations were clear, most QoS-related research in the past took place in the field of QoS procedures like admission control, routing mechanisms and QoS aware MAC protocols. The first example of traditional QoS architectures is the Asynchronous Transfer Model (ATM), that was targeted towards traditional communication networks like telephone connections. The following integrated services (IntServ) model was more focused on best-effort traffic than ATM and depended on a Resource Reservation Protocol (RSVP), which could be used by hosts to request a specific QoS from the network. The third model is the differentiated services (DiffServ) model. It took the heterogenous nature of wide area networks into account and focused more on a decentralized per-hop handling of different traffic types. Traditional parameters in these models were end-to-end delay, packet loss and jitter (slight variations in the delay) [64] [62].

However, these assumptions about traffic types, network medium, parameters and end-to-end connectivity don't hold anymore in times of Industrial IoT, that consist of wireless sensor and actuator networks and has different relevant parameter types. A new QoS models, that can cope with the challenges in these systems, is needed [65] [11] [66].

Several constraints that affect the quality of service in IWSNs, as connectivity and device part of an Industrial IoT system, have been identified in previous studies. An overview of them is shown in table 3.1. The *resource constraints* of end-nodes in terms of energy, bandwidth and processing power is most often named as a challenge in industrial wireless sensor networks. Also it can have an impact on QoS, because the protocols have to be energy-efficient as well. Next to the individual energy efficiency, also the *balanced energy consumption across nodes* is especially a topic in mesh-networks. Additionally the *network dynamics* impose QoS difficulties and can be caused by unreliability of the node or the wireless link, node-mobility, changing node states due to duty cycling and topology changes. *Data-redundancy* in the network may come from multiple sensor nodes that report the same value, leading to unnecessary network congestion, and *multiple traffic types* stem from a variety of use-cases and data-delivery schemes (periodic/aperiodic, ...), but also from a heterogeneity of devices and sensor types.

Though most sensor nodes only send to a single sink node, e.g. a gateway in a star network-topology, in some cases *multiple sink nodes*, such as actuators, can be the target, which can cause network congestion. In general, the *heterogeneity of QoS requirements* induces a lot of complexity, because each service class can have different service level agreements and a different criticality. *Scalability* and *security* are two usual issues of distributed systems, that also affect IWSNs. The stable provision of service quality, even with thousands of connected devices, has to be maintained. As QoS can be affected by the unavailability of the network through a denial of service attack, also security matters. Finally, there are also some more deployment-related concerns, such as the *integration with existing other industrial networks* or the Internet, but also the *node-deployment* in the field, which can be challenging in certain environments such as rough terrain.

Additional and partly complementary to the cited constraints, also a number of requirements for industrial wireless sensor networks have been identified in the past. As listed in table 3.2, the most often named requirement is the *reliability* of the network. Due to the challenge of network dynamics and wireless connection failures, reliability is meant primary as link reliability of the network. It has to be made sure, that every message is reliably delivered to its target. The QoS has to ensure that this is the case and *time synchronization* across nodes, e.g. for timeslotted wireless medium access with TDMA, can help to make sure that the network behaviour stays predictable. Also network reliability is important, especially in mesh networks, so that the failure of some nodes doesn't result in the collapse of the entire network. Closely related to reliability is the requirement of *low latency* of the network. Especially in closed-loop industrial control systems, the transmission of messages in near real-time with roundtrip-times of less than 10 ms is critical to avoid the emergency-shutdown of the production line. *Data fusion and localized processing* on gateways or event on sensor nodes ("intelligence on the edge") can help to reduce the network delay and is therefore a design requirement as well. The need for *energy efficiency* follows directly from the constraint of limited power supply, as a lot of sensor nodes will be

Challenges	Sources
Resource constraints	[67] [68] [63] [32] [66] [69] [37]
Network dynamics	[67] [68] [63] [32] [66] [69]
Data redundancy	[67] [68] [63] [32]
Multiple traffic types	[67] [68] [63] [69]
Multiple sink nodes	[67] [68] [63]
Scalability	[67] [63] [32]
QoS Heterogeneity	[32] [22] [37]
Security	[32] [37]
Node deployment / Implementation	[67] [37]
Heterogeneity of platforms and sensor nodes	[68] [69]
Energy balance across the network	[63]
Integration with Internet and other networks	[32]

Table 3.1.: Overview of Challenges in industrial Wireless Sensor Networks.

powered by batteries. Taking into account that other requirements are *reliability*, *self-organization* of the network and *security*, a tradeoff between all these requirements has to be made, as heavy protocols will drain the batteries very quickly and will thus impact the quality of service.

Furthermore the network should support energy-aware *QoS mechanisms* and service differentiation, so that the traffic of critical industrial applications can be transferred with higher priority than other traffic. Though *minimal cost and compactness* does not directly influence QoS, it has an impact on the overall applicability of the IWSN and on the possibility to scale it up. This *scalability* has to be also supported by the network through a scalable architecture and efficient protocols. Additional design considerations that are required for some use cases and that come along with certain sensor types are the support of *high sampling rates* and therefore also *fast transmission rates* of the network. Such faster sampling rates are much more common in industrial settings, compared to "normal" environmental wireless sensor network. Also here, the tradeoff between energy consumption and this design consideration has to be made. Finally, also *interoperability* between legacy system and new systems and interoperability of different sensor types has to be taken into account.

Due to the many constraints and design requirements, Willig et al. [34] advise to design the industrial application and the network in a joint operation, so that the needed and achievable quality of service becomes clear. During this joint operation, the constraints should already be factored in the system design, so that for example a short network outage doesn't affect the entire operation of the use case, such as a production process [34].

To sum up, the most mentioned constraints were scarce resources (battery, processing power, ...), network dynamics (link failures, node failures, ...), data redundancy in the network and multiple traffic types. Therefore, design requirements were first and foremost reliability, low latency and energy efficiency. After presenting challenges and requirements of wireless sensor and actuator networks in

Design Requirements	Sources
Reliability	[32] [33] [22] [70] [71]
Low latency	[22] [70] [50] [71]
Energy efficiency	[32] [33] [22] [71]
Self-organization	[32] [22] [70]
QoS Mechanisms	[63] [32] [22]
Minimal cost and compactness	[32] [22]
Scalability	[32] [22]
Data fusion and localized processing	[32] [22]
Time synchronization	[32] [33]
Security	[32] [50]
High sampling rates	[33] [71]
Fast transmission rates	[33] [70]
Interoperability	[33] [22]

Table 3.2.: Overview of design requirements in industrial Wireless Sensor Networks.

industrial settings that can impact the quality of service in these environments, the next section presents previous work on QoS system components.

3.3 QoS Model-Components for Industrial IoT

In this section, contributions from the literature in regard to QoS traffic models, parameters and service classes will be reviewed. These QoS model components will help later on to define service classes for the use cases presented in section 2.3 and in the recommendation of appropriate network technology.

3.3.1 Traffic Models

The first type of QoS system components that will be reviewed are traffic models. A more detailed traffic model was defined for the already mentioned IntServ QoS architecture (Figure 3.4). It was targeted towards diverse traffic and mainly differentiated between real-time traffic (e.g. for audio calls and video telephony) and elastic best-effort traffic. Especially the best-effort traffic was assumed to play an important role and was considered as the default. Real-time traffic was additionally divided in loss-tolerant and loss-intolerant traffic, where a late packet was not considered anymore. Finally, a distinction between adaptive and non-adaptive traffic was made, in regard to whether the real-time traffic could cope with variations in the delay of the packets [64]. Being very focused on real-time traffic for multimedia applications, the model is usable in the M2M space only to some extent. Additionally the values of the different parameters, such as "loss-tolerant" are not specified any further, leaving the reader alone in distinguishing what is loss tolerant and what is not.

Borges et al. [72] identified several types of traffic that occur in general wireless sensor networks and mapped them to the type of information they transfer (Table 3.3). In general, they distinguish audio, video and data traffic. *Audio traffic* is further split up into voice (VOI) and ambient traffic (AMB), such as background noises. For *video traffic*, the only assumed type is streaming video (STV). Audio and

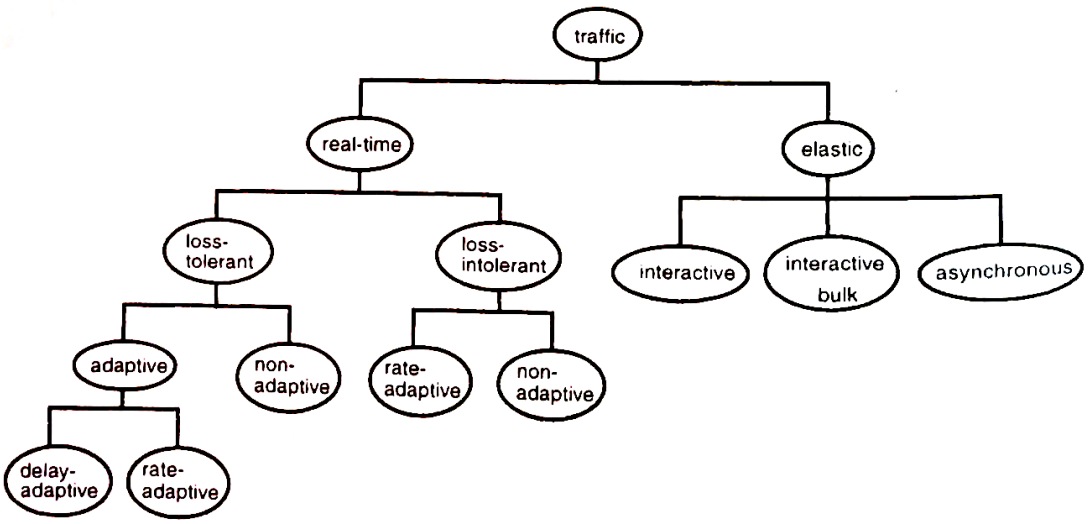

Figure 3.4.: IntServ traffic model [64].

	Types of Traffic					
	Audio		Video	Data		
Types of information	VOI	AMB	STV	LOD	MED	HID
Sensor Data	–	–	–	√	√	√
Sound	√	√	–	–	–	–
Video	–	–	√	–	–	–
Moving pictures and sound	√	√	√	–	–	–
Snapshot images	–	–	√	√	√	√

Table 3.3.: Traffic types in general Wireless Sensor Networks [72].

video can come separately or in combination. Finally, *data traffic* is differentiated in regard to the data rate, resulting in the types for low rates (LOD), medium rates (MED) or high data rates (HID) [72]. Through the emphasis on multimedia applications and only considering the bandwidth at data traffic, it's suitability for M2M IIoT communication is limited. Also, it is not specified when a data rate is high, low or medium.

Specifically for the industrial space, Moyne and Tilbury [73] specify three different types of application traffic that is transferred over the network, namely diagnostic traffic, control traffic and safety traffic. *Diagnostic information*, as from tool monitoring systems, are assumed to be sent infrequently, but in large amounts. An example could be the tool monitoring of a spindle (e.g. a lathe or the rotating part of a milling machine) that sends the monitoring data over the network after a part is produced. Thus, the network should support the timely transfer of the data and the emphasis on speed rather than determinism. Diagnostic traffic in this regard is not meant in terms of network diagnostic, but rather diagnostics of the connected system. *Control information* can be further divided into real-time and event based traffic. Real-time traffic has a time-bound for the transmission and examples include temperature and flow in a process system, limit switches and optical sensors in material flow applications (e.g., conveyors) and continuous feedback values (e.g., position, velocity, acceleration) for servo systems, such as servo motor based industrial manufacturing systems. The transmission of this traffic needs to be carried out with a high level of determinism. Event-based traffic can also be used to make decisions in the industrial process, but a time-deadline is not present here. The system is able to wait until the

information for the next step is arrived, such as when the handling of a part in a machine tool is finished and a decision about the next step is awaited. Also the data size of messages inside control networks can vary. Whereas some control signals consist of a single bit (e.g. for a switch), others can be much larger, such as it's the case for machine vision. Finally, *safety information* are the third identified traffic type in industrial networks. They are used to control safety interlocks on machines and have the strongest demand on determinism and jitter [73]. Though the classification makes very much sense for the part of Industrial IoT that is affected with manufacturing and process control, it is less suitable for other areas such as the commercial IoT sub-space or the area of logistics coordination.

Also the ISA 100 committee, the governing body behind the ISA 100.11a standard, classifies traffic into four broad classes. *Periodic data* is sent out regularly and timely delivery is often the core function. This is the case in a lot of sensor network applications, for example when a steady flow of temperature values has to be reported. *Event data* appears aperiodic, for example when a fire is detected or a temperature exceeds a certain threshold, but can result in bursty traffic when multiple sensor nodes report the same event. *Client/server communication* is required for several industrial protocols, where data is also bursty, but requires roundtrip-latency of tens of milliseconds. Finally, *bulky transfers* involve the transmission of bigger data blocks and normally occur only temporarily, e.g. when a software update is pushed out [18]. From all presented traffic models, this is the one that is most suited for the differentiation of traffic in IIoT networks, because it takes the primary nature of the traffic into account and allows the quick and fast classification, with clear boundaries between the traffic types. Nevertheless, is is very broad in nature and allows only for a broad overview of traffic types.

After presenting four ways to differentiate traffic inside of an industrial wireless sensor network, the next subsection covers different parameters that are relevant in regard to the quality of service of an application.

3.3.2 Parameters

Being a major part of the QoS declaration, parameters describe a certain property of the application service and can specify the network performance, but also other, non-network related attributes. The list of the parameters to be taken into account, form an important input for the definition of service classes later on. Therefore, the ITU came up with a document that specifies several considerations that should be made when identifying quality parameters, such as having a prioritized list of parameters and assigning the minimum and preferred performance values. Also it is noted that it is important to have the right number of parameters, as too many parameters may pose too much constraints on the network and too few parameters don't allow the proper specification of dedicated service classes [74].

An overview of QoS parameters related to industrial wireless sensor networks, as reported in the literature, is given in table 3.4. The parameters are classified, whether they are application-, network- or node-related, such as done by [68] [72] [63] and [2]. Another possibility would have been to cluster them according to the network layers, as done by [75] and [76]. However, the chosen clustering suits the target of this thesis, to define IIoT service classes, in a better way, as the high-level application related QoS parameters such as reliability, depend on lower-level network QoS parameters as e.g. packet delivery ratio.

The application-related QoS parameters are directly tied to the requirements that are imposed by the service. General parameters like reliability, coverage, lifetime, security and availability are included here. *Security* can be further broken down into confidentiality, integrity and authenticity of the data. While *reliability* is related to the reliable transmission of data, *availability* describes the degree to which a system is in a functioning state for a given period of time. *Lifetime* means the overall system lifetime and *coverage* is the area that is covered by the network. It can be restricted to a smaller (local) or larger area, such as nationwide or even bigger coverage (global). *QoS support* describes, whether active QoS procedures, such as prioritization of traffic by different services, are required, whereas the delay tolerance specifies the maximum delay that is acceptable by the application. This is especially important

	Parameter	Measure	Source
Application-related	Reliability	low/high	[77] [2] [78] [50] [70] [75]
	Coverage	local/global	[68] [72] [63] [2] [75] [37]
	Lifetime	years	[72] [2] [66] [75] [37]
	Security	low/high	[72] [77] [2] [78] [70]
	QoS Support	y/n	[72] [77] [2]
	Delay tolerance	low/high	[72] [77] [78]
	Availability	%	[77] [2] [78]
	Interactivity	y/n	[72] [63] [79]
	Mission-criticality	y/n	[72] [63] [79]
	End-to-End	y/n	[72] [63]
	Directionality	uni/bi	[72]
Network-related	Latency	ms	[72] [63] [77] [2] [38] [70] [79] [50] [66] [75] [69] [76]
	Throughput	kB/s	[72] [77] [2] [38] [75] [69] [76]
	Packet Delivery Ratio	%	[72] [77] [2] [75] [69] [76]
	Jitter	ms	[77] [2] [38] [69] [76]
	Fault-tolerance	low/high	[68] [77] [38] [66] [75]
	Scalability	low/high	[72] [77] [66]
	Hop-Count	no.	[75] [76]
	RF Signal Strength (RSSI, SNR)	dB	[76]
	Self-organization	y/n	[72]
Node-related	Energy Consumption	J/s	[72] [77] [70] [66] [75] [76]
	Accuracy	low/high	[68] [63] [2] [78] [66] [75]
	Sampling Rate	time int.	[72] [77] [2] [75]
	Processing power	low/high	[72] [2] [76]
	Node density	low/high	[72] [68] [63]
	Maintainability	low/high	[72] [77] [37]
	Time synchronization	y/n	[72] [2] [38]
	Heterogeneity	low/high	[72] [37]
	Mobility Support	y/n	[72] [2]

m: Meter; y/n: Yes/No; uni/bi: Uni-/Bidirectional; ms: Milliseconds; kB/s: Kilobyte per Second; no.: Number; dB: Dezibel; J/s: Joule per Second Hz: Hertz;

Table 3.4.: Overview of QoS Parameters for IIoT.

for real-time applications, such as industrial control systems. Somewhat related, *interactivity* differentiates between synchronous and asynchronous traffic, in terms of request-response interactions. Interactivity is of course only possible when bidirectional communication is supported. However, unidirectional communication is also possible, which is specified by the *directionality* parameter. The functioning of the application might be *mission-critical* (e.g. for heart-rate monitoring) or not and *end-to-end* or non-end-to-end applications exist. The application may be end-to-end in case where one end is formed of a sensor node and the other end is an actuator node. On the other hand, an application is not end-to-end when multiple sensor nodes that sense an event are at one end and at the other end is one gateway that collects the sensor data and only forwards it to another network node at a later stage.

