A Contribution to Industrial and Educational IoT

Ein Beitrag zum Einsatz von IoT-Technologien in Industrie und Bildung

Vom Fachbereich Elektrotechnik und Informationstechnik
der Rheinland-Pfälzische Technische Universität Kaiserslautern-Landau
zur Verleihung des akademischen Grades
Doktor der Ingenieurwissenschaften (Dr.-Ing.)
genehmigte Dissertation

von

Frederik Lauer

geboren in Neunkirchen (Saar)

Tag der Einreichung:	20.02.2024
Tag der mündlichen Prüfung:	28.05.2024
Dekan des Fachbereichs:	Prof. Dr.-Ing. Daniel Görges
Vorsitzender der Prüfungskommission:	Prof. Dr.-Ing. Daniel Görges
1. Berichterstatter:	Prof. Dr.-Ing. Norbert Wehn
2. Berichterstatter:	Prof. Dr. Jochen Kuhn (LMU München)

DE-386

Eidesstattliche Erklärung

Ich erkläre an Eides statt,

dass ich die vorliegende Dissertation selbst angefertigt habe und alle von mir benutzten Hilfsmittel angegeben habe,

dass ich die Dissertation oder Teile hiervon noch nicht als Prüfungsarbeit für eine staatliche oder wissenschaftliche Prüfung eingereicht habe, und

dass ich nicht die gleiche oder eine andere Abhandlung bei einem anderen Fachbereich oder einer anderen Universität als Dissertation eingereicht habe.

Korntal-Münchingen, 26. Januar 2024

Frederik Lauer

Abstract

The constantly expanding Internet of Things (IoT) poses significant challenges for the devices and systems involved. When transporting the enormous amounts of data that are collected every day by IoT devices, the security of the data transmission is a crucial factor, especially in areas like the Industrial IoT. While state-of-the-art security algorithms can achieve a high level of trust, the necessary underlying computations pose a major challenge for small embedded systems with very restricted energy budgets like small sensor nodes. The common approach of optimizing individual computational steps using special cryptographic hardware accelerators, however, still does not fully exploit the available potential in terms of energy efficiency and computation time. Therefore, in addition to the impact of the utilization of hardware accelerators, a holistic analysis approach is presented and evaluated in this thesis. The resulting optimized IoT system demonstrates that even with a small amount of energy, which can be collected, e.g., by an energy harvesting module, a wireless data transmission that meets today's security requirements can be realized.

In addition to the transmission of data, capturing the environment is an essential element of the IoT. New challenging multi-sensor systems are needed to answer many research questions, especially in the emerging field of Educational IoT and the associated digitalization of learning environments. In cooperation with colleagues from didactics research, a learning environment for augmented electrical experiments and a learning platform for the field of photometry were developed. This work focuses on the technical implementation, the required sensor systems, and the evaluation of the learning platforms.

The contributions of this work offer a clear added value for the related research projects and future research projects due to their project-oriented implementation. Furthermore, the modular and generic structure of the projects offers elementary adaptability to other domains and systems.

Acknowledgments

I am very grateful to all my colleagues, friends, and family who have supported me on my way to this thesis.

Especially I would like to thank my doctoral adviser Prof. Dr.-Ing. Norbert Wehn for the opportunity to work in the challenging field of data security for ultra-low power devices as well as in the emerging topic of Educational IoT with a focus on multi-sensor systems. Further more, I would like to thank for the continuous support, the opportunities to enhance my skills in various areas, and the numerous insightful discussions.

Many thanks to Prof. Dr. Jochen Kuhn for the multiple collaborative research projects and the beneficial conversations as well as for his interest in my thesis and for serving on my thesis committee.

I am very grateful for my friends and colleagues I had the chance to work with in the Microelectronic Systems Design Research Group: Dipl.-Inf. Claus Kestel, Dipl.-Ing. Matthias Herrmann, Dipl.-Ing. Sebastian Wille, Dipl.-Math. Uwe Wasenmüller, Dr.-Ing. Bilal Hammoud, Dr.-Ing. Christian Weis, Dr.-Ing. Deepak M. Mathew Dr.-Ing. Javier Alejandro Varela, Prof. Dr.-Ing. Matthias Jung, Dr.-Ing. Stefan Weithoffer, Dr.-Ing. Vladimir Rybalkin, M.Eng. Carl Rheinländer, M.Eng. Lucas Johannsen, M.Sc. André Lucas Chinazzo, M.Sc. Chirag Sudarshan, M.Sc. Jan Lappas, M.Sc. Johannes Feldmann, M.Sc. Jonas Ney, M.Sc. Kira Kraft, M.Sc. Lukas Steiner, M.Sc. Maximilian Schöffel, M.Sc. Menbere Tekleyohannes, M.Sc. Mohammad Hassani Sadi, M.Sc. Mohammadreza Esmaeilpour Quchani, M.Sc. Muhammad Mohsin Ghaffar, and M.Sc. Oliver Griebel.

Many thanks to our secretary Martina Jahn for her continuous support on all non-technical issues as well as Dipl.-Ing. (FH) Hans-Peter Goldhammer, Dipl.-Ing. (FH) Roland Volk, and Andreas Christmann, for their helpful technical and comprehensive support.

I would especially like to thank M.Eng. Carl Rheinländer and Dipl.-Inf. Claus Kestel, whose work laid the foundation for my research into data security in ultra-low power devices.

Also, I want to thank my colleagues M. Ed. Lena Geuer and Dr. rer. nat. Sebastian Kapp for their productive and fruitful collaboration in the area of smart learning platforms.

Special thanks go to my parents, my sister, and my girlfriend M.Sc. Michèle Latz for their continuous encouragement.

Thank you to all of you for making this achievement possible.

Contents

Chapter 1

Introduction

1.1 Motivation and Challenges

The amount of data worldwide was estimated at 33 billion terabytes in 2018 and is expected to grow further to approximately 175 billion terabytes in 2025 [1]. This data no longer consists only of information purposefully published by people, such as photos, news, blogs, and communication; rather, servers collect, process, and store the data in a fully automated way. In addition, more and more devices are being made "smart" by using network interfaces to become part of a local network or the internet where data is exchanged, stored, and used. This concept of networked devices and objects is called the *Internet of Things* (IoT). The term IoT was first used in 1999 by the British technology pioneer Kevin Ashton in connection with a multi-company *Radio-Frequency Identification* (RFID) infrastructure. However, the term gained immense popularity only after the significant progress in the fields of microelectronics and communication systems, which enabled much more powerful microcontrollers, sensors, and network interfaces at relatively low prices. Small gadgets up to complex industrial plants are equipped with sensors and actuators to create additional value. How exactly the obtained data is used depends very much on the individual application. In a smart home, for example, environmental sensors can be used for more integrated heating and ventilation control and ensure a better indoor climate while saving energy at the same time. In the industrial context, whereas, real-time sensor data from the process can be used to analyze, synchronize, and monitor processes, resulting in more efficient and safer operations. Due to a large number of possible areas of application, there are several variations of the term IoT. In the private sector, for example, it is often referred to as Consumer IoT, and in the industry context as Industrial IoT or "Industrie 4.0". Variations such as Educational IoT or *Internet of Medical Things* (IoMT) thus stand for networked devices in the respective area. A challenge that spans all areas of the IoT is data management. It includes the acquisition of data, the transmission of data, as well as the evaluation and use of data, whereby the requirements strongly depend on the application area. The contributions of this work are focused on two of these areas: data acquisition and data transmission.

Data Acquisition

Capturing information about the physical environment of devices is an essential part of the IoT and is key in the era of machine learning. It allows the analysis of the surroundings and, thus, the appropriate reactions. The selection of sensors nowadays available is almost incomprehensible. Especially the enormous progress in *Micro-Electro-Mechanical Systems* (MEMS) technology enables even more precise, cost-effective, energy-efficient, and novel sensors. As a result, new fields of application are constantly emerging, and new opportunities are being created. However, not all parameters can be measured directly with the available sensors. Often, information from several sensors must be combined to obtain the desired measurement results. Furthermore, a complex pre-processing of the sensor data is sometimes necessary before actually valuable data is available.