The lists of network-related parameters consists of criteria that are more technical in their nature. *Latency* marks a delay that is experienced when carrying out a specific action. *Jitter* is defined as the variation in this delay. Together with the *hop-count*, it is especially relevant in real-time environments. While some applications can deal with certain delay, they might be very sensitive to jitter, as e.g. in voice communication. *Throughput* is the amount of data that is received within a certain unit in time. It is dependent on the bandwidth and spectrum efficiency of the wireless channel. *Packet delivery ratio*, is, as the name implies, the percentage of correctly delivered packages over the network. Together with *fault-tolerance*, it is connected to the reliability of the network. *Scalability* refers to the ability of the network to be enlarged and still deliver the same quality of service. *Self-organization* describes the capability of the node, to establish the best communication path to another point in the network. Therefore, and for the general assessment of the wireless communication channel, the *RF signal strength* can be used, that can be described by the Received Signal Strength Indicator (RSSI) or by the Signal to Noise Ratio (SNR).

The third big group of parameters are those that are mainly related to the individual node in the field. A main concern here is the *energy consumption*, that is measured in Joule per second. In combination with the battery capacity, it determines the lifetime of the node. Furthermore the energy consumption is related to the *sampling rate* (measured in a time interval like milliseconds, seconds or minutes), the used *processing power* and the frequency by which the data is sent out to the gateway. Thereby, the sampling rate refers to the frequency by which the node senses its environment. *Accuracy* means the degree to which the measured data is correct, reliable and novel. *Node density* is the number of active sensors per unit of area and also describes the optimal number of active sensors, whereas *maintainability* is the ability to undergo modifications and repairs of the network. It is related to *heterogeneity*, which is the degree of similarity of the different nodes in the network, as a lot of heterogeneous nodes are harder to maintain. Especially needed for a predictable behaviour of the network is the *time synchronization* of nodes, to keep a uniform time reference and sample time-dependent data correctly. At last, the support of *node mobility* is an important QoS criteria, that is required by several applications where moving nodes are involved.

Though a lot of parameters were defined in the past, not all of them are suitable to be used in a QoS model. Some of them may be too technical (as the RF signal strength or the node processing power), too specific for certain topology types (as self-organization in mesh networks) or where only one viable parameter option exists (as e.g. bidirectional network service).

3.3.3 Service Classes

The last part of QoS architecture components that is presented here are the service classes, who represent sets of traffic that share common characteristics and require that the network meets specific parameter values. The degree, to which these values are met, is then the quality of service for these classes.

Burkhard Schmitt [64] sees the service classes as an interpretation framework for the quality assurance that is given to the user of a network. Beginning with a distinction of *best-effort traffic* and *guaranteed delivery*, five service classes emerge that are ordered according to the strength they assure the required service level. While *absolute classes* have a clear reliability value attached to them, the *relative class* could

be split up in subclasses that have a relative value of priority attached (e.g. class 1: 70% of bandwidth and class 2: 30% of bandwidth). Thus, absolute performance could still be bad for the subclass with the highest priority, while all relative requirements are met [64]. The heavy emphasis on real-time classes and very broad and generic definition of the model makes it hard to directly apply it to the IIoT space. Also, no parameters were specified, nor were given any hard parameter values, that would allow the easy classification of a new use case into one of the classes. Rather, it is a generic service class model, that can help in building and structuring a QoS model, as done in this thesis.

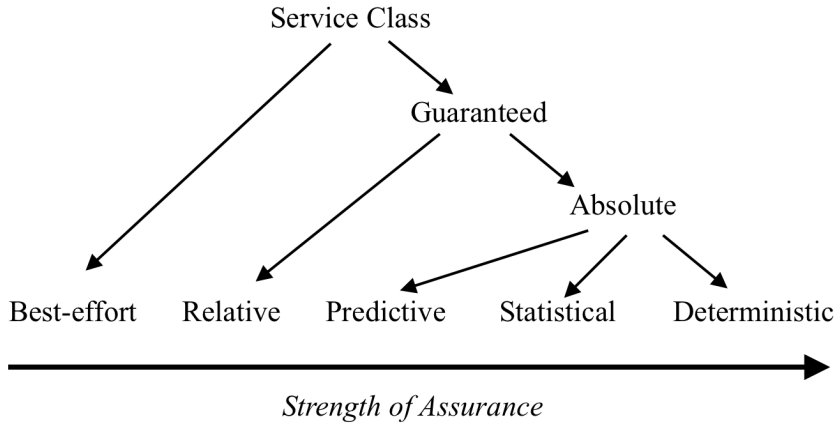

Figure 3.5.: Service classes of Burkhard Schmitt [64].

Similar to Burkhard Schmitt [64], also Borges et al. [72] distinguishes into *best-effort* and *real-time delivery*, but additionally also in *data* or *multimedia* streams and *loss-tolerant* or *intolerant* data. Data traffic is further mapped into traffic with *constant bit rate* (CBR, e.g. 100 kB/s all time) *real-time variable bit rate* (RT-VBR, e.g. range of 70-100 kB/s), *available bit rate* (ABR, with guaranteed minimum data rate, e.g. minimum bit rate of 70 kB/s) and *unspecified bit rate* (UBR), for which no guarantees are given [72]. However, again, no information were given when a traffic class is "loss intolerant" and many important QoS aspects of IIoT traffic other than network performance parameters, such as support of node mobility and coverage, are missing.

RFC 4594 of the Internet Engineering Task Force (IETF) specifies 12 service classes of the DiffServ QoS model, that was mentioned earlier. The service classes are depicted in table 3.5. As shown, the classes are differentiated in regard to the traditional network parameters *packet loss*, *delay* and *jitter* [1]. For this thesis especially relevant are the classes for low-latency and high-throughput data. The multimedia classes are less relevant, though they account for six of the overall 12 classes. As the 12 class model is very granular, it can be further broken down into eight or even only four classes, as described by Szigeti et al. [62]. However, again, only network-performance related parameters are taken into account, which doesn't allow to describe a holistic view of the quality of a M2M communication service. Also, as already mentioned, only half of the classes are of high relevance for IIoT.

A special QoS classification for IoT in general is given by Duan et al. [2]. They differentiate between *best effort* traffic, *differentiated services* and *guaranteed delivery* (table 3.6). Hereby, differentiated services are a mixture of best effort and real-time traffic. Additionally, they group IoT applications according to their task type and real-time properties and assign the appropriate service class to each application type [2]. Unfortunately, the description of their model is very short, and no additional explanations are given in regard to specific parameter ranges of the three service classes.

Nef et al. [79] base their service classes for wireless sensor networks on the parameters *interactivity*, *delay tolerance*, and *criticality*. Interactivity and criticality is defined as in section 3.3.2, while delay tolerance is further broken down in *non-realtime*, *soft-realtime* (probabilistic delay bound) and *hard-realtime* systems (deterministic end-to-end delay bound). A total of three service classes, named service models by Nef et al. [79], were defined, namely the *open*, *supple* and *complete* service model. The *open*

Service Class Name	Traffic Characteristics	Tolerance to Loss	Tolerance to Delay	Tolerance to Jitter
Network Control	Variable size packets, mostly inelastic short messages, but traffic can also burst (BGP)	Low	Low	Yes
Telephony	Fixed-size small packets, constant emission rate, inelastic and low-rate flows	Very Low	Very Low	Very Low
Signaling	Variable size packets, some what bursty short-lived flows	Low	Low	Yes
Multimedia Conferencing	Variable size packets, constant transmit interval, rate adaptive, reacts to loss	Low - Medium	Very Low	Low
Real-Time Interactive	RTP/UDP streams, inelastic, mostly variable rate	Low	Very Low	Low
Multimedia Streaming	Variable size packets, elastic with variable rate	Low - Medium	Medium	Yes
Broadcast Video	Constant and variable rate, inelastic, non-bursty flows	Very Low	Medium	Low
Low-Latency Data	Variable rate, bursty short-lived elastic flows	Low	Low - Medium	Yes
OAM	Variable size packets, elastic & inelastic flows	Low	Medium	Yes
High-Throughput Data	Variable rate, bursty long-lived elastic flows	Low	Medium - High	Yes
Standard	A bit of everything	Not Specified		
Low-Priority Data	Non-real-time and elastic	High	High	Yes

Table 3.5.: Service classes of IETF RFC 4594 [1].

Application type	I control	II query	III real-time monitoring	IV non real-time monitoring
QoS level	Guaranteed Service	Guaranteed Service /Differentiated Service	differentiated service	Best Effort

Table 3.6.: Service classes of Duan et al. [2].

	Open Services Model	Supple Services Model	Complete Services Model
Interactivity	Yes	Subscription-specific	No
Delay	Non-RT	SRT	SRT/HRT
Criticality	No	Yes	Yes

Table 3.7.: Service classes of Nef et al. [79].

Parameters	Class			
	Event-driven	Query-driven	Continuous	Time-driven
End-to-End	×	×	×	×
Interactivity	√	√	×	√
Delay tolerant	×	query-specific	√	√
Criticality	√	√	×	√

Table 3.8.: Service classes of Tilak et al. [66], Chen and Varshney [63] and Borges et al. [72].

service model covers simple applications, where content providers make information available to end-users, such as a web application. Thus they are not critical and very delay-tolerant. The *supple* ("flexible") service model is focused on content providers that provide sensorial or geographical information on a periodic basis. It can be non-interactive, when data is provided in regular intervals, or interactive, when it is query-based. Also it can provide service assurance to some degree without strict quality constraints, which covers critical applications with a moderate tolerance for delay. The *complete service model* addresses services that require the timely delivery of up-to-date information and the network is specifically used to run these services. As the data flow is often continuous, it is not interactive, but mission critical and the service can have little or medium delay tolerance, depending on the application domain [79]. The model is very generic in scope and was designed to cover the entire bandwidth of IoT applications, namely consumer, commercial and Industrial IoT. Following, most Industrial IoT services fall in the supple or complete service model, which is too broad to be of any use in the meaningful classification of IIoT services.

Similar and somewhat related to service classes, Tilak et al. [66] specify four basic data delivery models for wireless sensor networks, namely *event-driven*, *query-driven*, *continuous* or *hybrid* delivery, which are described in more detail by Chen and Varshney [63]. Borges et al. [72] added a fourth class, namely the *time-driven delivery* class (table 3.8). As the above described work of Nef et al. [79] is based on the parameters from Chen and Varshney [63], the criteria are *interactivity*, *criticality* and *delay tolerance* as well. Additionally, end-to-end vs. non end-to-end communication is a factor. In the *event-driven* class, the nodes are expected to observe data about critical events that should be transferred to the gateway as quickly as possible. As many sensors may sense the same event, bursty traffic might occur on the network. In the *query-driven* model, queries are sent out to the nodes on demand. Different to the event-driven model, where data is pushed to the sink, the sink pulls in the data in this case. In the *continuous model*, data is constantly sent out by sensor nodes to the gateway at a pre-specified rate. In this class, real-time or non real-time data can occur. The fourth *time-driven* class is similar to the continuous one, with the difference that the intervals between the transmission can be larger and that data processing is entirely performed on the sink nodes. Additionally, hybrid models are possible, that share characteristics of the other specified classes. Furthermore it is noted, that all classes are described as critical and non end-to-end, which marks the importance of WSNs and their distinction to traditional end-to-end network applications [72] [63] [66]. Similar to the models before, also this model lacks important parameters in it. Though already a mixture of network-related and application-related parameters are used, other IIoT relevant QoS parameters such as node mobility and coverage are missing. Also the data delivery nature of the classes doesn't allow to differentiate between more and less important traffic, which is relevant for the Industrial IoT setting.

Specifically targeted towards the industrial environment are the three broad categories and six service classes that have been specified along with the ISA 100.11a standard [18]. The classes are as follows:

- Safety
  - Class 0: Emergency action - Always a critical function
- Control

  - Class 1: Closed-loop regulatory control - Often a critical function
  - Class 2: Closed-loop supervisory control - Usually a non-critical function
  - Class 3: Open-loop control - Operator takes action and controls the actuator (human in the loop)
- Monitoring
  - Class 4: Alerting - Short-term operational effect (for example, event-based maintenance)
  - Class 5: Information gathering - No immediate operational consequence (e.g., history collection, preventive maintenance)

With decreasing class-number, the in-time delivery of the messages becomes more relevant. In general, jitter is equally important as latency in the control domain, because it can destabilize control algorithms [18].

Safety systems, with class number 0, have the most strict requirements on timely delivery, as countermeasures against malicious events, such as fire, have to be carried out in the orders of seconds or milliseconds. In Closed-loop regulatory control systems (class 1), feedbacks are used to regulate the system in real-time. Periodic measures that are delivered within strict time-bounds are critical. Closed-loop supervisory systems (class 2) are usually not that critical, as they don't depend on strict periodic measurements, but rather on the detection of trends over time that may be related to certain events. In open control system (class 3), there is no direct actuator node connected. Rather a human observes the data that is collected by the WSN and undertakes the required actions. Alerting systems (class 4) are used for regular or event-based alerting, such as the temperature monitoring in a furnace. Finally, simple information gathering systems (class 5) have the least requirements on real-time delivery and jitter. Equipment monitoring and asset tracking could fall into this category [22].

As Pister et al. [18] note in IETF RFC 5673, the deployment of wireless sensors is especially interesting in the classes 4 and 5, as well as in the non-critical areas of classes 2 and 3. Further they distinguish between low-rate control and fast control applications and state, that the strict latency requirements (tens of ms) in fast control systems are not suited for wireless networks. However, low-rate control systems with a human in the loop could be interesting. While Pister et al. [18] assume that the loops in the field will be closed in the future by wired connections of sensors and actuators, due to their short distance in the field, the connection to the usually more distant operator room could be via a wireless network. This reduces the strict latency and availability requirements, but allows to send diagnostic information and influence controller settings [18]. Being the most comprehensive model for IIoT so far, it is especially targeted towards the industrial manufacturing domain, with an emphasis on production and process control in a local area. Thereby it leaves out the commercial IoT part of Industrial IoT, where different classes might be required. Also the fact that it is advised to make services with class 0 or 1 not wireless at all, leaves only four classes for wireless sensor and actuator networks, which might not be sufficient to classify all use cases correctly and still giving a holistic view on each classified use case.

The real-time classes that are relevant in the industrial space are further broken down by Neumann [50]. He distinguishes three classes of traffic with real-time (RT) behaviour: soft RT, hard RT and isochronous RT. Soft RT has a scalable cycle time and is used in factory or process automation, while hard RT usually has cycle times between 1 and 10 ms and is used for control. Isochronous RT applications have the highest requirements, with cycle times of 250 µs to 1 ms and jitter of less than 1 µs. This is e.g. required in motion control [50]. While these real-time classes are very relevant for the industrial control domain, for a lot of other areas the soft RT class might be sufficient and thereby limit the applicability to classify the entire IIoT space.

3.4 Network Selection and Scoring Models

Next, related work in the field of network selection processes as well as scoring models is presented. This work will later be integrated in the development of a scoring model-based process for the selection of the most fitting wireless technology.

Previous approaches in the field of network selection were carried out by Song and Jamalipour [80] and Bari and Leung [81]. Song and Jamalipour [80] developed a network selection scheme that allowed to either pick WiFi or cellular UMTS for network access, to provide the best available quality of service. They selected throughput, timeliness, reliability, security, cost and availability as QoS parameters and used the analytical hierarchical process to derive the relative importance of each parameter. Finally, they simulated four cases of different network setups and used grey relational analysis for the calculation of a coefficient that determined whether to pick UMTS or WiFi for network access. Though the selection model might have been suitable for limited connectivity options in the year 2005, when their research was published, the number of options today is much bigger. Also their model doesn't include the energy consumption of the technologies, which is very important in the battery-operated IoT world.

Bari and Leung [81] developed a multi-attribute decision making model for network selection. The range of network technologies to choose from were UMTS, WiFi (802.11b/a/n) and LTE/4G. Their main focus was on the optimization of user activities in the Internet, such as voice calls, streaming of multimedia content and web browsing. They manually assigned weights to several QoS parameters, based on the indended use case of the user. Subsequently they used TOPSIS as decision making algorithm to rank the network technologies for each use case. As it becomes evident, the focus on consumer use cases is not suitable for the application on Industrial IoT systems. Similarly to the work of Song and Jamalipour [80], the legacy technology selection doesn't reflect the connectivity landscape of today.

Also Zöller [82] developed a scoring model that allows to evaluate the utility of alternatives, based on a selection of criteria. His first step is the derivation of a relative weight for each criterion, based on the pairwise criteria comparison in a matrix and the calculation of a relative weighting factor. Building on that, the alternatives were rated for each criterion and a score was calculated based on the relative weights and the assignments of each criterion. The main concept of the scoring model can be used to derive propositions about alternatives, which is related to the problem of network selection.

3.5 QoS Evaluation of LPWAN

Several evaluations of the quality of service in an urban environment of LoRaWAN, as a major LPWAN technology, were carried out in the past by Petäjäjärvi et al. [83] [84], Petri et al. [85], Augustin et al. [86], Centenaro et al. [54] and Kartakis et al. [87]. From these, Centenaro et al. [54] only measured the coverage, but not other QoS parameters such as reliability of the network connection. With LoRa spreading factor (SF) 12, they achieved connections up to 2km of distance, when placing the gateway on top of a high building with 19 floors. Augustin et al. [86] only assessed the LoRa physical layer without the LoRaWAN MAC protocol. Their longest achieved distance, by placing the gateway on a house at the side of a hill, was 3.4 km with SF and a packet delivery ratio (PDR) of less than 40%. However until 2.3km they achieved close to 100% PDR with SF12. Petri et al. [85] placed their gateway on top of a TV tower and measured the PDR in 3km distance. They experienced PDR as low as 47% for some places with SF10, depending on the position. Kartakis et al. [87] put their gateway on top of a 11 floor building in a city and measured the packet delivery ratio and achievable distance. Until around 250m, they had a PDR of 100% with SF12, that dropped to 86% at 406m and 72% at 760m. Petäjäjärvi et al. [83] [84] mounted their gateway on an antenna tower at a height of around 24m above sea level and operated their LoRa nodes at SF12. For outdoor measurements, where the LoRa module was attached to the top of a car, the PDR was 88% in up to 2km distance. In their indoor measurements, they achieved up to 94.7% PDR in a distance of around 390m. In a closely located anechoic chamber room, designed to absorb reflections of sound or electromagnetic waves, no connection was possible. Furthermore, they

report the problematic and strict duty cycle restrictions and the impact on the flawless operations of the LoRa device.

Though several test with LoRa have been conducted, not all of them were with LoRaWAN and none of them was in an industrial setting. Therefor, more research in this direction is needed.

3.6 Summary and Discussion

As it becomes evident, several work in the field of QoS models for networks in general and wireless sensor or IoT networks has already been carried out in the past. The traffic models of IntServ, Borges et al. [72], Moyne and Tilbury [73] and ISA 100 have been presented. However, all models face drawbacks that prevent the straightforward application to the IIoT domain, such as missing documentation, heavy focussing on multimedia traffic or emphasis on only one aspect of IIoT.

On the other hand, several service class models for general networks (Burkhard Schmitt [64], Borges et al. [72] and IETF RFC 4594/DiffServ), IoT and wireless sensor networks (Duan et al. [2], Nef et al. [79] and Tilak et al. [66]/ Chen and Varshney [63]/ Borges et al. [72]) and industrial networks (ISA 100 and Neumann [50]) have been established. Nevertheless also here, important deficiencies such as no detailed documentation and clarification of parameters and parameter ranges, a too generic approach or too heavy focus on manufacturing and process control limit the applicability to the entire IIoT space.

Furthermore it is sometimes hard to distinguish whether a model is a traffic- or a service class model, as both model types are somewhat related to each other. In the overview in this chapter the suggestion of the respective authors was followed, whether the model was a traffic- or service class model.

In terms of QoS parameters, a list was complied that gives an overview of the parameters in the literature. The parameters were classified into application related, network related and node related ones. The most high-level criteria are the application related parameters, that partially depend on lower level parameters, as it's e.g. the case with delay tolerance, latency and hop-count. However also here, not all parameter are suitable to include in a QoS model, as they may be too technical, too specific for one network topology type or where the parameter value is obvious.

All in all there is no ready to use QoS model yet that is suitable for the Industrial IoT domain. On the other hand, there is a lot to built on to form a new IIoT QoS model. Next to QoS model related work, also previous research on network selection was revisited. Here, shortcomings in terms of the applicability of the models to industrial settings and on the modern connectivity landscape were identified. Similarly, related work on the attempts to measure QoS performance of LoRaWAN was presented. However, none of the measurements were conducted in a real-world industrial environment. Therefore, more work is needed in these directions, which is aimed for during the next chapters of this research study.

4 A Quality of Service Model for Industrial IoT Networks

As laid out in the last chapter, the network QoS models that were defined in the past don't suit the entire Industrial IoT domain, either because they are too generic, too focused on one specific aspect or because they missed important features. Therefore a new quality of service model that is oriented towards the various IIoT use cases is developed in this thesis. The remainder of this chapter is as following: at first, the methodology that was used for creating the IIoT QoS model is presented, followed by the explanation of the parameters that were found to be relevant for the model. Next, the new IIoT QoS model is introduced, that builds on the selected parameters and defines various service classes for different use cases. As a last step, the service classes are explained and the use cases are assigned to the service classes. Finally, the chapter ends with a summary of the created IIoT QoS model and with remarks about the suitable application of it.

4.1 Methodology

This section describes the methodology that was used to create the new IIoT QoS model in this thesis. The creation was guided by the ITU recommendation G1000 [88], that includes a framework for the creation of a QoS specification. As the G1000 originally only targets the area of communication services like telephony, it was adapted to the IIoT domain, to be suitable for this thesis.

The first major step was to establish a matrix that includes the IIoT use case on the left side and a set of QoS parameters at the top.

Therefore the use cases from section 2.3 were listed in the first column of an allocation table and a unique identifier was assigned to each one. Next, the fitting traffic classes from Borges et al. [72], Chen and Varshney [63] and ISA100 were assigned to each use case, based on domain knowledge and information from the papers that described the use cases [72] [63] [18].

As a second part of the matrix, the list of used parameters within the QoS model had to be compiled. To do this, all parameters that were reported in the literature were listed up. This parameter list was then adapted to suit the needs and design challenges of IIoT. To achieve this, missing (but important) parameters were added and unnecessary, too technical or too generic parameters were deleted from the list. The final list was then included in the top row of the allocation table, so that a matrix with the use cases at the left and the parameters at the top was formed.

Now the next task was to fill the empty matrix and assign parameter values to each use case. The traffic classes that were assigned to each use cases were used to facilitate this process, though it became clear again that they are too generic in scope, to be of real value. The parameter values were then derived from the description of the use case in the respective literature source, domain knowledge and input from experts in the field of industrial IT and IoT.

Following, the uses cases were clustered into service classes through the comparison of their parameter assignments. Like this it was possible to build up a class taxonomy, that makes it easy to classify new use cases in the future. Therefore, all parameter assignments were compared and the most distinguishing parameter was used to split the use cases in two groups. Then, for each group, the next important parameter was used to split the use cases again. This was repeated, until a suitable number of service classes could be identified and the further breakdown wouldn't have made sense. As a last step, the taxonomy of the classes was built up, based on the splittings defined in the step before, to enhance the usability and comprehensiveness of the QoS model. Finally, all use cases were checked with the resulting QoS taxonomy, to ensure the correct reproducibility of the class assignments.

4.2 Industrial IoT QoS Model

In the following, the developed QoS model will be presented. First, the chosen parameters as the main building blocks of the model will be described. Next on, the created taxonomy will be presented and finally the different service classes will be explained to more detail.

4.2.1 Parameters

As described in ITU recommendation E802, the list of parameters should neither be too narrow, nor too long, to allow the proper specification of dedicated service classes without making the model posing too much constraints on the network [74].

From the 29 different parameters that were used in the literature in the past, six were directly used for the classification of IIoT use cases. These six were namely *reliability*, *(roundtrip) delay tolerance*, *coverage*, *interactivity*, *QoS support* and *sampling rate*, thus five application-related and one node-related parameters. Two parameters that were somewhat related to existing ones are *node mobility* (related to mobility support) and the probable *power source* (related to energy efficiency). The last parameter is the *usual message size* for the specific use case. In the following, the parameter choices are explained in more depth.

First, the choice to redact 21 parameters is laid out, starting with the six left out application related criteria. The parameter (system) *lifetime* is hard to specify in a WSN application and can be different from one case to another. Also it is related to the power source and the energy consumption, which is more easy to specify and more useful for a classification into service classes. Later on, the lifetime might be a parameter for a service level agreement with a service provider, but it is not directly useful in defining service classes. On the other hand, parameters such as security, mission-criticality, end-to-end behaviour and directionality are mainly the same for different IoT applications in the industrial space. All IIoT applications are *mission-critical* and should therefore aim for a maximum level of *security*. As already mentioned by Chen and Varshney [63], WSN applications are *non end-to-end* in general and therefore this criterion is unnecessary to mention. *Directionality* of the network should always be bidirectional, to allow maintenance and configuration management of the end-nodes. In terms of *availability*, the network should in the best case always be always available, but the severity of a network outage is also related to the reliability of the network.

Next, leaving out several network- and node-related parameters is explained. *Signal parameters* like SNR or RSSI, *jitter*, *time synchronization* and *processing power* are left out, because they are too technical to specify for every use case. Also the *node density* and *hop-count* is mainly relevant for the planning of mesh networks and is therefore not specified here. Other criteria, such as *scalability*, *accuracy* or *maintainability* should always be given by the network. *Heterogeneity* and *self-organization* of nodes is thereby related to maintainability. The network-related parameters *latency*, *throughput* and *packet delivery ratio* (as well as *fault-tolerance*) are connected to the selected high-level parameters reliability, roundtrip delay tolerance and message size, which will be explained in the following.

After laying out why some parameters were not used in the developed QoS model, now the selected parameters parameters will be described. The parameter *reliability* was chosen, because the industrial space demands highly reliable transmission in some areas (such as industrial control), but allows also less reliable data transfer for other use cases (e.g. maintaining statistics). Therefore it is necessary to distinguish between different levels of network-traffic reliability. Four levels of reliability were defined, based on the needed packet delivery ratio (PDR) of each level. The four reliability levels are:

- Very high (PDR > 99.995 %)
- High (PDR > 99 %)
- Medium (PDR > 90 %)
- Low (PDR < 90 %)

The service level agreements of AT&T, Verizon and MetroWireless, all service providers of mobile communication networks in the USA, as well as the research by Dong et al. [89] form the basis for the partitioning of the levels. The reliability is also related to the fault-tolerance parameter, but reliability, together with PDR, was found to better describe the needs from a use case perspective.

The next chosen parameter for the QoS model is *roundtrip delay tolerance*. It specifies the roundtrip latency, which is acceptable for the respective use case. Again, four levels of delay tolerance were defined:

- Very low (roundtrip latency < 0.01 second)
- Low (roundtrip latency < 0.1 second)
- Medium (roundtrip latency < 1 seconds)
- High (roundtrip latency < 10 seconds)

The levels were formed based on the requirements for hard-realtime applications in industrial control, ITU recommendation Y1541 and the upper latency bound of the NB-IoT technology [90] [50] [91]. Although reliability and roundtrip delay tolerance are not connected per se, frequently very high requirements for reliability come along with a very low delay tolerance, as for example in industrial control.

Coverage of the network is another parameter that is very important for different quality of service levels in IIoT. In this thesis, it is distinguished between local coverage, as coverage of a room, a building or a limited area, such as a plant site, and global coverage, such as nationwide or international coverage. Based on the required network scope, different considerations regarding wireless network technology and scalability have to be taken into account.

Somewhat related to the coverage parameter is the criteria of *node mobility*. Though not directly in the derived parameter list from the literature, it is also connected to the mobility-support node criteria. The node mobility parameter specifies whether a node usually moves during operation (as e.g. a mobile robot or a sensor on a shipping container) or not. Depending on the mobility, handoff mechanisms may be needed from the wireless technology, when the node moves from the range of one wireless gateway to another one. This has to be taken into account, when designing the network, for a flawless quality of service.

Next, there is the newly introduced parameter of the usual *message size* for the specific use case, which is connected to the already defined throughput parameter. While throughput is more a parameter for the bottom-up perspective, the message size is usually known for a use case and together with delay tolerance then forms the throughput requirements that is needed for the respective service class. This throughput-requirement then allows to preselect the possible wireless technologies for this service class. Three different levels of message sizes were specified, based on the size of different sensor readings by Samie et al. [92]:

- Small (size < 100 byte)
- Medium: (size < 100 kB)
- Large: (size < 1 MB)

Together with the message size, the *sampling rate* is another parameter that is important for the assessment of problems through network congestion. When too many large messages are sent out with a high sampling rate, but the network only has low throughput, network congestion occurs and the required quality of service can not be met anymore. While some use cases, as e.g. industrial control, require a very high sampling rate with lots of small messages, other applications allow a less frequent transmission of messages, which is more in the area of minutes or even hours. An overview of sampling rates for different applications is provided by Akerberg et al. [17].

Also necessary to specify is the *power source* of the node, which has an impact on the requirements for energy efficiency and allowed energy consumption. While most use cases will require battery operated nodes, in some cases also other options are possible. Actuator nodes usually are close to a wired power

supply that is used by the actuator and therefore don't face the challenge of energy resource constraints. In other scenarios, energy harvesting from the environment might be an option, e.g. through solar cells in outdoor locations.

In terms of the criterion *interactivity*, only a minority of the use cases is highly interactive. However, for these use cases it is highly relevant, as e.g. the interaction between a sensor and an actuator node in the case of industrial control systems. Therefore interactivity should be specified as well.

Finally, the question whether active *QoS support* of the network is relevant or not, marks the last parameter that needs to be determined for a use case. In general, QoS support should be available by the network, when the reliability of the use case is high or very high, so that the package of these services can be transferred with higher priority. Again, this will only be the case for a minority of the use cases, but is highly relevant for those that require it.

To sum up, a total of nine parameters were chosen for the classification of service classes. These nine were:

- Reliability
- Roundtrip delay tolerance
- Message size
- Coverage
- Node mobility
- Power source
- Interactivity
- Sampling rate
- QoS Support

These parameters allow the suitable differentiation of one class to another and form the basis for the QoS model that will be presented in the next section.