In the emerging field of Educational IoT, multisensor systems can offer many possible educational applications and are also an essential prerequisite for addressing many research questions in this context. Currently, IoT-technology is finding its way into learning environments. These so-called *smart* learning environments are an essential contribution to modern learning, learning analytics, and learning research [2, 3]. Today, education is confronted with increasing heterogeneity among learners. Hence, there is great demand for education that can be adapted to the knowledge status of the individual learners. Smart learning environments enable completely new, interactive, and collaborative learning methods. In addition, they allow precise analysis and validation of learning and learning success through data collection. This information can, in turn, be used to adapt and improve the learning environment or to customize it more precisely for specific individuals [4–6]. A smart learning environment can consist of a single app, a complex *Augmented Reality* (AR) experience, a full *Virtual Reality* (VR) environment, or other combinations of software and hardware solutions. Digital learning apps are known for their low entry barrier. Usually, only a smartphone, a tablet, or a PC is technically required to use the smart environment [7]. AR environments are characterized by their increased interactivity, allowing physical objects to merge seamlessly with the digital world. Concepts, such as magnetic fields [8], thermal flux [9], or the three-dimensional relationships between planets and stars in the solar system can be visualized and presented in an interactive and comprehensible way [10]. To use VR environments, however, special glasses are required, with the help of which the user can completely engage himself in a digital world. This enables very immersive learning experiences and insights into environments that are impossible in reality [11–14]. Additional hardware is often required, especially in the area of STEM experiments, to capture specific parameters in the experiment and use them in the learning environment. An example of such a system is the smart measurement platform for photometry and its digital twin, shown in Figure 1.1, which will be described in more detail in Section 3.3.

Intelligent learning platforms have many benefits, and the continuous development of technologies is opening up even more possibilities. Due to the ever-increasing

Figure 1.1: Example of a Smart Measurement Platform for Photometry in Education (SmaEPho) and its Digital Twin; More Information in Section 3.3

use of new technologies in everyday life, schools must also provide more training in the use of technology. But especially after the COVID-19 pandemic, where over 1.5 billion learners worldwide suddenly had to be taught at home, it became clear how important technology-supported learning platforms and their research are today [15]. This is also reflected in the increasing amount of research in the field of learning. Smart learning environments can be used to investigate a wide range of scientific questions. These relate, for example, to the analysis of learning methods, research into the learning process, or the influence of the technology itself.

A crucial factor for the quality and value of a smart learning platform is its usability. The tools have to be easy to set up and intuitive to use to achieve the greatest possible acceptance. This is a major challenge, especially in the field of AR-based learning environments. Since AR is primarily characterized by digital interaction with physical objects, the physical world must first be available, at least partially, in digital form. In this case, a necessary prerequisite is the physical position of the AR device within the environment. However, to exploit the full potential of an AR environment, as much information as possible from the physical world must be digitally available. Thus, for example, measured values in an experiment can be visualized directly at the point of occurrence. But, the sensor technology of such systems often poses a major challenge. A decisive factor is that the sensors must not negatively affect the

actual experiment or the person performing it. In addition, the system must be robust against external and unforeseen influences. Other challenges often include complex multi-sensor systems, budget constraints, latency and response times, privacy requirements, power supply, and data connectivity. Subsequently, these engineered smart learning platforms, which form an essential part of educational research, will themselves become part of necessary scientific questions in the field of electrical and information technology. They form a special use case for a multi-sensor device in the context of the IoT, whose concepts and insights can be generalized to many other applications.

The development and implementation of most learning platforms have been mainly driven by the fields of didactics and educational science. As a result, many platforms are specifically tailored to certain research questions and benefit from experience gained from previous experiments and studies in this area. From a technological point of view, very user-friendly off-the-shelf components such as Arduino-based microcontrollers, Raspberry PIs, and sensors on break-out boards are almost exclusively used. Although these components lead to quick results due to their widespread use in the *Do It Yourself* (DIY) sector, they always represent a compromise compared to customized solutions. The learning platforms presented in this thesis address this issue. Through close cooperation between the fields of didactics and electrical engineering, technically complex and specific embedded system solutions from the field of IoT are combined with the demanding requirements of modern learning environments to explore a wide range of didactic subjects. Concepts such as digital twins, advanced sensor networks, and special user interactions are thus finding their way into educational research.

Data Transmission

In addition to data acquisition, data transmission is also an essential key component of the IoT. Due to many different devices and environments, there is also a wide variety of requirements and prerequisites for data transmission. In the field of consumer IoT, the focus is often on flexibility and usability. The devices should be easy to set up and, if possible, use existing resources such as *Wireless Local Area Network* (WLAN) and power outlets. Smart lamps, for example, use the power supply of the actual device, since it is available anyway, and a wireless data connection via WLAN to avoid additional wiring. A smart room thermometer, in contrast, is often battery-powered because there is not necessarily a power outlet at the intended location. Therefore, an energy-efficient wireless protocol must be used to avoid draining the battery too quickly.

In the field of Industrial IoT, there is often a considerably more complex requirement profile. Today, many new devices are equipped with smart functions directly during development and can thus use the resources of the actual device. Especially in the industrial sector, machines, and devices are often in operation for many years or

even decades before a new generation replaces them. Solutions that retrofit devices with smart features are therefore extremely important. One use case, for example, is predictive maintenance [16], aiming to monitor machine parameters precisely and, as a result, perform more targeted maintenance. Since modifications to existing systems are usually complex and expensive, the retrofitted sensor devices must be as independent as possible to ensure quick installation. Systems that are not dependent on the power grid and have a wireless data connection are, therefore, often preferred. However, using a wireless data connection increases the already required high-security standard of systems in an industrial context even further [17]. On the one hand, the encryption of the data must be ensured. On the other hand, the communication partners must verify each other to guarantee that the data either sent or received has not been manipulated. This is extremely important, especially in critical infrastructure, as invalid data or data leaks can have serious consequences. But security is also playing an increasingly decisive role in other areas. Botnets for example, in which IoT devices are attacked on a large scale and misused for illegal purposes, emphasize the need for a certain level of security even further [18, 19].

There are several standardized procedures for securing data connections. Using approved and open standards, such as the *Transport Layer Security* (TLS) protocol, brings major advantages. First, the compatibility of the individual systems is increased by common interfaces and protocols. Second, the widespread use of a procedure ensures that potential attacks can be found and eliminated more quickly. Third, the disclosure of a procedure also significantly increases trust in a solution. The already mentioned TLS protocol is supported by all of the top 100 websites and is used by 97 of them as default[1]. For modern servers, PCs, and smartphones, the additional effort required for secure connection establishment and encryption is very low. However, for resource-constrained embedded systems, the complex cryptographic computations required for a TLS connection often pose a major challenge [20–24]. In addition, the increased communication overhead is required to establish the connection. Methods and solutions that make established cryptographic protocols feasible for resource-constrained embedded systems provide immense added value in the field of Industrial IoT. Furthermore, the results can also be used in other areas such as smart homes or the IoMT.

[1] https://transparencyreport.google.com/https/overview, accessed January 16, 2023

1.2 Contributions and Outline

Figure 1.2 provides an overview of the various challenges in the IoT that are relevant to this work and how they are interrelated. Although the broad scope of the IoT is extremely diverse, there are significant overlaps in terms of requirements and challenges for devices and solutions. This work is focussed on both the area of Educational IoT and the area of Industrial IoT. Yet many of the solutions and contributions can be applied to multiple sectors of the IoT.