4.2.2 QoS Taxonomy

Next on, the developed IIoT QoS taxonomy will be presented, with an emphasis on the identified service classes and their application. Also a taxonomy will be presented, that can be used for the easy classification of future use cases.

Building on the parameters identified in the last section, a matrix with use cases and parameter assignments for each use case was created. The complete list of matrices for all use cases is attached in appendix A.1. An excerpt of the matrix is shown in table 4.1, which features three different use cases that show the diversity of the different scenarios.

While a use case for the tracking of the quality of a product along the supply chain demands global coverage, node mobility, battery-power supply and medium delay tolerance and reliability requirements (UCPc01), closed loop control of a manufacturing process has very strict delay and reliability criteria, while the actuator node probably runs on normal power supply (UCPc18). Of course there might also be cases where other parameter assignment are suitable for a certain use-case. However, the parameter assignments were meant to represent the average and usual conditions, based on the input from the literature sources, domain knowledge and from reviews of experts in the field of Industrial IoT and industrial information systems. Based on the assignments of QoS parameters to the use cases, the most distinguishing parameters were identified as split criterion for the creation of an IIoT QoS taxonomy. The first split criteria is therefore the required coverage and it is distinguished between global and local coverage. Also the service classes are divided in the two groups of service classes for the demand of global coverage (G*x* classes) or local coverage (L*x* classes), as the further requirements differ substantially between them.

For the global service classes, the next split decision is based on the reliability, as this is a major criterium for network traffic and a traditional QoS criteria, as well as roundtrip delay tolerance. Finally,

		Supply chain	Process and equipment monitoring	Control purposes
Use Case		Track the physical integrity and quality of the product	Predictive maintenance	Closed loop control (process manufacturing)
Use Case ID		UCPc01	UCPc05	UCPc18
Reliability		medium	medium	very high
Roundtrip Delay Tolerance		medium	high	very low
Message Size		medium/small	medium	small
Global Coverage		x		
Local Coverage	**Room**		x	x
	Building		x	x
	Area		x	x
Node mobility		y	y / n	n
Power Source		Battery	Battery/ Power supply	Power supply
Interactivity		n	n	y
Sampling rate		Depends	10 m	1-10ms
QoS Support		n	n	y

Table 4.1.: Examples of IIoT process use cases with assignment of QoS parameters

the usual message size of the use-case is a last criteria that distinguishes some of the service classes. Together with the roundtrip delay tolerance it determines the required throughput from the wireless technology to achieve the desired quality of service.

For the local classes, slightly different subsequent split criteria apply. The first split is based on the combination of reliability and roundtrip delay tolerance, as it turns out that there exist some frequent combinations of both. Very high requirements for reliability often come with very low tolerance for roundtrip delay, as for example in the field of industrial control. On the other hand, there exist a couple of applications that have less demanding requirements for both criteria. Next on, the use cases are split according to the usual message size, that is sent out, similar to the part of the taxonomy for global coverage. However, instead of stopping there, the use cases are further broken down according to the maximal local area they have to cover. Here it is distinguished between the coverage of a room or the coverage of a building or a wider area, such as an entire production site. For a room, it is further distinguished between a room with normal or with challenging conditions, like when there are heavy sources of interference or reflections, as it might be the case in a machine room or a laboratory.

The final taxonomy is depicted in figure 4.1. The general idea behind it is to place extreme use cases as early as possible in certain service classes and split other use cases into less restrictive, but distinguishable classes subsequently.

The ordered numbering is inspired from the classes of ISA 100 and the emphasis on delay tolerance and reliability similar to IETF RFC 4594, Nef et al. [79] and Chen and Varshney [63]/Borges et al. [72]. Also the visualization of the classes by the means of a taxonomy is motivated by the representation of [64] and of the IntServ traffic model. However the clear emphasis on Industrial IoT use cases, that can be classified into service classes by the means of a taxonomy with specific parameter value assignments for each service class is a new type of QoS model.

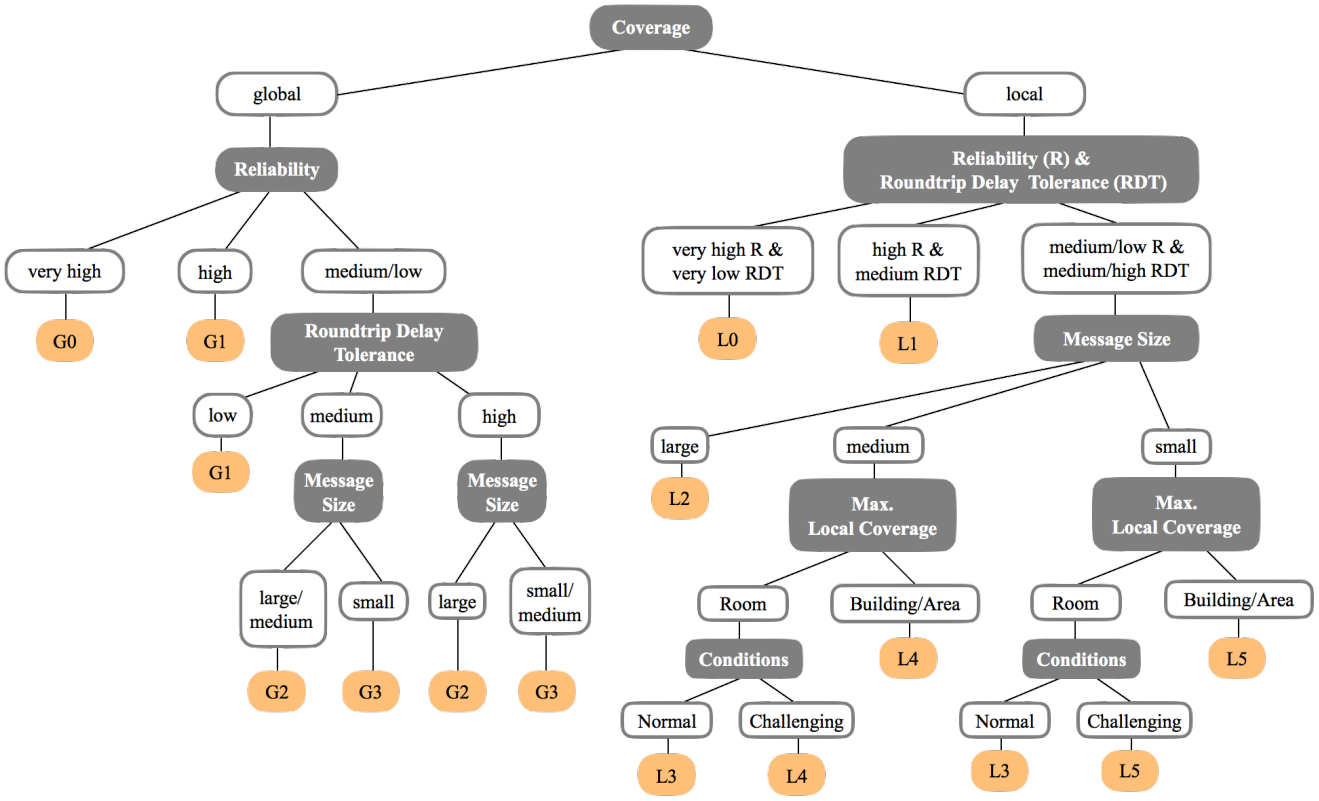

Figure 4.1.: An IIoT QoS Taxonomy.

4.2.3 Service Classes

In the following, the different service classes, that are the outcome of the created taxonomy, are explained to more detail. As already said, the classes are distinguished in those for global and local coverage. Additionally, the criticality of the service class is shown by the digit of the class. Classes with higher criticality have a lower number and the other way around. Therefore, the class with L0 would be a class that has a high criticality and requires local coverage, while the class G3 is less critical and demands global coverage. A detailed presentation of the service classes is given below.

Service Class G0

This is the most critical global service class, with reliability requirements of more than 99.995 % packet delivery ratio. Usually such a high reliability is not required on a global scale, though rare cases might occur where the main value driver of a product is the sensing capability and the sensed data is very critical and doesn't allow for dropped packages. In that case, the architecture of the product should be reconsidered so that the data is transferred in a more secure way, e.g. through a cable to a local processing system.

Service Class G1

Though less critical than G0, service class G1 still demands high reliability and a packet delivery ratio of 99% or more. This might be needed for smart products that include sensor devices in the packaging and have to report the status of the package content with high reliability or for pay-as-you-go pricing models of products that are frequently changing the location. Another type of applications that fall into the G1 category are those that have a very low roundtrip delay tolerance of less than 100 ms. For these classes, it should be considered to ensure a service level agreement with the provider of the communication service (such as mobile network carriers as Vodafone or AT&T). Another option is to

connect to a local gateway that aggregates the data and ensures the reliable transfer later on or acts as an intermediate processing and platform hub (fog computing).

Service Class G2

Service class G2 is focused on everything that demands less reliable data transfer (PDR < 99%), but where a certain connection throughput is required to achieve the quality of service. This could either be the case when a medium roundtrip delay tolerance (RDT) (< 1 second) is required and large (< 1 MB) or medium (< 100 kB) message sizes occur or when the RDT is high (< 10 seconds) and large message sizes are present. This class is therefore suitable for uncritical applications with somewhat bigger message sizes, that can stem from the transmission of e.g. voice, a stream of images or from larger sensor values like from a velocity sensor. Use cases in this class can come from the product or process area. From the product area, especially the improvement of customer support has to be mentioned here, while the continued insurance of the physical integrity and quality of the product as well as the compliance to regulations along the supply chain are relevant topics from the industrial process area.

Service Class G3

By far the most use cases are incorporated in class G3. Equally to G2, the demand for reliability is less strict here (PDR < 99%). Furthermore also the required throughput of the connection can be lower, so that applications with medium delay tolerance (< 1 second) and small message sizes (< 10 kB) or with high delay tolerance and medium or small message sizes. These smaller messages sizes can stem from the transmission of simple commands or from sensors that generate data less frequent, like it's the case with temperature. Examples from smart products are cases where it's tracked how the product is used, the delivery of predictive maintenance or where sensors in the product or the packaging have to transmit smaller data-points. From the industrial process perspective, all supply chain related activities may fall into this category, when the size of the transferred messages allows it.

Service Class L0

After having presented the global service classes, the most critical local service class is L0. Here, a combination of very high reliability requirements with packet delivery ratio of greater than 99.995% and very low roundtrip delay tolerance of less than 10 ms are present. This is the case for emergency monitoring services like fire detection systems and for closed-loop industrial control systems, including manufacturing control and smart power control scenarios. Due to the high criticality of these services, it is advised to consider using a cable for these activities, as an outage of the wireless network (either due to an error or due to a jamming attack) can cause severe damage and lead to high cost.

Service Class L1

The class L1 is similar to the class G1, in that it requires high reliability combined with medium roundtrip delay tolerance. Also the associated use cases are the same as for G1, with the difference that it's enough for the linked use cases to cover a local, instead of a global area. Also here, one measure might be to ensure a service level agreement with the provider of the network service. Additionally, there is the option to use a licensed wireless frequency band for the connectivity or to design the application in a way so that the data is saved temporarily at a gateway and the data is transferred when the next reliable connection is established.

Service Class L2

Next to a medium or low required reliability and medium or high roundtrip delay tolerance, service class L2 comes with large message sizes. This is closely related to class G2, where larger message sizes from transmission of voice, image streams or more frequent sensor values (e.g. velocity sensor) can occur. Again, it could be the scenario that the customer support is enhanced through smart product features or that the general monitoring and information gathering of the environment takes place.

Service Class L3

In terms of reliability and delay tolerance, service class L3 is equal to class L2. However, differences arise in the message size and the maximum local coverage that is required by the use case. Class L3 therefore covers all case, where the maximum coverage is a single room and the conditions in this room are normal (e.g. no sources of heavy interference and no dominant spots of reflection) and the message size is medium or small. This can be the case for nearly all product related scenarios and for predictive maintenance in non-hostile industrial environments.

Service Class L4

Service class L4 comes with medium/low reliability and medium/high roundtrip delay tolerance. Also it is only associated with medium sized messages and covers use case that either have to cover a wider area (as e.g. an entire production site), a building or a room in a hostile industrial environment. All cases face similar challenges in terms of interference and obstructions through reflections. Therefore they are considered equal to some extent. Cases might be again the smart products or predictive maintenance or information gathering in a usual industrial setting.

Service Class L5

The service class L5 is similar to L4, as it also covers medium/low reliability, medium/high roundtrip delay tolerance and a maximum local coverage of a wider area, a building or a room with challenging conditions. The only difference is that it covers only use cases with small message sizes, that are produced by sensors with less frequent data generation rates, as for example a temperature sensor or GPS coordinates. By far the most use cases fall into this category, as maintaining statistics, tracking inventory and meter energy consumption are not business critical applications.

Finally, table 4.2 gives an overview about which use case falls into which service class. Some use cases, as e.g. smart products where the main value driver is the sensing functionality (UCPd01), can come in a wide range of flavours and therefore fall into multiple class categories. Other use cases however, such as the localization and tracking of unfinished parts for inventory management (UCPc23) can be narrowed down to unique parameter values that apply in the average scenario.

Service Class	**Assigned Use Cases**
G0	UCPd01
G1	UCPd01, UCPd05, UCPd06
G2	UCPd01 UCPd04 UCPd06 UCPc01 UCPc03
G3	UCPd01 UCPd02 UCPd03 UCPd06 UCPc01 UCPc02 UCPc03 UCPc04
L0	UCPd01 UCPc08 UCPc11 UCPc18 UCPc19 UCPc20 UCPc21
L1	UCPd01 UCPd05 UCPd06
L2	UCPd01 UCPd04 UCPc09
L3	UCPd01 UCPd02 UCPd03 UCPd04 UCPd06 UCPc05
L4	UCPd01 UCPd02 UCPd03 UCPd04 UCPd06 UCPc05 UCPc09
L5	UCPd01 UCPd06 UCPc09 UCPc10 UCPc12 UCPc13 UCPc14 UCPc15 UCPc16 UCPc17 UCPc22 UCPc23

Table 4.2.: Service class with assigned use cases.

4.3 Summary and Discussion

In this chapter, the primary aim was to develop an IIoT QoS model that is specifically targeted towards the Industrial IoT domain. Therefore, the identified use cases were listed and used as the basis for the development of the model. Next on, suitable QoS parameters were selected based on previous research and from requirements of the industrial domain. Now parameters were assigned for each use cases, based on information from the literature sources of the use cases, domain knowledge and input from experts in the field of industrial IT and IoT. Building on that, the QoS taxonomy was iteratively developed by splitting the use cases into classes, based on different criteria. The final taxonomy allows the easy classification of future use cases into the different service classes. A total of ten classes was identified, that are split into global and local coverage classes and further ranked according to their criticality in descending order (0 being the most critical). The classes were described and the use cases that formed the starting point were assigned into the respective service classes.

Different to previous QoS models, the classes are clearly distinguishable, so that the unambiguous classification of new use cases is possible. This was achieved, by allotting clear parameter values to each split point in the taxonomy, so that each class has a unique parameter configuration. Also it was made sure that the classes are neither too broad, nor too narrow, so that they have a meaningful scope and fit the right coverage level.

The developed QoS model therefore provides a new way of evaluating IIoT use cases, to assess the criticality and required quality of service level that comes with their connection via a wireless network.

5 Scoring Model based Wireless Technology Selection

After having presented the developed IIoT QoS model, the next step now is to select the technologies, that are most suitable for each service class and for a specific use case in particular. Therefore, several techniques are applied to identify the most fitting technology, out of the technologies presented in section 2.4.3. The chapter is organized as follows. First, the methodology behind the selection of the technologies is laid out. Next, the technologies that meet the minimal requirements of each service class are presented. Finally, the scoring model is presented and a summary is given.

5.1 Methodology

The following methodology was applied to determine the best wireless connectivity option for a specific scenario. First, the technologies that meet the minimum requirements of the service class in terms of coverage, reliability, latency and message size are preselected. This was done based on the information about the technology capabilities, as shown in section 2.4.3.