The overall structure of the thesis is shown in Figure 1.3. Chapter 2 covers secure data transmission in the Industrial IoT with a focus on maximizing energy efficiency. For this purpose, the selected application domain of the Industrial IoT system is first explained in more detail in Section 2.1. The corresponding design space exploration follows in Section 2.2 with further related work. The overall concept and structure of the Industrial IoT network system are detailed in Section 2.3. Section 2.4 presents the evaluation of the general feasibility of the setup as well as insights into the limited use of isolated optimization of cryptographic operations with *Cryptographic Hardware Accelerators* (CHAs). Section 2.5 provides a more complete overview by applying a holistic analysis approach and identifies limiting factors as well as related optimizations. Finally, Section 2.6 evaluates the system for being powered by a *Thermoelectric Generator* (TEG) and indicates the resulting challenges. Chapter 3 addresses data acquisition with complex multi-sensor systems in the field of Educational IoT. Therefore Section 3.1 gives a brief overview of learning theory background. Section 3.2 covers the sensor technologies of a smart learning environment for electrical experiments that have also been optimized for use with AR glasses. Section 3.3, in turn, focuses on the sensor technology of a smart learning environment for photometric experiments, which relies on the connection with a digital twin. Chapter 5 summarizes the whole subject of the thesis and gives an outlook on possible future research questions.

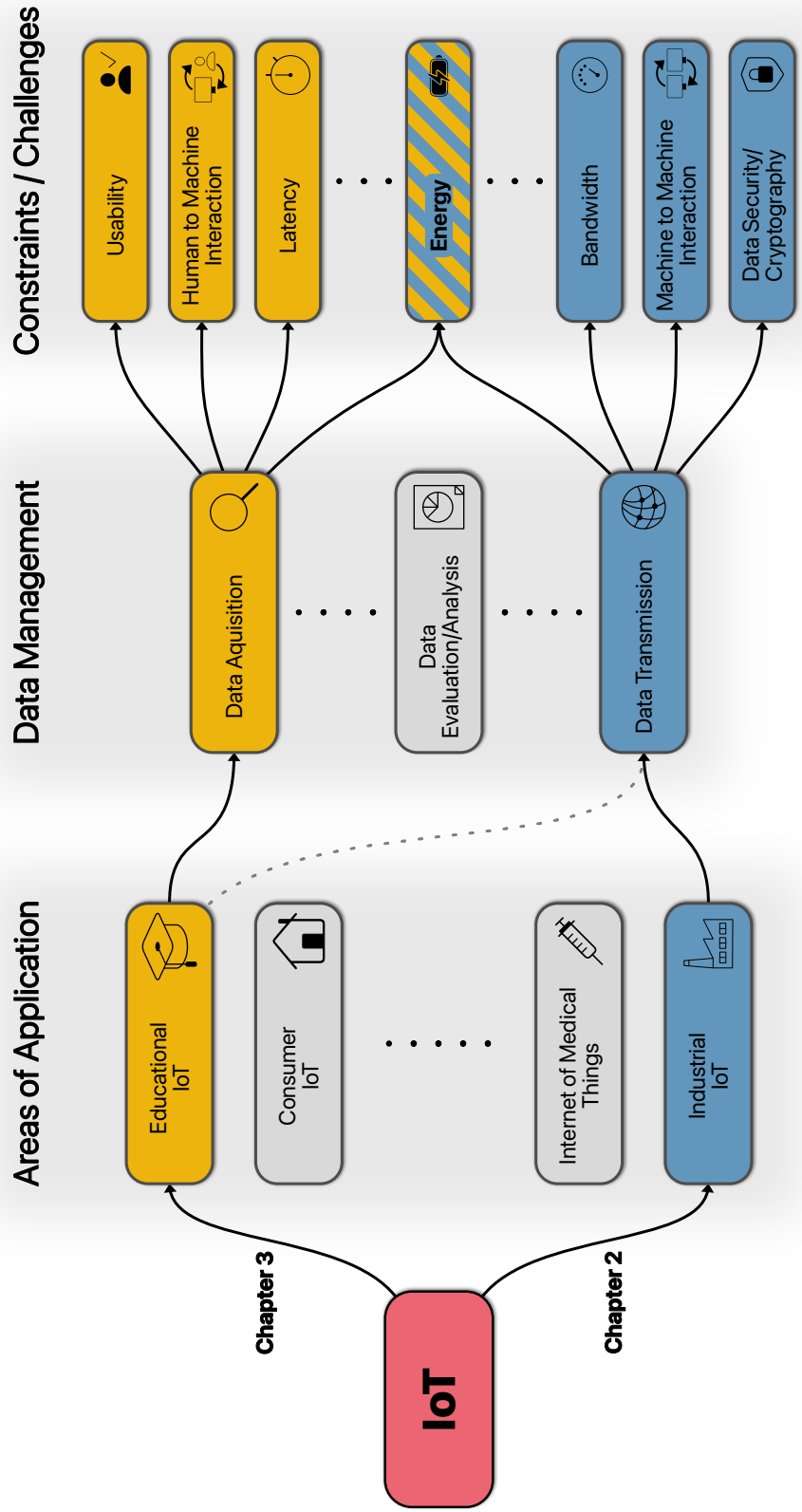

Figure 1.2: An Overview of the Interconnection of the different Areas and Challenges of the IoT considered in this Thesis