Following, some service classes may end up with multiple technologies that would suit the required needs, of which one technology has to be selected. Therefore, a scoring model was developed, that allows the easy selection of the most suitable technology, based on criteria like scalability, energy consumption and further preferences that are specific to the use case (e.g. preference of a time synchronized network). The scoring model was developed in accordance with the work of Zöller [82], who created a similar model for the evaluation of alternatives. Also Song and Jamalipour [80] and Bari and Leung [81] developed related models for network selection in the past, though they are very focused on consumer end-users, don't reflect the connectivity landscape of today and are not integrated with a holistic QoS model.

To develop the model, the first step was to come up with a list of criteria that is used for calculating the scoring value of the wireless technology. The list was partially based on the QoS parameters that were too detailed for the service classes or that were not used in the taxonomy due to their technical nature. Other important parameters for the evaluation of wireless technologies, such as the topology, duty cycle regulations or service provider operated vs. self operated mode, were included as well.

The next step, was to determine the weight of each criterion in the scoring model. To do that, the matrix-based weight determination mechanism of Zöller [82] was used, which is similar to the analytic hierarchy process used by Song and Jamalipour [80]. A pairwise criteria comparison was performed, where the relative importance $c_i j$ of each criteria c_i was determined (Equation 5.1).

$$\text{Relative importance } c_{ij} := \begin{cases} 2, & \text{if } c_i \text{ more important than } c_j; \\ 1, & \text{if } c_i \text{ as important as } c_j; \\ 0, & \text{if } c_i \text{ less important than } c_j. \end{cases} \tag{5.1}$$

The overall weight w_{c_i} of each criteria was then determined by dividing the sum of all relative importance values of a criterion c_i gathered during the pairwise criteria comparison, by the overall sum of all relative importance values (Equation 5.2).

$$\text{Weight } (c_i) := w_{c_i} = \frac{\sum_j c_{ij}}{\sum_i \sum_j c_{ij}} \tag{5.2}$$

After determining the weight w_{c_i} of each criterion, the assignments of values for each criterion for each wireless technology had to be accomplished. Two types of criteria existed. The first type of criteria c_l could be rated on a 5-point Likert scale from very low (1) to very good performance (5). The second type of criteria c_d are dichotomous (value -1 or 1), as for example whether a network is self-operated or not. The assignment of values v_{c_i} for the criteria was based on the technical information from section 2.4.3 and from additional literature sources [9] [93] [94] [95]. Finally the overall score of each technology had to be calculated. For the dichotomous criteria, it is possible to include preferences $pref_{c_d}$ for one case in the score calculation. The final score s_t for a technology was calculated according to equation 5.3. The higher the score, the better rated is the technology.

$$\text{Score}\,(t) := s_t = \sum_l w_{c_l} \frac{v_{c_l}}{5} + \sum_d w_{c_d} pref_{c_d} v_{c_d} \tag{5.3}$$

The equation thereby consists of two sums for the Likert-rated and dichotomous criteria. The calculation of the Likert-rated criteria is thereby straight forward. v_{c_l} is at least 1 and maximal 5 and thereby the second term is $\frac{1}{5} = 0.2$ respectively $\frac{5}{5} = 1$. For the dichotomous variables, a preference $pref_{c_d}$ could be stated, that is either 1 or -1, based on the use case. For example it might be preferred to engage with a service provider of a network service (value -1) while the technology has to be self operated (value 1). In that case, a negative value would be the outcome ($1 * -1 = -1$), that decreases the final score, as the preference could not be met. In case both options are equally good and no option is preferred, $pref_{c_d}$ can be set to 0, to not influence the decision by this criterion.

By comparing each score of the subset of technologies that achieve the minimal requirements of the service class, the technology with the highest score is the one that should be selected for the desired use case.

5.2 Preselected Wireless Technologies

The first step is to preselect a number of technologies that fit the needs of the desired service class. Following, the selected technologies for each service class are presented. For the local classes, always the best self-operated and provider-operated technologies are included. Furthermore only energy-efficient options are considered, to already narrow down the set of options.

As already written, for service class G0 and L0 it is not recommended to use any wireless connection at all, as they are too critical to be exposed to inevitable link failures due to interference or jamming attacks. This is in line with the recommendations of IETF RFC 5673, who also propose to desist from connecting highly critical applications via a wireless link [18].

For class G1, a reliable globally available connection can be established by using LTE or NB IoT with a service level agreement (SLA) of the mobile network carrier. When an international operation is required, additional roaming agreements with a multitude of carriers have to be established. LTE under an SLA can also be used for applications with very low roundtrip delay tolerance of less than 100 ms, as it has a transmission time interval (the duration of a transmission on the radio link) of less than 40 ms, compared to 640 ms for NB IoT [60]. Another option is to design the application in such a way that a connection to a local gateway is established by the means of WiFi 802.11ac or Bluetooth, where the gateway acts as a local processing and command hub and transfers the data reliably via LTE or NB IoT.

The only viable connectivity option for class G2 is LTE. The bigger message sizes and medium roundtrip delay tolerance require a high performance, that can not be delivered by NB IoT.

For class G3, two options are feasible. A seamless operation by meeting the QoS requirements should be possible with NB IoT. The smaller message sizes or relaxed delay tolerance requirements make NB IoT preferable here over LTE, as the energy consumption is lower and the QoS criteria are still met. Another way to connect G3 services could be by using LPWAN carriers, that span their network across

the country and allow access based on monthly or yearly fees. One example is SigFox, though the usage of this service is not recommended here, due to no encryption of the wireless channel.

Similar to class G1, also the services in class L1 can be connected through LTE or NB IoT in combination with an SLA from the service provider or the use of a local gateway. Additionally, the operation of the wireless link in a licensed frequency band might be an option. This could be done with ISA 100.11a, Symphony Link or Weightless-P. Depending on the use case, the mesh-network based ISA 100.11a, in case of a dense deployment for industrial control, or one of the two LPWAN technologies Symphony Link or Weightless-P, for a wider field, are favourable.

Also equal to class G2, class L2 has to deal with large message sizes. Therefore the options are LTE and additionally WiFi 802.11ac, as they allow very high data transmission rates.

For class L3, which deals with the connection of nodes in a room under normal conditions, Bluetooth Low Energy (BLE) or NB IoT are good connectivity options. They allow the most energy-efficient data-transmission for the connected devices. As the environment is not hostile, they should be sufficient to achieve the desired QoS level.

Class L4 has a multitude of connectivity options. First and foremost, the upcoming low-power WiFi 802.11ah standard has to be mentioned here. Through the higher data transmission rate and IPv6 out-of-the-box, it is very suitable here. If the delay tolerance is higher, also LPWAN solutions like LoRaWAN can be an option here. Due to the higher required throughput, NB IoT could be chosen as well, although the operational expenses will probably be higher due to the necessary contract costs. As all technologies operate in the sub GHz area, they are also better suited for the connection of nodes in a room under challenging conditions. Additionally, technologies with spread spectrum technologies are good in this space.

Finally, service class L5 can be entirely covered by LPWAN technologies or by NB IoT. The small package sizes don't pose a problem for the limited throughput of technologies like LoRaWAN, Weightless-P or Symphony Link and allow the most cost-effective and widespread coverage of the required local areas.

Service Class	**Suitable Wireless Technology**
G0	/
G1	With SLA: LTE; NB IoT With intermediate gateway: WiFi 802.11ac; Bluetooth
G2	LTE
G3	NB IoT; LPWAN carrier (SigFox, Ingenu)
L0	/
L1	With SLA: LTE; NB IoT With licensed band: ISA 100.11a; Symphony Link; Weightless-P With intermediate gateway: WiFi 802.11ac; Bluetooth
L2	WiFi 802.11ac; LTE
L3	BLE; NB IoT
L4	WiFi 802.11ah; LPWAN (if high delay tolerance); NB IoT
L5	LPWAN; NB IoT

Table 5.1.: Service classes with suitable technologies.

5.3 A Scoring Model for Technology Selection

After preselecting the suitable technologies for each class, all classes other than G0, L0 and G2 end up with multiple connectivity options. The next step is now to select the best technology for a certain use case. This is done through the already mentioned scoring model.

First, the list of criteria that is used for the scoring is described. The *energy efficiency* (c_e), *throughput* (c_t), *scalability* (c_{scal}) and *security* (c_{sec}) are all QoS relevant parameter that were not directly included in the QoS taxonomy. Nevertheless, due to their technical nature, they are suitable to be included in the scoring model for technology evaluation. All of them can be rated on the 5-point Likert scale. Furthermore, technical criteria like required compliance to legal *duty cycle regulations* in the EU (c_{dc}), the *network topology* (c_{top}; 1 = start topology, -1 = mesh topology), the support for time sychronization of nodes (c_{ts}; 1 = time synchronized, -1 = not time synchronized) and the *mode of operation* (self-operated vs. service provider-operated) (c_{op}; 1 = self-operated, -1 = provider-op.) are included. The first of those can also rated on a 5-point Likert scale, while the other three are of dichotomous nature.

Next on, the relative weight of each criteria has to be determined, as described in the methodology section. The matrix for the weight evaluation is depicted in table 5.2. As shown, duty cycle compliance, energy consumption and security achieve the highest weight, because they have the greatest impact on the QoS performance of a wireless technology, if they are insufficient.

	c_e	c_t	c_{scal}	c_{dc}	c_{sec}	c_{top}	c_{op}	c_{ts}	Sum $\sum_j c_{ij}$	Weight w_{c_i}
c_e	1	2	1	0	1	2	2	2	11	0.17
c_t	0	1	1	0	1	1	0	0	4	0.06
c_{scal}	1	1	1	0	1	2	1	2	9	0.14
c_{dc}	2	2	2	1	1	2	2	2	14	0.22
c_{sec}	1	1	1	1	1	2	2	2	11	0.17
c_{top}	0	1	0	0	0	1	0	2	4	0.06
c_{op}	0	2	1	0	0	2	1	2	8	0.13
c_{ts}	0	2	0	0	0	0	0	1	3	0.05
									64	1.00

Table 5.2.: Matrix-based weight determination of scoring criteria.

Now the values of each criterion had to be assigned for every technology. As already written, this was done based on the information from section 2.4.3 and from the respective literature sources used there. For the continous-rated technologies, the best option was rated with a five and the other technologies subsequently, based on their relative performance. The final assignment is shown in table 5.3.

Finally, the overall scores of the technologies can be calculated, based on the weighting of the criteria, the criterion assignments and the preference for the dichotomous criteria. The calculation was carried out as described in the methodology section earlier. Table 5.4 shows the scores for all technologies with different preference configurations.

Service class L3 for example initially had the option to chose between BLE and NB IoT. Now, depending on the preference selection, one of these options comes out as the winner that will be the clear recommendation for the desired use case.

		c_e	c_t	c_{scal}	c_{dc}	c_{sec}	c_{top}	c_{op}	c_{ts}
Short-Range Wireless Netw.	BLE	5	3	1	5	4	1	1	1
	ISA100.11a	4	2	3	5	4	-1	1	1
Wireless Local Area Networks	802.11ac	2	5	4	5	3	1	1	-1
	IEEE 802.11ah	4	1	4	2	3	1	1	-1
Low Power Wide Area Networks	LoRaWAN	4	1	3	1	4	1	1	-1
	Symphony Link	4	1	3	5	4	1	1	1
	Weightless-P	4	1	4	5	5	1	1	1
	WAVIoT NB-Fi	4	0	4	1	5	1	1	-1
	Ingenu RPMA	4	1	4	5	4	1	-1	-1
	SigFox	4	1	3	1	1	1	-1	-1
Cellular Networks	LTE	2	4	5	5	5	1	-1	-1
	NB IoT	4	2	5	5	4	1	-1	-1

Table 5.3.: Assignments of values for each criterion for each wireless technology.

		Score				
		$pref_{c_{top}} = 1$ $pref_{c_{op}} = 1$ $pref_{c_{ts}} = 1$	$pref_{c_{top}} = -1$ $pref_{c_{op}} = 1$ $pref_{c_{ts}} = 1$	$pref_{c_{top}} = 1$ $pref_{c_{op}} = -1$ $pref_{c_{ts}} = 1$	$pref_{c_{top}} = 1$ $pref_{c_{op}} = 1$ $pref_{c_{ts}} = -1$	$pref_{c_{top}} = 0$ $pref_{c_{op}} = 0$ $pref_{c_{ts}} = 0$
Short-Range Wireless Netw.	BLE	0.83	0.70	0.58	0.73	0.59
	ISA100.11a	0.71	**0.84**	0.46	0.62	0.60
Wireless Local Area Networks	802.11ac	0.65	0.53	0.40	0.74	0.51
	IEEE 802.11ah	0.54	0.41	0.29	0.63	0.40
Low Power Wide Area Networks	LoRaWAN	0.56	0.43	0.31	0.65	0.42
	Symphony Link	0.83	0.70	0.58	0.73	0.59
	Weightless-P	**0.89**	0.76	0.64	**0.79**	0.65
	WAVIoT NB-Fi	0.61	0.48	0.36	0.70	0.47
	RPMA Ingenu	0.51	0.38	0.76	0.60	0.62
	SigFox	0.20	0.08	0.45	0.30	0.31
Cellular Networks	LTE	0.54	0.42	0.79	0.63	0.65
	NB IoT	0.55	0.43	**0.80**	0.64	**0.66**

Table 5.4.: Scoring values of wireless technologies for different preference assignments.

5.4 Summary and Discussion

By using the previous developed QoS model as an input, this chapter was targeted towards presenting a scoring model based approach for the selection of the best wireless technology for a certain use case. Based on the QoS taxonomy, it is possible to assign a service class to an IIoT scenario, that implies their criticality and the required service level parameters. Following, the first step in this chapter was to preselect suitable technologies for each service class, that meet their minimum requirements. After that, a service class may end up with multiple matching technologies, of which one has to be selected. Therefore, a scoring model was developed, that allows to optionally influence the decision based on certain preferences, such as whether a technology is operated by a service-provider or not. By using the scoring model, a score can be calculated for each preselected technology. The technology with the highest score is then the best option to choose.

Other than the previous work on network selection of Song and Jamalipour [80] and Bari and Leung [81], this research study is specifically targeted towards the Industrial IoT space, instead of only having a consumer-user focused view. In fact, both previous research studies mainly focus on network traffic from voice, streaming and web browsing or other file transfers. Additionally, the newly developed model reflects the connectivity landscape of today, by including cutting-edge technologies in the selection process. Furthermore, the wireless network selection is fully integrated with the QoS model developed before, to enable a truly end-to-end selection process beginning at the use case and spanning to the winning wireless technology.

To sum up, the developed scoring model, in combination with the QoS model, enables to quickly select the best connectivity option for a specific IIoT use case, based on its functional requirements and optional preferences about the technology.

6 Experimental QoS Evaluation of LoRaWAN and LTE

The last two chapters covered the theoretical models that were developed during this research study. Building on that, this chapter is concerned with the experimental evaluation of the achievable quality of service by LTE and LoRaWAN, as a promising LPWAN technology. As already described in section 2.4.3 on wireless technologies for IIoT, LoRaWAN is a widespread LPWAN technology that has a growing community in the IoT field. Although the outcome of the scoring model is, that other technologies might be a better technical fit, LoRaWAN is the only technology that is currently available in the Euorpean Union while having an industrial-ready company behind it. Therefore it was selected for this evaluation. It was compared to LTE, as the current "gold-standard" in terms of coverage, reliability and latency. The evaluation was performed in a real-world industrial setting, to get results that are representative for an Industrial IoT solution.

The chapter is organized as follows. First, the methodology of the evaluation will be explained. After that, the results will be presented and a summary is given.

6.1 Methodology

The methodology section starts with general information on the site of the evaluation, presents the assessed QoS parameters coverage, reliability, latency and supported message size, and finally goes on with information about the test and measurement setup of the LTE and LoRaWAN evaluation.

The experimental evaluation took place at a production site of a large international science and technology company, operating in the area of pharmaceuticals, life science and special materials. The production site forms the major production campus, with 10.000 people working there and a total area of 1.5 km^2.