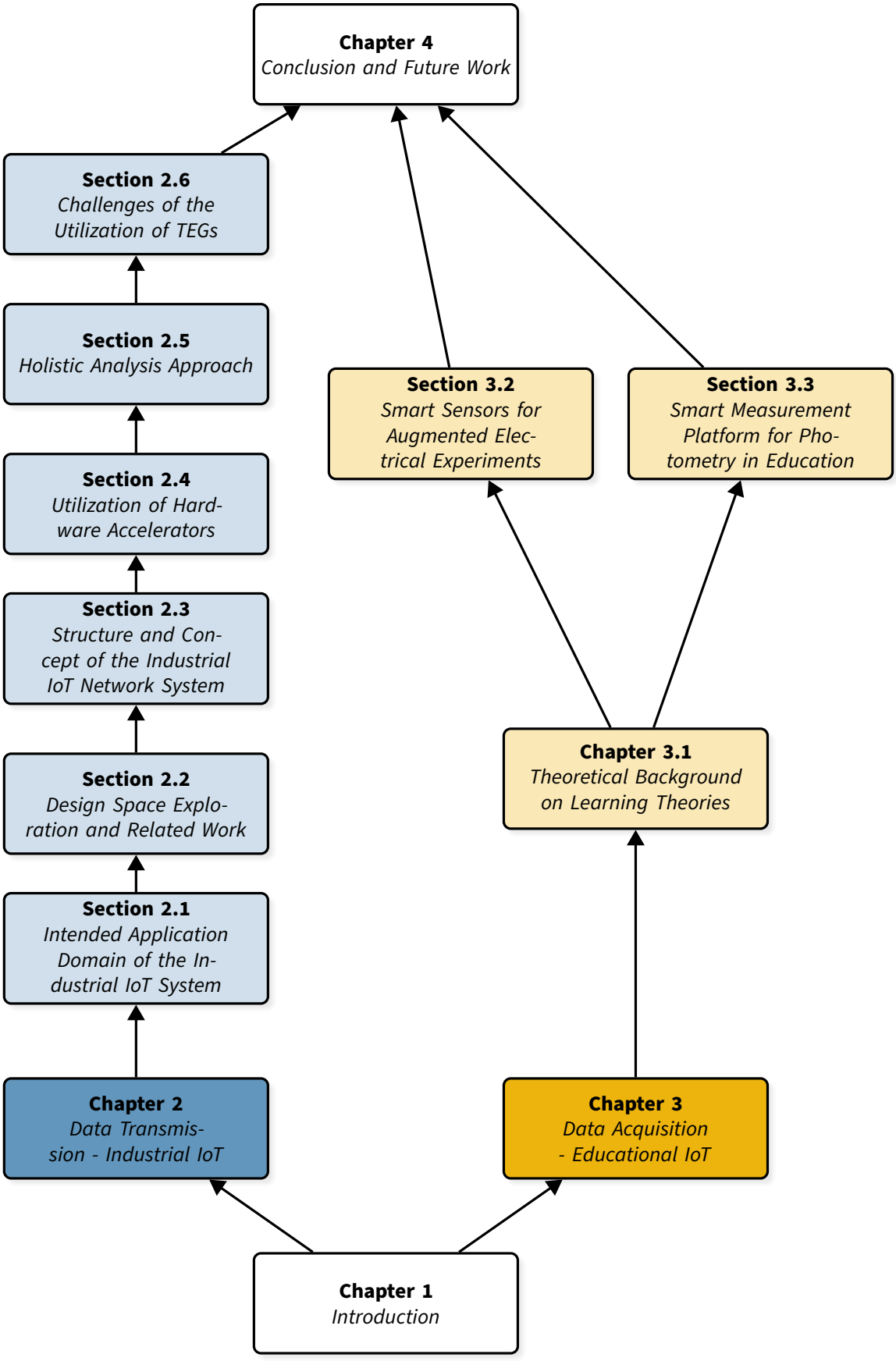

Figure 1.3: Thesis Outline

1.2.1 Key contributions in the field of Industrial IoT

The contributions in the field of Industrial IoT, focus on secure data transmission with a very limited energy budget (energy consumptions of less than 1000 mJ on the edge device, per connection establishment). To ensure compliance with proven security standards like the TLS protocol, a well-defined set of cryptographic algorithms and procedures must be employed. However, these are considered to be very computationally intensive for microcontroller-based low-power devices and are, therefore, in direct contrast to the low energy budget. In order to reduce energy consumption, many state-of-the-art systems rely on alternative protocols, which usually offer neither the high compatibility nor the widespread trust as already well-established protocols. Therefore this work presents a systematic approach to successfully utilize the widespread standard for secure data connections, the TLS protocol, also in low power IoT edge devices. It demonstrates that in contrast to related work, battery-powered edge devices with a wireless data connection can also benefit from the trust and security features of TLS while still achieving excellent battery life. Moreover, it is demonstrated that thermoelectric energy harvesting can adequately power such an edge device at temperature differences of just a few degrees. The contributions in the field of Industrial IoT are structured as follows:

- **Application Domain, Design Space Exploration and Concept of the Industrial IoT Network System (Section 2.1-2.3)**
  Based on a specific industry-related use case in the field of predictive maintenance, the associated requirements are identified and used for a subsequent design space exploration that evaluates and assesses possible technologies, setups, and solutions. The results are presented in the form of an aggregated Industrial IoT network system, which forms the basis for the following investigations. Both the design space exploration and the resulting Industrial IoT network system can be used as a reference for other domains of application.

- **Utilization of Hardware Accelerators (Section 2.4)**
  The use of CHAs to improve the speed and energy efficiency of cryptographic operations is a common approach for the optimization of embedded systems. In this section, the general feasibility of the previously defined setup is evaluated and presented as a battery runtime estimation. Furthermore, the impact of an isolated optimization by utilizing different CHAs in the TLS-based low-power Industrial IoT network system is shown.

- **Holistic Analysis Approach (Section 2.5)**
  This section contributes a holistic analysis approach for the TLS-based low-power Industrial IoT network system, which identifies limiting factors and corresponding optimizations. To the best of my knowledge, the resulting system is the first that closes the gap between using well-established security standards and low-power devices in the area of Industrial IoT network systems.

- **Challenges of the Utilization of TEGs (Section 2.6)**
  This section contributes a quantitative evaluation of the utilization of thermoelectric energy harvesting in a TLS-based low-power Industrial IoT network system considering different storage technologies. The results allow a direct correlation between the usable temperature difference of the energy harvester and the resulting minimum time interval for accumulating the energy required to establish a new connection for sending data to the cloud.

The contributions have been published in the following journal and conference papers:

- **TLS-Level Security for Low Power Industrial IoT Network Infrastructures [25]**
  This paper presents a secure Industrial IoT network system with battery-powered edge devices, based on the TLS protocol that is suitable for industry use. To address energy concerns, dedicated hardware accelerators are used to optimize the computationally-intensive cryptographic algorithms.

- **Analysis and Optimization of TLS-based Security Mechanisms for Low Power IoT Systems [26]**
  This paper presents a holistic analysis and optimization of the previously in [25] presented Industrial IoT network system. The overall energy consumption for ephemeral TLS handshakes was reduced by half and the associated latency by about one order of magnitude compared to related work.

- **Exploration of Thermoelectric Energy Harvesting for Secure, TLS-based Industrial IoT Nodes [27]**
  This paper investigates the use of a TEG for the battery-independent operation of an edge device based on the previously published Industrial IoT network system. The findings demonstrate that temperature differences as small as 1 K at the TEG are sufficient to ensure a secure connection to the cloud multiple times per hour.

The presented work also contributed to publications in the area of post-quantum cryptography [28, 29].

1.2.2 Key contributions in the field of Educational IoT

The smart learning environments presented in this work are the outcome of a close collaboration between the research areas of didactics and electrical engineering. Most state-of-the-art learning environments are limited by their use of only off-the-shelf components that are very user-friendly. Transferring classic IoT concepts and advanced technology to learning environments and thus creating an educational IoT opens up completely new possibilities. Examples include the concept of a digital twin or the creation of a sensor base for the use of artificial intelligence. The contributions in the field of Educational IoT are split into two sections:

- **Smart Sensors for Augmented Electrical Experiments (Section 3.2)**
  This section presents a smart sensor system for educational *Science Technology Engineering Mathematics* (STEM) experiments in electrical circuits with a focus on usage in an AR environment. It consists of sensors for voltage and current measurement, position identification with a focus on a 2D plane, and cable identification for circuit reconstruction. In addition, a solution for an energy-efficient and robust data transmission of the measured values to the Microsoft HoloLens 2 through the use of the state-of-the-art *Bluetooth Low Energy* (BLE) standard is contributed. Furthermore, an evaluation of the installed sensor systems in terms of accuracy and precision is presented.
- **Smart Measurement Platform for Photometry in Education (Section 3.3)**
  This section contributes a portable photometric measuring system with smart electronics for inquiry-based learning in STEM lessons together with a digital twin of the including visualization and recording function implemented on a tablet. Through the detailed tracking of all user interactions, this platform forms the foundation for a wide range of future research questions on advanced learning analytics and technology-enhanced learning approaches.

The contributions have been published in the following journal papers:

- **Smart Sensors for Augmented Electrical Experiments [30]**
  This paper presents the smart sensor system for educational STEM experiments in electrical circuits with a focus on usage in an AR environment which is described in Section 3.2. Additionally, the paper includes a usability study conducted with 20 pupils at a German high school. The evaluation resulted in a usability rating of 94 out of 100 points.
- **SmaEPho–Smart Photometry in Education 4.0 [31]**
  This paper presents a smart learning platform and its digital twin for inquiry-based learning in STEM, with a focus on electrical circuits and photometric measuring. The system is described in depth in Section 3.3. Moreover, the paper features a usability study with 52 students which confirmed the excellent usability of the smart learning platform.

The work presented here on Educational IoT has also contributed to the following publications [32–37].

Apart from that, publications in the area of application-specific memory controllers [38] and in the area of transiently-powered IoT sensor devices [39] have been supported.

A part of this research in the area of smart learning environments is supported by the project “U.EDU” (Funding number: 01JA1916 and 01JA2029) of the “Qualitätsoffensive Lehrerbildung”, a joint initiative of the Federal Government and the Länder which aims to improve the quality of teacher training. The program is funded by the Federal Ministry of Education and Research. The author is responsible for the content of this publication.