Eleven measurement points were selected across the production site. The points were evenly distributed across the campus and the measurement took place inside of different representative building types, such as laboratory buildings, office buildings, engineering and maintenance machine shops. Also safe parts of buildings in explosive areas (so called EX areas) were included in the test. An overview of the measurement points is depicted in figures 6.1 and 6.2.

The test was conducted during one day in mid of February 2017. The weather conditions at the day were bad, as it was raining, the sky was cloudy, humidity was at 82% and barometric pressure at 1025 mbar. The temperature was around 8řC during the day.

A total of three message types were included in the test. The first message type (termed ping) was a very small message, with only one byte payload. It represented a single value, as e.g. for the transmission of a button-press or for the command to change the status of a switch.[1] The second message type was a small message of 83 bytes, that represented a typical JSON object with a sensor value.[2] A bigger message was chosen as third message type, consisting of 242 bytes (the biggest possible message size for LoRaWAN) that also form a JSON object with larger sensor readings.[3]

All in all, the following QoS parameters were measured. The coverage of the technology was judged based on whether the data could be sent at the measurement point or not. Additionally, RSSI and SNR were used as an indicator of signal quality for LoRaWAN. For reliability, the ratio of sent vs. delivered packages was used (PDR). Finally, latency was measured for both technologies. The detailed measurement setup is described below.

[1] Ping message: *0*

[2] Small message: { *'ID': '0', 'time': 1351824120, 'sensorName': 'TempSensor1', 'sensorValue': 23, 'Unit': 'C'*}

[3] Big message: { *'ID': '0', 'time': 1351824120, 'sensorName': 'VibrSensor1', 'sensorValue1': '123456789012345678JHGAHJSGFDHJFAHSJDFHJGAFSHDJGFHJSAGSJKHDGFJKAGSDKFHGKHGFKHGASFDKHGKHASGDFDCVAHJGSDVCHGSADFGHASFHJDGFHJSFDHJGASFDHJGHAGSFDHGFASHDGFHJAGSDF', 'Unit': 'Vibr'* }

Figure 6.1.: Measurement points of the experimental evaluation (View 1).

Figure 6.2.: Measurement points of the experimental evaluation (View 2).

The statistical tests for the final evaluation were conducted with IBM® SPSS® Statistics [96].

6.1.1 LTE Setup

Concerning the LTE evaluation, the entire production site is provided with LTE coverage of the carrier Deutsche Telekom with speeds of up to 150 MB/s, partially also 300 MB/s [97].

The setup of the LTE QoS evaluation is described in the following. For the measurement and for the collection of the data, an iPhone 6s with a Deutsche Telekom SIM card was used as LTE gateway and was connected to an Apple MacBook Pro by cable. The MacBook served as processing and data storage unit. The iPhone was set to tethering mode and all other network connections of the MacBook were switched off, to force the connection via LTE. Also network-consuming services on the MacBook were stopped, to not interfere with the test results.

To have a realistic Industrial IoT scenario and to achieve real-world conditions, a web service in form of a Amazon Web Service (AWS) Lambda function in combination with AWS API Gateway was created, that served as test-endpoint. AWS services are frequently used in the industrial world and at the science and technology company and therefore mark a good reference of this test.

A node.js application was written, that runs on the MacBook and connects to the AWS network endpoints. The application measured and stored the latency of the connection.

For the ping message, latency was measured as the time it took to reach the AWS endpoint. For the small and big messages, the latency marked the time the system needed to transfer the JSON objects to the AWS Lambda function and get back the response of successful transmission.

All latency values were stored in a CSV file by the node.js script, together with metadata of the measurement such as message type, measurement location and a timestamp.

The complete setup of the nodes in the field is depicted in figure 6.3.

Figure 6.3.: Example setups during measurement process.

6.1.2 LoRaWAN Setup

After having described the setup of the LTE evaluation, now the LoRaWAN setup is laid out.

As written in the wireless technology section, LoRaWAN is a star-of-start networks, that consists of nodes, a gateway and a network backend-server.

A Lorank 8 gateway as used as LoRaWAN gateway, which was provided by Ideetron. The Lorank 8 device has professional specifications and is a full-fletched LoRaWAN bridge. The gateway was installed at the center of the production site on top of a large storage house. The height of the storehouse was around 30 meter above the ground. Therefore the installation took place with help of an aerial ladder

Figure 6.4.: Installed gateway on top of storage house.

truck if the fire department at the production site. A picture of the installed gateway is depicted in figure 6.4 and the position of the gateway on the industrial production site is marked by the red star in figure 6.1 and 6.2. The eleven measurement points were chosen around this storehouse, to cover the entire production site.

The gateway was connected via Ethernet to a Raspberry Pi board, which acted as a network bridge and was connected to an LTE router for access to the LoRaWAN backend server. The Things Network was chosen as LoRaWAN backend, due to the big community and the easy handling of the platform. The backend server handles the network access of the nodes in the field and fulfil the transmission of the messages to the final application server.

As LoRaWAN node, a RN2483 module from drotek was chosen, that was readily equipped with a 5dB 868 MHz antenna. The module was connected to an Arduino MEGA 2560 microcontroller board, that acted as a controller of the module. The Arduino was also connected to the MacBook, to capture the transmission data of the LoRaWAN connection. The box in figure 6.3 contains thereby the LoRa module as well as the Arduino board. The data was again captured by a node.js application, that consisted of two capturing parts. The first part was used for the RN2483 module, to capture errors, transmission time and SNR values. The measured airtime of the transmission was thereby used as a proxy for the latency of the connection. The second part was for the The Things Network LoRaWAN server backend, to store information from the gateway about RSSI, SNR and successful delivered messages. The different between the number of sent messages at the node and the captured messages at the gateway thereby formed the basis for the calculation of the packet delivery ratio (PDR).

LoRaWAN distinguishes between so called spreading factors (SF), that affect the coverage, the bandwidth and the time it takes to transmit a frame. Similar to Augustin et al. [86], spreading factors 7 and 12 were chosen for the tests. While factor 12 has the lowest data rate and the longest transmission time, it also covers a larger area than factor 7 [86]. While the node configured with SF 7 was able to send all message types, with SF 12 only the sending of the ping message was possible, due to the low available throughput and the limited message size to 50 byte. Other LoRaWAN factors that influence the transmission quality are the coding rate and the channel bandwidth. Both parameters were set to the standard values (coding rate: 4/5; channel bandwidth: 125kHz), as also done by Augustin et al. [86] and Adelantado et al. [48].

To be compliant to the duty cycle regulations, a time delay between the transmission of the messages was set. For SF7, first the ping message was sent out, followed by the small and the big message in a time distance of 10 seconds each. Then, it was waited for 35 seconds until the next cycle started. For SF12, the attempt to send a ping message was started every 15 seconds.

6.2 Results of the Evaluation

This section presents the results of the experimental connectivity evaluation. At first, the LTE results will be presented, before the LoRaWAN data is introduced. For both technologies, coverage, reliability and latency, as well as the covered QoS classes from chapter 4 will be reported. Finally, the performance of the two technologies will be compared.

For LTE, a total of 2865 messages were sent out to the AWS Lambda service during a time-period of 4 hours and 3 minutes. Thereby each message type (ping/small/big) was delivered 955 times.

The coverage of LTE was flawless. The connection was possible at each of the 11 measurement points, even in the building in the Ex area, that had specially coated windows that reduces the transmission of electromagnetic waves.

Also the reliability of LTE was very good, with a packet delivery ration of 100%. All messages were delivered to AWS Lambda without an error.

The latency in terms of roundtrip delay (from sending the request to the delivery of the response) was rather dependent on the message type (ping vs. small/big). The measurement point on the other hand didn't have a reasonable impact on latency. While ping messages had a median latency of 170 ms, small ones had a median latency of 325 ms and big ones of 327 ms. A two-sample t-test of ping and small as well as big messages confirmed a significant difference (p=0.0). The standard deviation of the latency was rather high ($\sigma_{ping} = 173ms; \sigma_{small} = 191ms; \sigma_{big} = 208ms$), which were caused by a couple of outliers above 1000ms. In fact, the 75 % quantile is only 192 ms for ping and 373/378 ms for small/big messages (Figure 6.5). The minimal achieved latency value is 77 ms, which shows what LTE is capable of under best conditions.

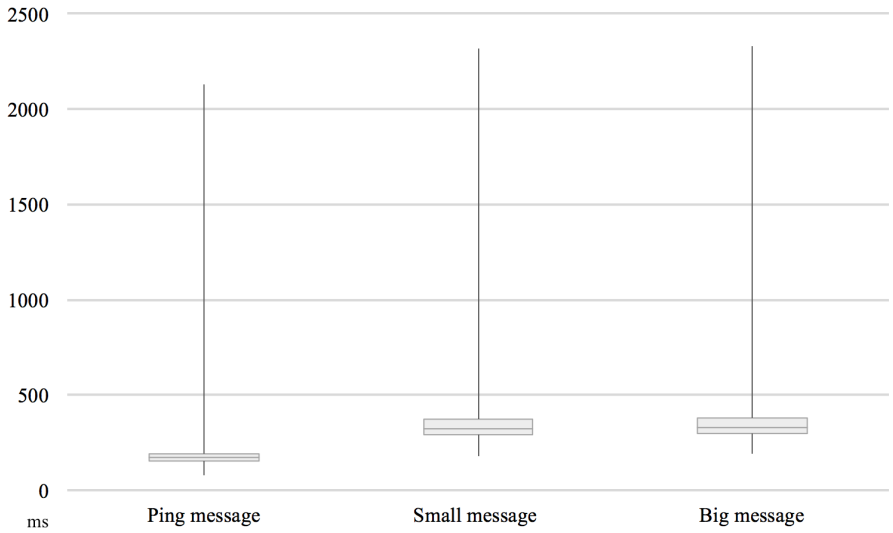

Figure 6.5.: Boxplot of LTE Latencies for different message sizes.

Table 6.1 depicts an overview of the measurements for the ping messages. The data of the ping messages was chosen for the table, as it was the message type that was transferred in the majority of LoRaWAN measurements. The median and median absolute deviation (MAD) was chosen in favour of the average and standard deviation values, as it is better suited to cope with outliers and allows the

better comparison of the results [98]. As shown, the highest median value is 197 ms for measurement point M07, while all other latency medians are in the range of 153 and 175 ms (Mean: 170 ms). Also the median absolute deviation is relatively stable around 11 to 24 ms (Mean: 15ms).

Measurement Point	PDR	Latency (ms)	
		Median	MAD
M01	100%	173	12
M02	100%	153	11
M03	100%	168	10
M04	100%	155	24
M05	100%	170	13
M06	100%	173	19
M07	100%	197	11
M08	100%	164	18
M09	100%	171	13
M10	100%	175	22
M11	100%	170	11

Table 6.1.: Measuremenet values of LTE at the measurement points.

All in all, several QoS service classes from the previous developed QoS model can be covered. From the global classes, class G1 can be supported when a service level agreement with the mobile network carrier for prioritized network access is arranged. Then, a constant low roundtrip delay tolerance of less than 100 ms can be achieved. The reliability of more than 99 % packet delivery ratio is also possible, as the ratio in the evaluation was already at 100%. Class G2 can be covered almost entirely, especially the part where latency requirements are only below 10 seconds. Though in more than 98% of cases the roundtrip delay was below one second, some transmissions took up to two or even three seconds. Therefore, if it is very crucial for the application to stay below the 1 second delay bound, a service level agreement should with the provider should be established as well. Though class G3 can be covered as well, it might be too heavyweight and energy-intensive for the desired use cases. Once NB-IoT becomes available, this should be the preferred option instead of LTE. If preferred, also classes L1 (with SLA) to L5 could be covered, though it might be too heavyweight and costly there as well.

After having described the results of LTE as reference, now the LoRaWAN measurement data will be presented.

First, the results on the coverage will be introduced. Of the 11 measurement points, two were not covered by the LoRaWAN gateway and a connection could not be established. The first location that could not be covered was a room in a building in an Ex area, that had specially coated windows to prevent heavy RF impulses. The people working there gave the information that also their cellular connections of their mobile phones get affected from time to time. The second place where a connection was not possible was in a heavy concrete building, where the point of measurement was at the diagonal opposite to the building-side that faced the gateway location. A transmission with SF 7 was only possible at three of the remaining nine measurement points, so that the majority of the test was conducted with SF 12, where only a ping message could be sent out. Therefore all data will be reported for SF12, with exception for measurement point M01, where no transmission with SF12 was conducted. A detailed list of RSSI and SNR values and other measurement values is shown in table 6.2. It becomes clear, that especially M02, M08 and M10 had low signal qualities, but only M08 and M10 were affected by that.

For reliability measurement, the packet delivery ratio (PDR) is used. The ratio specifies the difference between the amount of messages that were sent out at the node vs. the messages that were received

Measurement Point	RSSI (dB)		SNR (dB)		PDR	PDR_{total}	Airtime added (s)
	Mean	SD	Mean	SD			Median
M01 (SF 7)	-104.75	1.92	4.48	0.97	72.7%	64.0%	0.06
M02	-110.64	1.87	-6.61	3.02	100.0%	78.6%	1.25
M03	-104.55	4.34	1.75	3.26	100.0%	55.0%	1.25
M04	-102.40	2.65	3.22	0.84	100.0%	100.0%	1.25
M05	-107.75	5.43	-3.08	3.35	92.3%	66.7%	1.25
M06	NA	NA	NA	NA	NA	NA	NA
M07	-99.92	3.25	3.68	1.45	100.0%	72.2%	1.25
M08	-112.22	1.40	-13.81	1.45	36.0%	29.0%	1.25
M09	NA	NA	NA	NA	NA	NA	NA
M10	-111.67	1.75	-8.11	2.79	85.7%	75.0%	1.25
M11	-93.73	1.29	6.38	0.80	84.6%	57.9%	1.25

Table 6.2.: Measuremenet values of LoRaWAN at the measurement points.

at the gateway. Additionally, the total PDR (PDR_{total}) is shown, that includes the messages that should have been sent, but that were redacted by the module due to "no free channel access", which means that the EU duty cycle regulations would have been violated if the message would have been sent. As shown, in only four of eleven cases, a PDR of 100% could be achieved, with the lowest value at M08, where only 36% of messages were successfully delivered. As M08 also had the lowest signal strength, this is not surprising. Over all measurement points, 78.7% of ping messages could be delivered. Results get worse when the total PDR is assessed. Of a total of 166 messages that should have been sent, 39 could not be sent due to duty cycle regulations ("no free channel" error of module). Of the remaining 127 messages that were sent out, 100 could be successfully delivered, leaving with a total PDR of 60.2%.

The latency in terms of airtime is rather stable across all measurement-places. For SF12, the airtime is 1.25 seconds and for SF7 60ms. It has to be noted again, that this is the airtime for a one byte message and a longer message would have increased the airtime further. Like this, only 28 messages can be sent per hour per node with SF12, as the duty cycle regulations only allow the channel occupation of 36 seconds per hour.

After assessing all measured parameters, LoRaWAN should only be used for applications that require service class L5 of the previous developed IIoT QoS model. Additionally, only those applications with low reliability and high delay tolerance should consider LoRaWAN, as the packet loss can increase further with a growing number of nodes in the network and latency increases with a bigger message size.

6.3 Summary and Discussion

Following the presentation of the results, the outcomes will be discussed and summarized.

In terms of coverage, the clear winner is LTE. The connection via it was successful in all locations, compared to LoRaWAN that only worked at nine out of eleven measurement points. From these nine, six were only reachable via SF12. However, this is still a huge achievement in comparison to other currently available connectivity technologies as Bluetooth or WiFi.

Also the reliability as 100% PDR of LTE is much better than the 78% PDR of LoRaWAN. This highlights the missing automatic repeat request (ARQ) feature of LoRaWAN, where the message is resent when no acknowledgement from the gateway is received in a given timeframe. Though ARQ would be helpful, it would also collide with the duty cycle regulations that LoRaWAN faces. To avoid also this issue, listen-

before-talk techniques could be used. This also highlights the need for upcoming technologies like Link Labs Symphony Link and Weightless-P, that provide exactly these features.