Chapter 2

Data Transmission - Industrial IoT

The concept of Industrial IoT extends the IoT into the industrial environment. By connecting a wide variety of devices, systems, and sensors, a broad range of process parameters, environmental data, and machine information can be collected and made available to other systems. The resulting potential is vast and spans across various industrial sectors. Manufacturing [40, 41], healthcare [42–44], transportation [45], agriculture [46], energy [46] and logistics [47] are just a few domains where the Industrial IoT is having a significant impact. The resulting benefits range from improved operational efficiency, predictive maintenance, and increased security to real-time monitoring and automation. Highly popular topics such as machine learning are contributing further to the enormous growth of the Industrial IoT and enabling a wide variety of new possibilities. This significant evolution is only possible due to the massive progress in microelectronics. Innovations enable more powerful processors, larger memories, and greater energy efficiency. This progress has been mainly determined by the constantly reduced feature size of the transistors. This made it possible, as Gordon Moore predicted in 1965, to double the number of transistors in an *Integrated Circuit* (IC) approximately every two years [48] (denoted as Moore's Law).

The central component of most (Industrial-) IoT devices is a microcontroller. Microcontrollers typically consist of a microprocessor, memory to store the application data, several peripheral interfaces, and an integrated power supply to generate the different voltage levels required for the various internal components. Having all the necessary parts directly on the chip drastically reduces the number of components and the system's overall complexity. The significant advancements in transistor technology have also resulted in major progress in the development of microcontrollers. About 20 years ago, the ATmega16[1] from Microchip, was an average and very popular microcontroller. It features a 16 MHz main clock, 1 kB *Random-Access Memory* (RAM) and 16 kB flash. Nowadays, there are a huge number of microcontrollers that

[1] https://www.microchip.com/en-us/product/atmega16, accessed April 28, 2023

serve various application areas and are optimized correspondingly. Performance-targeted devices like the i.MX RT1050[2] series from NXP Semiconductors reach clock frequencies of 600 MHz, others like the EFM32PG23 Gecko Family[3] from Silicon Labs are tailored for minimal energy consumption and use only 70 µW/MHz while running code from flash. Yet other devices were developed with a focus on extremely small package sizes or with special security requirements. In addition, modern microcontrollers contain more and more peripherals such as application-specific interfaces, wireless modules, or customized hardware accelerators. Due to the constantly growing amount of features included in the devices, manufacturers are increasingly referring to them as *System on Chips* (SoCs). A good example here is the recently introduced nRF54H20 SoC[4] from Nordic Semiconductor. Besides several Arm Cortex-M33 processors, multiple RISC-V coprocessors, and specialized cryptographic hardware accelerators, the SoC also features 2 MB non-volatile memory, 1 MB RAM, a built-in Bluetooth 5.4 capable radio, as well as a number of other interfaces such as high-speed *Universal Serial Bus* (USB) and *Controller Area Network Flexible Data-Rate* (CAN FD). In addition, the SoC is specifically designed for wireless applications with limited energy budgets. The availability of such powerful SoCs in combination with the necessary energy efficiency opens up a wide range of new possibilities and fields of application. On the one hand, computationally intensive applications such as machine learning or sensor fusion at the edge benefit from higher computing capacities, larger memories, and various special hardware accelerators. On the other hand, this progress also offers new opportunities and desperately needed approaches in the area of security.

The large number of increasingly powerful devices in the Industrial IoT combined with the high level of connectivity represents a great opportunity for cybercriminals. Botnets such as Mirai [18, 19] have clearly demonstrated the damage that can be caused by weak or even unsecured systems. Moreover, due to the steady progress in the field of quantum computers, which can solve certain algorithms, such as Shor's Algorithm [49], much faster due to their specific structure, they pose a major threat to many common cryptographic methods. The implementation and utilization of security mechanisms that reliably defend against these different hazards are essential for the further expansion and development of the Industrial IoT. This has led to a significant increase in research activities in the area of Industrial IoT over the past years, with the main focus on authentication, data security, and data sharing as well as security monitoring [50]. Due to the different requirements of the various sectors in the Industrial IoT, the resulting procedures and solutions vary greatly even within the individual sectors. In particular, sectors with very limited energy budgets often deviate from well-established standards in data security, like public-key cryptography

[2] https://www.nxp.com/products/processors-and-microcontrollers/arm-microcontrollers/i-mx-rt-crossover-mcus/i-mx-rt1050-crossover-mcu-with-arm-cortex-m7-core:i.MX-RT1050, accessed April 28, 2023

[3] https://www.silabs.com/mcu/32-bit-microcontrollers/efm32-gecko, accessed April 28, 2023

[4] https://www.nordicsemi.com/Products/nRF54H20, accessed April 28, 2023

or the general TLS protocol, referring to the excessive computational intensity for constrained IoT devices [20–24]. As a result, various custom solutions and lightweight alternatives are being developed to avoid those calculations and protocols that are considered computationally intensive. This not only limits system compatibility and lack of confidence in well-established protocols but also hinders the adaptability of new procedures and insights.

The demand for a baseline system for data transmission between edge devices and the cloud that meets today's security requirements, such as for example those defined by the *Bundesamt für Sicherheit in der Informationstechnik* (BSI) [5], as well as provides extensibility for future security updates, is extremely high, especially in the Industrial IoT. Using proven protocols and algorithms is essential to maintain compatibility and trust. The limiting factor of such a solution is, in general, the very restricted energy budget of the edge device, which prevents the use of extensive protocols and computationally intensive algorithms. This work addresses this challenge based on a real-world industry example by exploiting the potential of modern, state-of-the-art SoCs with integrated specialized hardware accelerators as well as various analysis and optimization methods. The result is an Industrial IoT system for transmitting data between edge devices and the cloud, which, contrary to related work, closes the gap between well-established security standards and low-power edge devices.

The further course of this chapter is structured as follows: In Section 2.1, the exact scope of application of the system and the consequential parameters, as well as the generalisability of the requirements, are described. The resulting prerequisites serve as the inputs for the design space exploration, which is performed in combination with related work in Section 2.2. Thereby, the essential components of the system are described in detail one after the other, and design decisions for the resulting Industrial IoT system are derived. The section concludes with an overview of other secure low-power Industrial IoT network systems. The exact design and structure of the system resulting from the design space exploration, which will be used throughout this chapter, is described in detail in Section 2.3. Section 2.4 is dedicated to the general feasibility of the system and shows initial measurement data and performance characteristics. In Section 2.5, more detailed analyses and optimizations on the system level are performed which lead to a significant reduction in the energy required by the edge device. Taking into account the area of application presented in Section 2.1, the possibility of powering the edge device through thermoelectric energy harvesting is investigated in more detail in Section 2.6. Finally, Section 2.7 describes limitations and Section 2.8 further scientific research based on this system.

The key contributions of this chapter are already summarized in Section 1.2.1

[5] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf, accessed November 12, 2023

2.1 Intended Application Domain of the Industrial IoT System

The concept of Industrial IoT describes the constantly increasing linkage of sensors, devices, and systems in the industrial environment. In order to be prepared for this new age, many modern machines are therefore equipped with appropriate sensors and interfaces to provide process parameters directly to the relevant systems. Older machines usually do not offer these functions. This is a considerable problem, especially in areas with machines that have a very long lifespan. Edge devices equipped with the appropriate sensors for capturing the required process parameters and a suitable network system offer a way of adding this functionality post hoc. In order to optimize subsequent installation, these edge devices are usually equipped with a wireless data connection and are battery-powered which makes them independent from the power grid. Energy efficiency is consequently a central factor in the development of such edge devices allowing an extended operation time and a reduction of maintenance intervals. However, this is inevitably in direct contrast to the high-security requirements for data transmission in the Industrial IoT, since the use of cryptographic operations inherently leads to increased computational effort and thus higher energy requirements.

A specific example of the use of a low-power/energy edge device with high data security requirements can be found in the field of predictive maintenance for industrial pumps. Since pumps are often required in critical infrastructures such as the cooling circuits of power plants, fire-fighting systems, or water supply systems, reliable operation, ensured by regular maintenance intervals, is essential. Companies such as KSB [6], one of the world's largest manufacturers of pumps and industrial valves, are aiming to achieve both more accurate monitoring of operations and more targeted maintenance through the use of predictive maintenance using advanced sensor systems and analysis algorithms. The amount of data that needs to be sent to the cloud is usually relatively small, <1 kB/h can be taken as a rough approximation. In addition, the data does not need to be sent continuously, consolidated updates at intervals of 30 minutes up to several hours are sufficient. However, since the lifetime of such pumps is typically several decades, there are many pumps already in the field that are far from reaching the end of their lifetime. Therefore, the need to equip these pumps with the new sensor technology is very high.

While the pumps have a direct power supply, the process of rewiring and adopting power domains on already deployed pumps to connect the sensor devices often incurs substantial expenses, especially in an industrial context. To be a viable solution, it is important that the sensor devices can be attached post hoc on existing machines.

[6] https://www.ksb.com/, accessed April 28, 2023

Therefore, these devices generally must be battery-powered and communicate wirelessly with data collection units or cloud systems. As a result, low-power/energy system design becomes essential in order to reduce costly battery replacement cycles. Furthermore, as wireless communication is always exposed to attackers, the security aspect of the communication becomes a primary requirement for such Industrial IoT systems. It is, therefore, not enough to encrypt the data itself, but also to ensure data integrity and authentication of the communication partners. To provide this end-to-end encryption and authentication, the edge device must be able to communicate directly with state-of-the-art cloud infrastructure without relying on additional security-critical intermediate systems. However, it is not necessary to maintain this connection continuously, since the sensor data usually does not require real-time availability. This enables the edge device, for instance, to awaken every fifteen minutes, retrieve the data, and transmit it to the cloud over a secure connection. The system can go into a deep sleep mode between these connections.

Although the above requirements are derived from a direct use case, they are also applicable to many other application areas. The increased flexibility and ease of installation of edge devices, due to their independence from extensive cabling, allows them to be deployed quickly or even temporarily in a wide range of applications in various industry fields. The need for state-of-the-art security mechanisms is also essential in effectively all wireless networks, regardless of their application.

2.2 Design Space Exploration and Related Work

Based on the requirements described in the previous chapter, this section elaborates on a system architecture and defines the underlying components and mechanisms. Since the security of the data transmission determines the specifications for the wireless data communication technology, some key aspects of secure data transmission are discussed below and related work is assigned. This is followed by an overview of the selected wireless data communication technology and its differentiation from alternative approaches. Subsequently, the off-the-shelf SoC, which forms the core of the edge device, is selected. The chapter concludes with an overview of related secure low-power IoT network systems.

2.2.1 Data Security in the Industrial IoT

The importance of advanced security standards for IoT and especially in Industrial IoT is well-known and has been intensively studied, e.g. [22, 51]. In particular, when used in critical infrastructures, state-of-the-art security mechanisms are unavoidable [19, 50, 52].

Cryptographic Algorithms

Cryptographic algorithms are one of the key components of data security. They are used to ensure confidentiality, data integrity, and data authenticity. Accordingly, there is a wide variety of algorithms and procedures to perform a range of different tasks. A general distinction can be made between symmetric and asymmetric encryption methods as well as hash functions.

Symmetric encryption methods are designed to ensure confidentiality and have only one key that is used for both encryption and decryption. Use cases include the encryption of stored data as well as data that is transmitted over a public channel such as the Internet. One of the most widely used methods is the *Advanced Encryption Standard* (AES) [53], which is also recommended by the BSI [54]. The AES algorithm is known to be relatively efficient to execute on processors, and there are many specific implementations with the goal of energy efficiency or performance [55, 56]. Even small microcontrollers with a focus on high energy efficiency are able to execute an AES operation relatively fast. A major challenge in the use of symmetric encryption methods is the distribution and handling of the key since there is only one key that must be known to all participating parties.

Asymmetric encryption methods use two different keys: a private key, and a public key. These two keys can be used for several applications. On the one hand, the public key can be used to encrypt messages that can only be decrypted with the corresponding private key. On the other hand, messages can be signed with the private key, which in turn can be verified with the public key. Furthermore, the *Diffie-Hellman*

(DH) method can be used to enable a secret exchange of keys over a public, eavesdropping line. They are thus an essential component of modern cryptography and enable the establishment of a *Public Key Infrastruktur* (PKI) for the purpose of digital authentication. Frequently used algorithms are, for example, *Elliptic Curve Cryptography* (ECC), *Rivest Shamir Adleman* (RSA), *Digital Signature Algorithm* (DSA), DH. In general, asymmetric encryption methods are known to be less efficient than symmetric methods, due to the usually more complex underlying mathematical problems. Since these methods are typically only used to encrypt short sequences such as hash values for signature or keys for use with symmetric methods, the higher computing requirements for computers and servers are usually negligible. However, this does not necessarily apply to low-power embedded devices. Depending on the method, this represents a major challenge in terms of memory requirements and computing power [44, 57, 58].

Cryptographic hash functions are a special case of cryptographic operations. They generate a value with a fixed size, the so-called hash, from a value of arbitrary size. Accordingly, this is a function where it is practically impossible to invert or reverse the calculation. Cryptographic hash functions are, for instance, used in digital signatures and message authentication but also in many other fields of applications. Popular hash functions are for example *Secure Hashing Algorithm 2* (SHA-2), *Secure Hashing Algorithm 3* (SHA-3), *Message-Diges Algorithm 5* (MD5) or BLAKE. Due to their structure, they can be executed relatively efficiently even on resource constraint devices [59–61].

Due to the enormous progress in the development of quantum computers, the field of ***Post-Quantum Cryptography* (PQC)** is becoming increasingly important. Since quantum computers are likely to solve certain mathematical problems like Shor's Algorithm [49] in the future much faster due to their special structure, they pose a major threat, especially to state-of-the-art asymmetric encryption methods. PQC is an active research area, and standardization efforts are ongoing to identify and select the most promising post-quantum crypto algorithms. These algorithms are being developed based on mathematical problems that are currently considered to be resistant to attack by both classical and quantum computers. They come from various areas of mathematics, such as lattice theory, code-based cryptography, multivariate polynomials, hash-based signatures, and others. In addition to the actual security, a central research topic is the significantly higher performance requirements compared to conventional cryptographic processes. These refer to the necessary memory demand, the key size, and the required computing power.

Cryptographic Hardware Accelerators

Hardware accelerators are dedicated components optimized for a specific workload such as machine learning, cryptography, graphics rendering, and many others. This optimization does not necessarily have to be aimed at computational performance,

but can also focus on energy efficiency, chip size, or a combination. These improvements are achieved through specialized architectures. Typically, hardware accelerators can offer orders of magnitude improvements in performance per cost and performance per watt over general-purpose computers [62] but lag in flexibility.

Hardware accelerators for cryptographic operations, so-called CHAs, are available for a wide variety of cryptographic functions and applications. In the application area of microcontrollers, these are either connected as an external component via a standard interface or directly integrated into system-on-chips. The range of supported algorithms varies greatly depending on the application target. For example, cryptographic coprocessors such as the external ATECC508A by Microchip or the CryptoCell-310, which is integrated into the nRF52840 SoC by Nordic Semiconductor, are designed for more widespread functions like RSA, ECC, SHA-2, and AES. CHAs like presented in [63], on the other hand, are strongly optimized for the execution of a single primitive. In addition to optimizing the calculations, the CHAs often have other features such as true random number generators, secure key memories, or resistance to tampering. Usually, CHAs are offering a considerable advantage, especially for asymmetric encryption processes and when processing large amounts of data [26, 64, 65]. Hardware accelerators also play a crucial role in the context of PQC. They represent a large research area and make many of the PQC algorithms suitable for general use. Especially in the course of the NIST standardization process for PCQ algorithms [7], a huge number of different hardware accelerators for different algorithms and different approaches have been published [63, 66–69].