Speaking of latency, a combined up- and downlink transmission of LTE is about seven times faster than only the uplink of LoRaWAN with SF12 (170ms vs. 1250ms). This changes, when SF7 is used, where the airtime for the uplink to the gateway was only 60ms. However, SF7 was only possible at three locations, so that a usual use of SF12 is likely.

While LTE can therefore be used for almost all QoS classes (G1 and L1 with SLA), LoRaWAN is only capable to serve the portions of service class L5 that have low reliability and high delay tolerance requirements. It might be used for sensor metering applications, where only very infrequent messages have to be sent out and where the loss of one or more messages doesn't affect the system health. It is less suited for scenarios where a reliable delivery is required in most of the cases and when the system depends on user interaction. For such scenarios it should at least be clear when a message could not be delivered, but this is currently not possible with the LoRaWAN protocol.

Compared to previous study covering LoRa and LoRaWAN, the experimental evaluation extends the current research on LPWAN and connectivity technologies for IIoT.

Augustin et al. [86] did also an experimental test in an urban environment, but only assessed the LoRa physical layer without the LoRaWAN MAC protocol. Accordingly, they were not bound to duty cycle regulations and sent out 10000 messages during their test period. Also they reported much wider coverage than compared to the results of this study, with nearly 100% PDR until a distance of 1.4km with SF12. However their gateway was positioned in a house at the steep side of a hill (thus an elevated position) and the nodes were located in the surrounding valley. This is not representative for an industrial environment and therefore the results are not 100% comparable.

Though it appears that Petäjäjärvi et al. [84] [83] did their also with LoRaWAN, their experimental setup is not representative for an industrial setting either. In [84], the node module was mounted on the top of a car or on a boat and no measurements inside of a building were conducted. Nevertheless in their test with a car and the gateway located 24m above ground, they experienced PDR of 88% in a range of up to 2km, which is comparable to the results in this study. In [83], indoor measurements were conducted. However the measurement with the largest distance to the gateway was at only around 390m. There, they experienced a PDR of 94.7%, which is comparable to the results here. Also their inability to transfer messages from the anechoic chamber is similar to the results from the Ex area and the large concrete building. Additionally they also report issues due to duty cycle regulations in both studies.

Similar to the results of Petri et al. [85], also this evaluation revealed a low packet delivery ratio with SF12. However, the gateway at [85] was placed at a higher point and the measurement points were at a larger distance.

The overall results of Kartakis et al. [87] on the other hand are comparable to the experiences made here. In 760m distance to the gateway, the PDR was 72% for SF12. However all tests were conducted outside, which leads to the assumption that indoor measurements would have been even worse.

To the knowledge of the author, this is the first study that evaluated LoRaWAN with a professional gateway in an industrial setting and in direct comparison to a cellular technology like LTE. All in all, the experimental evaluation revealed the weaknesses of LoRaWAN in comparison to an established and reliable, but also costly technology as LTE. Though LTE performs very well, the high energy consumption and increased operational expenses are probably a show-stopper for medium-dense deployments of IIoT devices on a large scale. LoRaWAN on the other hand might be sufficient for some use cases where high reliability and bigger message sizes are not needed. Even so, there are plenty of use cases where the performance of LoRaWAN will not be sufficient. Therefore, it is recommended to follow new promising technologies like Symphony Link, Weightless-P and especially NB IoT closely, to avoid bad surprises after a broad deployment of LoRaWAN.

7 Conclusion and Outlook

The aim of this research study was to shed light on the broad wireless connectivity landscape of Industrial IoT, by using a quality of service model based approach and developing an end-to-end framework for technology selection. To achieve that, the first step was to introduce the concept and the components of IoT in general and Industrial IoT specifically. An overview of potential IIoT scenarios, of wireless networking basics and of the current and upcoming IIoT connectivity landscape was given. A thorough overview about related work on constraints on quality of service in Industrial IoT environments and about previous QoS models were presented. Also the shortcomings of these models were discussed. Next on, an IIoT QoS model was developed, that consists of ten service classes, which were defined and explained. Alongside, a QoS taxonomy was created, that allows the easy identification of the right service class for a use case. After that, the most suitable technology for each service class had to be selected. To achieve that, the fitting connectivity options for each class were preselected and a scoring model was developed that allows to pick the best technology for a given use case. The scoring model optionally allows to include preferences, such as whether a wireless technology should be provider operated (e.g. by a cellular service provider) or not. Finally, an experimental evaluation of the connectivity technologies LTE and LoRaWAN was carried out in a real-world industrial setting. The QoS parameters coverage, reliability and supported message size were measured at eleven points on the production site of a large science and technology company. LTE achieved 100% coverage and proved to be an energy intensive and costly, but also reliable and universal connectivity option that could be used to connect applications across several QoS classes. On the other hand, LoRaWAN was only able to successfully connect in nine out of eleven measurement points and showed several shortcomings in terms of reliability, allowed message size and permitted duty cycle, that limited it's use only to applications in the QoS class with the lowest message size and criticality.

Although this research study was carried out with scientific rigor in mind, it is not without limitations. Though the assignment of QoS parameters to use cases, that formed the basis of the developed QoS model, were reviewed by experts in the field of industrial IT and IoT, an evaluation with a broader audience would be helpful. This could be done by surveying a number of domain experts in the fields of the respective use cases, to gather their insights as well and thereby enhancing the generalizability of the study. The same holds true for the parameter assignments of the scoring model, which would also benefit from the input of a wider audience. Regarding the experimental technology evaluation, a repetition with upcoming promising LPWAN technologies as Link Labs Symphony Link and Weightless-P would be interesting. Also 802.11ah and NB IoT should be included here, once they become available in the future. However, it should be made sure that the setting in which the evaluation takes place is representative for Industrial IoT, to avoid distorted results. Finally, also simulation studies could be helpful, to estimate the network behaviour and the compliance to QoS classes under load. The simulation models could be based on real-world measurements in the field, similar to the work of Bor et al. [99].

Despite the limitations described above, to the knowledge of the author this is the first study that provided a complete end-to-end view of connecting the Industrial Internet of Things. Thereby the contribution to the literature is threefold.

Following calls from Gubbi et al. [7], Rawat et al. [11] and Ray et al. [12], the developed QoS model for IoT and Industrial IoT in particular allows the classification of heterogeneous network requirements. Also the demand from Atzori et al. [6] for more research on traffic characterization in IoT is covered here and was even extended by the focus on IIoT.

Second, the limited research on network selection by Bari and Leung [81] and Song and Jamalipour [80] is broadened by the development of an IIoT specific scoring model based network selection process.

Third, the QoS assessment of the current trend-technology LoRaWAN in an real-world industrial setting was the first of its kind, to the knowledge of the author. It adds to the body of literature about

LPWAN performance, similar to the studies of Augustin et al. [86], Petäjäjärvi et al. [84] and Kartakis et al. [87], and extends them by using LTE as reference.

The developed QoS and scoring models, as well as the results of the experimental evaluation, can be used by research scholars and practitioners alike. For the research community, they add to the body of literature about IoT QoS and network selection, as well as to the research about real-world evaluations of LPWAN technologies, as described above. For practitioners, the QoS taxonomy, together with the scoring model, can be a great starting point for the network planning of Industrial IoT solutions. Also the insights of the LoRaWAN and LTE performance evaluation allow to make more informed decisions for the planning of IIoT networks.

As already suggested, the IIoT connectivity landscape is far from being complete. With technologies like software defined radios (SDR) in the pipeline, that allow the flexible reconfiguration of the used wireless channel through the software implementation of traditional hardware radio components, ample of wireless networking opportunities for Industrial IoT arise [100]. One of them is the possibility to build cognitive radios, that continuously sense their environment (e.g. the occupied spectrum), analyze and reason about it and finally adapt to it (e.g. set the used spectrum to a current spectrum hole). These intelligent radios, would allow to greatly improve the connectivity efficiency [100]. Also the upcoming 5G networks rely heavily on software defined networking and potentially bring other options, such as very low-power millimeter wave technologies on the table, that are even more battery friendly than NB IoT [5]. One can safely assume, that the landscape of IIoT connectivity option stays interesting. Therefore a universal QoS and scoring model based approach as the one followed here, where new technologies can be easily integrated, is even more future-proof and stays constantly relevant.

Bibliography

[1] IETF, "RFC 4594 - Configuration Guidelines for DiffServ Service Classes," Tech. Rep., 2006.

[2] R. Duan, X. Chen, and T. Xing, "A QoS architecture for IOT," *Proceedings - 2011 IEEE International Conferences on Internet of Things and Cyber, Physical and Social Computing, iThings/CPSCom 2011*, pp. 717–720, 2011.

[3] S. Haller, S. Karnouskos, and C. Schroth, "The Internet of things in an enterprise context," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 5468, pp. 14–28, 2009.

[4] J. Rivera and R. van der Meulen, "Gartner Says the Internet of Things Will Transform the Data Center," 2014. [Online]. Available: http://www.gartner.com/newsroom/id/2684616[Accessed: 10.02.2017]

[5] M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, and L. Ladid, "Internet of Things in the 5G Era: Enablers, Architecture, and Business Models," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 510–527, 2016.

[6] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[7] J. Gubbi, R. Buyya, and S. Marusic, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Future Generation Computer Systems*, no. 1, pp. 1–19, 2013.

[8] L. D. Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[9] S. Andreev, O. Galinina, A. Pyattaev, M. Gerasimenko, T. Tirronen, J. Torsner, J. Sachs, M. Dohler, and Y. Koucheryavy, "Understanding the IoT connectivity landscape: a contemporary M2M radio technology roadmap," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 32–40, sep 2015.

[10] R. Sanchez-Iborra and M. D. Cano, "State of the art in LP-WAN solutions for industrial IoT services," *Sensors (Switzerland)*, vol. 16, no. 5, 2016.

[11] P. Rawat, K. D. Singh, H. Chaouchi, and J. M. Bonnin, "Wireless sensor networks: A survey on recent developments and potential synergies," *Journal of Supercomputing*, vol. 68, no. 1, pp. 1–48, 2014.

[12] A. Ray, J. Akerberg, M. Bjorkman, and M. Gidlund, "Future research challenges of secure heterogeneous industrial communication networks," in *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, sep 2016, pp. 1–6.

[13] ITU, "Y2060 - Overview of the Internet of things," 2012.

[14] R. Drath and A. Horch, "Industrie 4.0: Hit or Hype? [Industry Forum]," *IEEE Industrial Electronics Magazine*, vol. 8, no. 2, pp. 56–58, jun 2014.

[15] P. Daugherty, P. Banerjee, W. Negm, and A. E. Alter, "Driving Unconventional Growth through the Industrial Internet of Things," *Accenture*, 2014.

[16] International Trade Centre, "Trade Map Germany 2015," 2015.

[17] J. Akerberg, M. Gidlund, and M. Bjorkman, "Future research challenges in wireless sensor and actuator networks targeting industrial automation," in *2011 9th IEEE International Conference on Industrial Informatics*. IEEE, jul 2011, pp. 410–415.

[18] K. Pister, P. Thubert, and T. Phinney, "RFC 5673 - Industrial Routing Requirements in Low Power and Lossy Networks," Tech. Rep., 2009.

[19] M. E. Porter and J. E. Heppelmann, "How Smart, Connected Products Are Transforming Competition," *Harvard Business Review*, 2014.

[20] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[21] F. Wortmann and K. Flüchter, "Internet of Things: Technology and Value Added," *Business and Information Systems Engineering*, vol. 57, no. 3, pp. 221–224, 2015.

[22] A. A. Kumar S., K. Ovsthus, and L. M. Kristensen., "An industrial perspective on wireless sensor networks-a survey of requirements, protocols, and challenges," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1391–1412, 2014.

[23] I. F. Akyildiz and M. C. Vuran, *Wireless sensor networks*. John Wiley & Sons, 2010, vol. 4.

[24] G. Reinhard, V. Jesper, and S. Stefan, "Industry 4.0: Building the digital enterprise," *2016 Global Industry 4.0 Survey*, pp. 1–39, 2016. [Online]. Available: www.pwc.com/industry40[Accessed: 17.12.2016]

[25] General Electric, "THE WORLD'S FIRST DIGITAL WIND FARM," 2016. [Online]. Available: https://www.gerenewableenergy.com/wind-energy/technology/digital-wind-farm.html[Accessed:17.12.2016]

[26] S. Mukherjee, "Rolls-Royce connecting jet-engine data to Microsoft's intelligent cloud," 2016. [Online]. Available: http://techseen.com/2016/04/26/rolls-royce-connecting-jet-engine-data-microsofts-intelligent-cloud/[Accessed:17.12.2016]

[27] D. Knight, "Welcome to the commercial Internet of Things," 2015. [Online]. Available: http://www.computerworld.com/article/2991498/internet-of-things/welcome-to-the-commercial-internet-of-things.html[Accessed:18.12.2016]

[28] K. S. Low, W. Nu, N. Win, M. J. Er, and W. N. N. Win, "Wireless Sensor Networks for Industrial Environments," *International Conference on Computational Intelligence for Modelling Control and Automation and International Conference on Intelligent Agents Web Technologies and Internet Commerce CIMCAIAWTIC06*, vol. 2, pp. 271–276, 2005.

[29] C. H. Potter, G. P. Hancke, and B. J. Silva, "Machine-to-Machine: Possible applications in industrial networks," in *2013 IEEE International Conference on Industrial Technology (ICIT)*. IEEE, feb 2013, pp. 1321–1326.

[30] M. Bal, "Industrial applications of collaborative Wireless Sensor Networks: A survey," *2014 IEEE 23rd International Symposium on Industrial Electronics (ISIE)*, pp. 1463–1468, 2014.

[31] T. Arampatzis, J. Lygeros, and S. Manesis, "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks," *Proceedings of the 2005 IEEE International Symposium on, Mediterrean Conference on Control and Automation Intelligent Control, 2005.*, pp. 719–724, 2005.

[32] V. C. Gungor, G. P. Hancke, and S. Member, "Industrial Wireless Sensor Networks : Challenges , Design Principles , and Technical Approaches," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 10, pp. 4258–4265, 2009.

[33] L. Hou and N. W. Bergmann, "System requirements for industrial wireless sensor networks," *Emerging Technologies and Factory Automation (ETFA), 2010 IEEE Conference on*, pp. 1–8, 2010.

[34] A. Willig, K. Matheus, and A. Wolisz, "Wireless Technology in Industrial Networks," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1130–1151, 2005.

[35] S. Wang, J. Wan, D. Li, and C. Zhang, "Implementing Smart Factory of Industrie 4.0: An Outlook," *International Journal of Distributed Sensor Networks*, vol. 2016, pp. 1–10, 2016.

[36] U. Doe, "Industrial wireless technology for the 21st century," *Industrial Wireless Workshop*, p. 50, 2002.

[37] G. Zhao, "Wireless sensor networks for industrial process monitoring and control: a survey," *Network Protocols and Algorithms*, vol. 3, no. 1, pp. 46–63, 2011.

[38] A. Flammini, P. Ferrari, D. Marioli, E. Sisinni, and A. Taroni, "Wired and wireless sensor networks for industrial applications," *Microelectronics Journal*, vol. 40, no. 9, pp. 1322–1336, 2009.

[39] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach (6th Edition)*, 6th ed. Pearson, 2012.

[40] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low Power Wide Area Networks: An Overview," *IEEE Communications Surveys and Tutorials*, pp. 1–15, jun 2017.

[41] X. Xiong, K. Zheng, R. Xu, W. Xiang, and P. Chatzimisios, "Low power wide area machine-to-machine networks: Key techniques and prototype," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 64–71, 2015.

[42] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2481–2501, 2014.

[43] P. Radmand, A. Talevski, S. Petersen, and S. Carlsen, "Taxonomy of wireless sensor network cyber security attacks in the oil and gas industries," *Proceedings - IEEE International Conference on Advanced Information Networking and Applications, AINA*, pp. 949–957, 2010.

[44] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey," *Security in Distributed, Grid, Mobile, and Pervasive Computing*, pp. 367–410, 2007.

[45] ETSI, "ETSI EN 300 220-2 V3.1.1 - Short Range Devices (SRD) operating in the frequency range 25 MHz to 1 000 MHz; Part 2: Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU for non specific radio equipment," Tech. Rep., 2016.