Cryptographic Protocols

Cryptographic protocols are another key component to achieving state-of-the-art security requirements. They define strict rules and procedures on how certain cryptographic algorithms must be applied in order to establish, for example, a secure connection between two communication partners. This form of standardization offers many advantages, such as the validation of protocols, increasing interoperability, and simplifying their implementation. A very popular cryptographic protocol is the *Secure Shell* (SSH) protocol. It is generally used for secure remote login and command line execution. The *Internet Protocol Security* (IPsec) is another cryptographic protocol that provides a secure connection between two computers on an *Internet Protocol* (IP) network. It is mainly used to establish *Virtual Private Network* (VPN) connections. The most widely used cryptographic protocol on the modern internet is the TLS protocol. In fact, it is supported by all of the top 100 websites and is used by default by 97 of them[8]. As TLS is also the standard for secure communication with the IoT applications of the leading cloud platforms, it is discussed in more detail in the next section.

[7] https://csrc.nist.gov/projects/post-quantum-cryptography, accessed April 28, 2023
[8] https://transparencyreport.google.com/https/overview, accessed January 16, 2023

TLS Protocol

TLS is an *Internet Engineering Task Force* (IETF) standard proposed in 1999. The current version, TLS 1.3 was defined in August 2018. It is a standardized cryptographic protocol for client/server applications to secure communications against eavesdropping, tampering, and message forgery [70]. The protocol consists of two layers. The lower layer (TLS Record Protocol) is based directly on the transport layer (*Transmission Control Protocol* (TCP)) and ensures both the encryption of the application data using symmetric cryptographic algorithms and the integrity and authenticity through a *Message Authentication Code* (MAC). It also manages message fragmentation and compression. The upper layer (TLS Handshake Protocol) is responsible, on the one hand, for negotiating the cryptographic procedures and keys to be used for the connection. On the other hand, it is responsible for the authentication and identification of communication partners using asymmetric encryption methods. TLS supports various methods based on different cryptographic algorithms for secure key exchange, authentication, and encryption of the data connection. To determine which procedures are used to establish a secure connection, so-called ciphers are used. An example of a cipher would be *"TLS ECDHE ECDSA AES 128 GCM SHA256"*. It consists of a key exchange algorithm (*ECDHE*), an authentication algorithm (*ECDSA*), an encryption algorithm (*AES 128*), a message authentication code algorithm(*GCM*), and a hash algorithm(*SHA256*) (see below for a more detailed explanation). Since the ciphers are renegotiated between the connection partners for each new connection, this approach offers an extremely high degree of flexibility. A server can allow several combinations of procedures to meet a wide range of requirements. This also makes it possible to subsequently exclude or give preference to certain procedures. Especially in the context of the new PQC algorithms, this mechanism is extremely useful, as it allows individual, potentially compromised algorithms to be exchanged for PQC algorithms. In short, the TLS protocol provides a framework around various cryptographic algorithms and defines a fixed procedure for using them.

There are a number of libraries for using the protocol on different target platforms, the most popular open-source library available for a variety of platforms being OpenSSL [9]. There are also a variety of specific libraries developed for embedded applications, such as mbedTLS [10] or wolfSSL [11]. However, the generally high memory requirements of the TLS protocol, due to package size and handling, as well as the computationally intensive cryptographic algorithms pose a major challenge for resource-constrained embedded devices [20–24]. Therefore, several lightweight protocols such as *Energy Efficient Datagram TLS* (eeDTLS) [71], E-Lithe [72] and *Compact TLS* (CTLS) [73] have been proposed to reduce both the complexity of the cryptographic computations and the amount of data that has to be handled, e.g. [74–78]. These alternatives, however, do either not provide the same level of trust as TLS

[9] https://www.openssl.org/, accessed April 28, 2023
[10] https://github.com/Mbed-TLS/mbedtls, accessed January 16, 2023
[11] https://www.wolfssl.com, accessed January 16, 2023

or are not supported by leading cloud platforms like AWS IoT [79] or Google IoT Core [80], which prevents proper end-to-end encryption.

In terms of data security, the use case described in Section 2.1 poses clear requirements for state-of-the-art security mechanisms for data transmission. These include end-to-end encryption with unique keys generated for each session and explicit authentication of communication partners via a PKI. Furthermore, the integrity of the transmitted data must be guaranteed in order to detect possible manipulations. In addition to the security requirements, the use case also defines compatibility with state-of-the-art cloud services without having to rely on additional security-critical intermediate systems. This requires direct IP communication between the cloud server and the edge device, enabling true end-to-end encryption and authentication.

The TLS protocol provides both the necessary security and compatibility, as well as the high level of trust that derives from its widespread use as a standard for secure communications on the internet. Despite the increased demands on embedded hardware in terms of memory and processing power, the benefits of using such an established protocol outweigh the drawbacks. Furthermore, given the huge improvements in the performance and energy efficiency of embedded hardware, and the availability of various cryptographic hardware accelerators, the benefits of using such an established method clearly dominate.

> *Due to its support for state-of-the-art security mechanisms, high flexibility, and broad compatibility with leading cloud platforms, the TLS protocol was selected for this work to be used in the proposed Industrial IoT setup.*

In all the upcoming experiments, unless explicitly described otherwise, the cipher suite *"TLS ECDHE ECDSA AES 128 GCM SHA256"* is used. This implies the use of the following cryptographic procedures:

- *Elliptic Curve Diffie-Hellman Ephemeral* (ECDHE): The shared secret, used to encrypt the transmitted data is generated using the elliptic-curve-based key agreement protocol with ephemeral keys.
- *Elliptic Curve DSA* (ECDSA): Elliptic-curve-based certificates are used for mutual authentification and identification of the communication partners. Both parties verify each other.
- AES 128 and *Galois/Counter Mode* (GCM): The shared secret is used with AES 128 and GCM to encrypt the data.
- SHA-2: All hashing operations are performed using the SHA256 algorithm.

2.2.2 Wireless Comunication

The choice of wireless data transmission technology has a significant impact on the overall performance of the system. This includes energy efficiency, potential data rate, transmission range, the ability to use local gateways, robustness, and much more.

> *Based on the requirements defined in the previous sections, BLE, together with the Internet Protocol Version 6 (IPv6) over Low power Wireless Personal Area Network (6LoWPAN) protocol, was chosen for this work to establish an IPv6 connection to the cloud server.*

This selection is explained in more detail below, using various properties and parameters.

End-to-End IPv6

The integration of IoT devices through standard internet communication protocols opens up a wide range of possibilities as well as seamless integration with existing infrastructure. Each server can be reached via the *Internet Protocol Version 4* (IPv4) and/or IPv6 protocol. IPv6 has several advantages over IPv4, including the increased number of IP addresses, which is a major benefit given the enormous growth in the number of IoT devices. The advantages and opportunities of using IPv6 in the IoT have already been published in various papers (e.g.: [81–83]). In the given use case of predictive maintenance, the implementation of the IPv6 protocol enables the direct use of the TLS protocol, providing the basis for state-of-the-art security and direct compatibility with the leading cloud platforms.

6LoWPAN Standard

Back in 2004, the IETF 6LoWPAN Working Group started the standardization to transmit IPv6 packets over IEEE 802.15.4. IEEE 802.15.4. is a transmission protocol for *Wireless Personal Area Networks* (WPANs) and forms the core of wireless networks such as ZigBee. In 2013, the IETF *IPv6 over Networks of Resource-constrained Nodes* (6Lo) Working Group launched to standardize an IPv6 adaptation for other low-power wireless transmission technologies. With the publication of *RFC 7668* [84] in 2015, a standard for the transmission of IPv6 packets via BLE was published. Today, even a default Linux kernel includes an implementation of the *RFC 7668* standard, so a simple Raspberry Pi [12] with a built-in BLE module can be used as a gateway. However, the 6LoWPAN standard is frequently incorrectly equated with IEEE 802.15.4. In fact, 6LoWPAN acts purely as an adaptation layer to the actual network layer. The

[12] https://www.raspberrypi.com, accessed January 16, 2023

underlying link layer and physical layer are then provided either by BLE or by IEEE 802.15.4. Figure 2.1 shows an example of a complete protocol stack.