[46] ——, "ETSI EN 300 220-1 V3.1.1 - Short Range Devices (SRD) operating in the frequency range 25 MHz to 1 000 MHz; Part 1: Technical characteristics and methods of measurement," Tech. Rep., 2016.

[47] ——, "EN 300 328 - V2.1.1 - Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU," Tech. Rep., 2016.

[48] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia, and T. Watteyne, "Understanding the limits of LoRaWAN," pp. 8–12, jul 2016.

[49] Bluetooth SIG, "BLUETOOTH SPECIFICATION Version 4.2 / Vol 0 - 7," Tech. Rep., 2014.

[50] P. Neumann, "Communication in industrial automation-What is going on?" *Control Engineering Practice*, vol. 15, no. 11, pp. 1332–1347, 2007.

[51] S. Petersen and S. Carlsen, "WirelessHART versus ISA100.11a: The format war hits the factory floor," *IEEE Industrial Electronics Magazine*, vol. 5, no. 4, pp. 23–34, 2011.

[52] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[53] E. Perahia and R. Stacey, *Next Generation Wireless LANS: 802.11 n and 802.11 ac*. Cambridge university press, 2013.

[54] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, "Long-Range Communications in Unlicensed Bands: the Rising Stars in the IoT and Smart City Scenarios," *IEEE Wireless Communications*, no. October, pp. 1–7, 2016.

[55] K. E. Nolan, W. Guibene, and M. Y. Kelly, "An evaluation of low power wide area network technologies for the Internet of Things," in *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, sep 2016, pp. 439–444.

[56] Link Labs, "Symphony Link vs. LoRaWAN - A Guide for Engineers and Decision Makers," Tech. Rep., 2016. [Online]. Available: https://www.link-labs.com/low-power-wide-area-network-lpwa/[Accessed:05.01.2017]

[57] Weightless SIG, "LPWAN Technology Decisions: 17 critical features," Tech. Rep., 2016.

[58] WAVIoT, "NB-Fi vs Competitors - COMPARISON OF LPWAN TECHNOLOGIES," 2016. [Online]. Available: http://dgmatics.com/technology/waviot-lpwan-technology-comparison[Accessed:28.12.2016]

[59] A. Rico-Alvariño, M. Vajapeyam, H. Xu, X. Wang, Y. Blankenship, J. Bergman, T. Tirronen, and E. Yavuz, "An overview of 3GPP enhancements on machine to machine communications," *IEEE Communications Magazine*, vol. 54, no. 6, pp. 14–21, 2016.

[60] Y.-P. E. Wang, X. Lin, A. Adhikary, A. Grövlen, Y. Sui, Y. Blankenship, J. Bergman, and H. S. Razaghi, "A Primer on 3GPP Narrowband Internet of Things (NB-IoT)," *arXiv preprint arXiv:1606.04171*, 2016.

[61] ITU, "E800 - Definition of terms related to quality of service," *Telecommunication Standardization Sector of Itu*, pp. 1–30, 2008.

[62] T. Szigeti, C. Hattingh, R. Barton, and K. Briley, *End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks*, 2nd ed. Indianapolis: Cisco Press, 2013.

[63] D. Chen and P. K. Varshney, "QoS Support in Wireless Sensor Networks: A Survey," *International Conference on Wireless Networks, (ICWN '04), Las Vegas*, vol. 13244, pp. 227–233, 2004.

[64] J. Burkhard Schmitt, *Heterogeneous Network Quality of Service Systems*. Boston: Kluwer Academic Publishers, 2001.

[65] D. Christin, A. Reinhardt, P. S. Mogre, and R. Steinmetz, "Wireless Sensor Networks and the Internet of Things : Selected Challenges," *Structural Health Monitoring*, vol. 5970, pp. 31–33, 2009.

[66] S. Tilak, N. B. Abu-Ghazaleh, and W. Heinzelman, “A taxonomy of wireless micro-sensor network models,” *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 6, no. 2, pp. 28–36, 2002.

[67] J. Balen, D. Zagar, and G. Martinovic, “Quality of Service in Wireless Sensor Networks : A Survey and Related Patents,” pp. 188–202, 2011.

[68] B. Bhuyan, “Quality of Service (QoS) Provisions in Wireless Sensor Networks and Related Challenges,” *Wireless Sensor Network*, vol. 02, no. 11, pp. 861–868, 2010.

[69] F. Xia, “QoS Challenges and Opportunities in Wireless Sensor/Actuator Networks,” *Sensors*, vol. 8, no. 2, pp. 1099–1110, 2008.

[70] X. Li, D. Li, J. Wan, and A. V. Vasilakos, “A review of industrial wireless networks in the context of Industry 4.0,” *Wireless Networks*, 2015.

[71] P. Radmand, A. Talevski, S. Petersen, and S. Carlsen, “Comparison of industrial WSN standards,” *4th IEEE International Conference on Digital Ecosystems and Technologies - Conference Proceedings of IEEE-DEST 2010, DEST 2010*, pp. 632–637, 2010.

[72] L. M. Borges, F. J. Velez, and A. S. Lebres, “Survey on the Characterization and Classification of Wireless Sensor Network Applications,” *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1860–1890, 2014.

[73] J. R. Moyne and D. M. Tilbury, “The Emergence of Industrial Control Networks for Manufacturing Control, Diagnostics, and Safety Data,” *Proceedings of the IEEE*, vol. 95, no. 1, pp. 29–47, 2007.

[74] ITU, “E802 - Framework and methodologies for the determination and application of QoS parameters,” 2007.

[75] Y. Wang, X. Liu, and J. Yin, “Requirements of Quality of Service in Wireless Sensor Network,” *International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06)*, 2006.

[76] D. Yuan, S. S. Kanhere, and M. Hollick, “Instrumenting Wireless Sensor Networks - A survey on the metrics that matter,” *Pervasive and Mobile Computing*, 2016.

[77] J. Chen, M. Díaz, L. Llopis, B. Rubio, and J. M. Troya, “A survey on quality of service support in wireless sensor and actor networks: Requirements and challenges in the context of critical infrastructure protection,” *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1225–1239, 2011.

[78] K. Islam, W. Shen, S. Member, X. Wang, and S. Member, “Wireless sensor network reliability and security in factory automation: A survey,” *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews*, vol. 42, no. 6, pp. 1243–1256, 2012.

[79] M.-A. Nef, S. Karagiorgou, G. I. Stamoulis, and P. K. Kikiras, “Supporting Service Differentiation in Wireless Sensor Networks,” *2011 15th Panhellenic Conference on Informatics*, pp. 127–133, 2011.

[80] Q. Song and A. Jamalipour, “Network selection in an integrated wireless LAN and UMTS environment using mathematical modeling and computing techniques,” *IEEE Wireless Communications*, vol. 12, no. 3, pp. 42–48, 2005.

[81] F. Bari and V. C. M. Leung, “Automated network selection in a heterogeneous wireless network environment,” *IEEE Network*, vol. 21, no. 1, pp. 34–40, 2007.

[82] S. Zöller, *Events in logistics : efficient detection and transmission with wireless sensor network technology*, 1st ed. München: Verlag Dr. Hut, 2015.

[83] J. Petajajarvi, K. Mikhaylov, M. Hamalainen, and J. Iinatti, "Evaluation of LoRa LPWAN technology for remote health and wellbeing monitoring," *International Symposium on Medical Information and Communication Technology, ISMICT*, vol. 2016-June, 2016.

[84] J. Petäjäjärvi, K. Mikhaylov, A. Roivainen, T. Hänninen, and M. Pettissalo, "On the coverage of LPWANs: Range evaluation and channel attenuation model for LoRa technology," *2015 14th International Conference on ITS Telecommunications, ITST 2015*, pp. 55–59, 2016.

[85] T. Petri, M. Goessens, L. Nuaymi, A. Pelov, T. Petri, M. Goessens, L. Nuaymi, A. Pelov, and L. T. Measure, "Measurements , Performance and Analysis of LoRa FABIAN , a real-world implementation of LPWAN," *HAL*, 2016.

[86] A. Augustin, J. Yi, T. Clausen, and W. Townsley, "A Study of LoRa: Long Range & Low Power Networks for the Internet of Things," *Sensors*, vol. 16, no. 9, p. 1466, 2016.

[87] S. Kartakis, B. D. Choudhary, A. D. Gluhak, L. Lambrinos, and J. A. McCann, "Demystifying low-power wide-area communications for city IoT applications," in *Proceedings of the Tenth ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation, and Characterization - WiNTECH '16*. New York, New York, USA: ACM Press, 2016, pp. 2–8.

[88] ITU, "G1000 - Communications quality of service: A framework and definitions," 2001.

[89] W. Dong, Y. Liu, Y. He, and T. Zhu, "Measurement and Analysis on the Packet Delivery Performance in A Large Scale Sensor Network," *IEEE/ACM Transactions on Networking*, pp. 2679–2687, 2013.

[90] ITU, "Y.1541 - Network performance objectives for IP-based services," 2011.

[91] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, and A. Ghosh, "NB-IoT System for M2M Communication," no. Wd5g, pp. 2–6, 2016.

[92] F. Samie, L. Bauer, and J. Henkel, "IoT technologies for embedded computing," *Proceedings of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis - CODES '16*, no. October, pp. 1–10, 2016.

[93] M. Lauridsen, I. Kovács, P. E. Mogensen, M. Sørensen, and S. Holst, "Coverage and Capacity Analysis of LTE-M and NB-IoT in a Rural Area," *Vehicular Technology Conference, 2016 Ieee 84th*, 2016.

[94] J. S. Lee, Y. W. Su, and C. C. Shen, "A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi," *IECON Proceedings (Industrial Electronics Conference)*, pp. 46–51, 2007.

[95] Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. McCann, and K. Leung, "A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities," *IEEE Wireless Communications*, vol. 20, no. 6, pp. 91–98, 2013.

[96] IBM, "IBM® SPSS® Statistics, Version 23.0.0.2," 2016.

[97] Telekom, "Telekom Netzausbau." [Online]. Available: https://www.telekom.de/start/netzausbau[Accessed:15.02.2017]

[98] C. Leys, C. Ley, O. Klein, P. Bernard, and L. Licata, "Detecting outliers: Do not use standard deviation around the mean, use absolute deviation around the median," 2013.

[99] M. Bor, U. Roedig, T. Voigt, and J. M. Alonso, “Do LoRa Low-Power Wide-Area Networks Scale ?” in *The 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, 2016.

[100] P. Rawat, K. D. Singh, and J. M. Bonnin, “Cognitive Radio for {M2M} and Internet of Things: A survey,” *Computer Communications*, vol. 94, pp. –, 2016.

Appendix

A Appendix

A.1 IIoT Use Cases with QoS Parameter Assignments

		Discrete manufacturing					Process manufacturing
Use Case		Monitoring is the main driver of business value	See how the product is used	Deliver predictive maintenance	Improve the customer support	Pay-as-you-go pricing models	Include sensor devices in the packaging
Use Case ID		UCPd01	UCPd02	UCPd03	UCPd04	UCPd05	UCPd06
Reliability		very high/high/ medium	medium/low	medium	medium	high	high/medium/ low
Roundtrip Delay Tolerance		low/medium/high	high	high	medium	medium	medium
Message Size		Depends (Video feed?)	medium	medium	medium/large	small	small/medium
Global Coverage		x	x	x	x	x	x
Local Coverage	**Room**	x	x	x	x	x	x
	Building	x	x	x	x	x	x
	Area	x	x	x	x	x	x
Node mobility		y / n	y / n	y / n	y / n	y / n	y
Power Source		Battery/ Power supply	Battery/ Power supply	Battery/ Power supply	Battery/ Power supply	Battery/ Power supply	Battery
Interactivity		n	n	n	y	n	n
Sampling rate		Depends	Depends	1 m	10 s	Depends	Depends
QoS Support		y	n	n	n	y	n

Table A.1.: IIoT product use cases with assignment of QoS parameters

		Supply chain				Process and equipment monitoring
Use Case		Track the physical integrity and quality of the product	Ensure the integrity of the route	Track compliance to legal regulations	General global tracking of assets and transportation vehicles	Predictive maintenance
Use Case ID		UCPc01	UCPc02	UCPc03	UCPc04	UCPc05
Reliability		medium	medium	medium	low	medium
Roundtrip Delay Tolerance		medium	medium	medium	medium	high
Message Size		medium/small	small	medium/small	small	medium
Global Coverage		x	x	x	x	
Local Coverage	**Room**					x
	Building					x
	Area					x
Node mobility		y	y	y	y	y / n
Power Source		Battery	Battery/ Power supply	Battery/ Power supply	Battery/ Power supply	Battery/ Power supply
Interactivity		n	n	n	n	n
Sampling rate		Depends	1 m	10 s	10 s	10 m
QoS Support		n	n	n	n	n

Table A.2.: IIoT process use cases with assignment of QoS parameters (1/4)

		Monitoring of the environment				Reduce energy consumption		
Use Case		Indoor location	Outdoor location	Monitoring of emergency services (e.g. fire detection)	General monitoring and information gathering	Smart metering	Smart power control systems	Efficient use of utilities
Use Case ID		UCPc06	UCPc07	UCPc08	UCPc09	UCPc10	UCPc11	UCPc12
Reliability		depends	depends	very high	medium	medium	very high	medium
Roundtrip Delay Tolerance		low/high	low/high	very low	medium	high	very low	high
Message Size		depends (Video feed?)	depends (Video feed?)	small	small/medium/ large	small	small	small
Global Coverage								
Local Coverage	**Room**	x						
	Building	x					x	
	Area	x	x	x	x	x	x	x
Node mobility		y / n	y / n	n	y / n	n	n	n
Power Source		Battery/ Power supply	Battery	Power supply	Battery/ Power supply	Power supply	Power supply	Power supply
Interactivity		n	n	n	n	n	n	n
Sampling rate		depends	depends	0.5 s	5 m	1 s	1-10 ms	1 s
QoS Support		n	n	y	n	n	y	n

Table A.3.: IIoT process use cases with assignment of QoS parameters (2/4)

		Maintain statistics			Model of the plant operations	
Use Case		Production rates, quality parameters and volumes	Logistics coordination	Automation of the plant processes	Forecast expenditure and expansions	Get insights on the effects of other changes
Use Case ID		UCPc13	UCPc14	UCPc15	UCPc16	UCPc17
Reliability		low	low	low	low	low
Roundtrip Delay Tolerance		high	high	high	high	high
Message Size		small	small	small	small	small
Global Coverage						
Local Coverage	**Room**					
	Building					
	Area	x	x	x	x	x
Node mobility		n	y	n	n	n
Power Source		Battery/ Power supply	Battery/ Power supply	Battery/ Power supply	Battery/ Power supply	Battery/ Power supply
Interactivity		n	n	n	n	n
Sampling rate		1 m	1 m	1 m	5 m	5 m
QoS Support		n	n	n	n	n

Table A.4.: IIoT process use cases with assignment of QoS parameters (3/4)

		Control purposes				Inventory management	
Use Case		Closed loop control (process manufacturing)	Control by interlocks (start/stop) (process manufacturing)	Robots (discrete manufacturing)	Conveyor belts, machinery (discrete manufacturing)	Locality and quantity information of items	Localization and tracking of unfinished parts
Use Case ID		UCPc18	UCPc19	UCPc20	UCPc21	UCPc22	UCPc23
Reliability		very high	very high	very high	very high	medium	medium
Roundtrip Delay Tolerance		very low	very low	very low	very low	high	high
Message Size		small	small	depends (Video feed?)	small	small	small
Global Coverage							
Local Coverage	**Room**	x	x	x	x		
	Building	x		x			
	Area	x		x		x	x
Node mobility		n	n	y/n	n	y	y
Power Source		power supply	power supply	power supply	power supply	battery	battery
Interactivity		y	y	y	y	n	n
Sampling rate		1 - 10ms	1 - 10ms	1 - 10ms	1 - 10ms	1 m	1 m
QoS Support		y	y	y	y	n	n

Table A.5.: IIoT process use cases with assignment of QoS parameters (4/4)