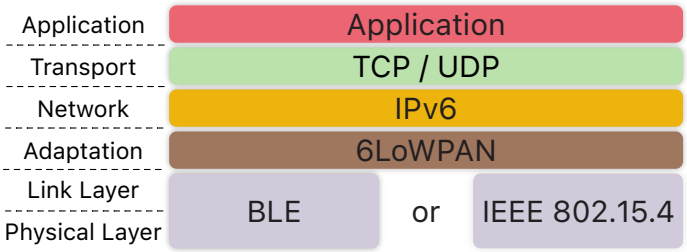

Figure 2.1: Example Protocol Stack with 6LoWPAN Adaptation Layer

Range vs. Energy

The length of the distance to be covered wirelessly has a significant influence on the energy required. With comparable antenna size and data rate, more energy must be used to transmit the data over a greater distance. As a basic approximation, the intensity decreases quadratically with the distance (Inverse-square law). In a system with severely limited energy, it is therefore necessary to evaluate the radio range that is really needed. The actual range of a BLE radio connection ranges from a few meters to over 50 m, depending on, for example, external interferences used transmit power, and the positioning of the antenna. However, under the expected conditions, the range of BLE is sufficient for the proposed scenario in Section 2.1. With a radius of about 20 m, even multiple sensors can be covered by one gateway. Wireless standards such as NB-IoT or LTE-M, with their much longer ranges and consequently higher energy requirements for transmitting the same amount of data, are therefore not being considered.

Gateway

Wireless connections always require a gateway that provides a network connection to the target server in the cloud. This service can be handled either by a mobile network provider, such as NB-IoT, or by a private gateway, such as a WLAN access point. As the pumps considered in our use case are often deeply integrated into large industrial plants or used in underground installations, the dependency on network coverage or the respective mobile network providers is a major limitation. The use of the BLE protocol requires the installation of dedicated gateways. However, these are independent of providers and license fees for radio bands and can be deployed flexibly. It is important to note that in the chosen configuration, the gateway only acts as a kind of switch that forwards the IPv6 packets received via BLE over the wired *Local Area Network* (LAN) interface or vice versa. The gateway does not represent a security-critical component within the data transmission itself, as the actual protection of the data connection takes place directly between the edge device and the server.

Energy

The energy consumption of different wireless technologies is influenced by various parameters such as frequency and transmission power, but also protocol overhead. Shahzad et al. [85] analyzed the energy consumption of three different short-range wireless technologies - BLE, ZigBee based on IEEE 802.15.4 and WLAN - depending on the amount of data transmitted. The results show that ZigBee required the least energy for small amounts of data up to 500 B and WLAN for large amounts of data over 800 kB. BLE proved to be the most energy efficient for the range in between. BLE has also proven to be more energy efficient than IEEE802.15.4 when using the 6LoWPAN standard [86]. In [87] and [88], an IPv6 connection over BLE between two Raspberry PIs is established and examined in more detail. The amount of data to be transmitted in the use case described in Section 2.1 is approximately 4-10 kB for the TLS handshake and less than 1 kB for sensor data.

Connection Robustness

BLE uses a *Frequency Hopping Spread Spectrum* (FHSS) technique to minimize the influence of interference from other wireless devices operating in the same frequency band. This approach involves rapidly switching the operating frequency within the 2.4 GHz band, which reduces the impact of narrowband interference and enables coexistence with other wireless technologies such as WLAN. In addition, *Adaptive Frequency Hopping* (AFH) dynamically selects the channels with the least interference to provide a stable connection even in environments with a high density of wireless devices. Moreover, the use of error detection and correction mechanisms helps to improve data integrity and reduces the likelihood of retransmissions due to erroneous data.

2.2.3 System on Chip

Apart from energy consumption, the selection of the SoC significantly influences the actual potentialities and restrictions of the system. As mentioned above, there are a large number of different SoCs available today, with various features and application targets.

> *For the application context described in the previous section, an Arm Cortex-M4-based SoC (nRF52840) from Nordic Semiconductor [13] was chosen for this work.*

[13] https://www.nordicsemi.com/products/nrf52840, accessed April 28, 2023

The requirements and considerations for this choice are described in more detail below.

The proposed application scenario and the considerations described in Chapter 2.2.1 and Chapter 2.2.2 set the first baseline requirements for the SoC. Initial experiments have shown that a minimum RAM size of 128 kB is required for a robust implementation. This results primarily from the presence of the necessary network stack that dynamically receives and parses packets, as well as the processing of certificates, keys, and signatures during the TLS handshake. The chosen SoC features 256 kB of RAM, providing some flexibility for future extensions or other cryptographic procedures such as PQC. Since the SoC communicates directly with the network, computation times must not exceed a certain runtime in order to avoid network timeouts. Initial tests have shown that the 64 MHz clock frequency of the nRF52840 SoC is sufficient to avoid the *Central Processing Unit* (CPU) becoming a bottleneck for the network performance. An integrated hardware accelerator for various cryptographic operations such as RSA, ECC, SHA-2, AES, and *True Random Number Generator* (TRNG) allows for offloading some of the heavy cryptographic workload from the processor and enables energy-efficient computation of these operations. The required wireless communication interface is provided by an integrated multiprotocol Bluetooth 5.4 radio that supports BLE, Bluetooth mesh, *Near Field Communication* (NFC), Thread, and Zigbee protocols. The nRF52840 SoC has already been tested in various projects to be very energy efficient, especially in combination with the integrated BLE radio.

Besides the specific technical data of the SoC, the available tool environment, including measurement and debugging methods, as well as existing experience, always has an impact in the field of embedded development. The nRF52840 SoC from Nordic Semiconductor was chosen based on both technical requirements and personal preference. Therefore, it is important to note that similar controllers, such as, for example, the EFR32BG24 from Silicon Labs * or the STM32WB5MMG from ST Microelectronics *, should lead to at least similar results.

2.2.4 Related Work

When considering related work, I only refer to TLS-based systems or systems with a comparable security approach.

The security of low-power wireless networks has been considered in multiple surveys [89, 90]. Many solutions have been proposed, such as the use of intermediate gateways [91, 92], or lightweight protocol alternatives to TLS. Although TLS and the use of a PKI are often dismissed as not suitable for IoT devices [20–23, 93, 94], there are many papers that have still investigated the performance of TLS on resource-constrained devices. For example, [95] investigates the performance of TLS and *Datagram TLS* (DTLS) on various Arm Cortex-M3 and Cortex-M4 controllers, but omits the impact of wireless data transmission. [96] evaluates the performance of TLS and DTLS using

Zephyr OS, a widely used open source IoT operating system. [97] analyzes the impact of different TLS cipher suites using two WLAN-connected IoT boards utilizing an Arm Cortex-R4 each. The influence of connection properties such as packet loss on a TLS secured *Message Queuing Telemetry Transport* (MQTT) connection is explored in [98]. [99] compares the influence of the different versions TLS 1.2 and 1.3 as well as DTLS 1.2 and 1.3 with each other.

However, to the best of my knowledge, there was no work prior to our publications [25–27] that focused specifically on low-power sensor devices while still using standard TLS with state-of-the-art security levels.

2.3 Structure and Concept of the Industrial IoT Network System

The areas of application and, thus, the resulting requirements for data transmission in the IoT vary greatly. Due to this diversity, there will not be a solution that covers all areas of application in the best possible way. In the subsequent analyses and optimizations in this chapter, though, the same general structure and setup will be used. This setup is derived from the decisions and considerations in the previous design space exploration and presented in the following. Although this system was derived from a specific use case, the layered structure of this setup allows the system to be adapted to a wide range of other applications. At the same time, many of the results can be transferred and applied to other similar systems.

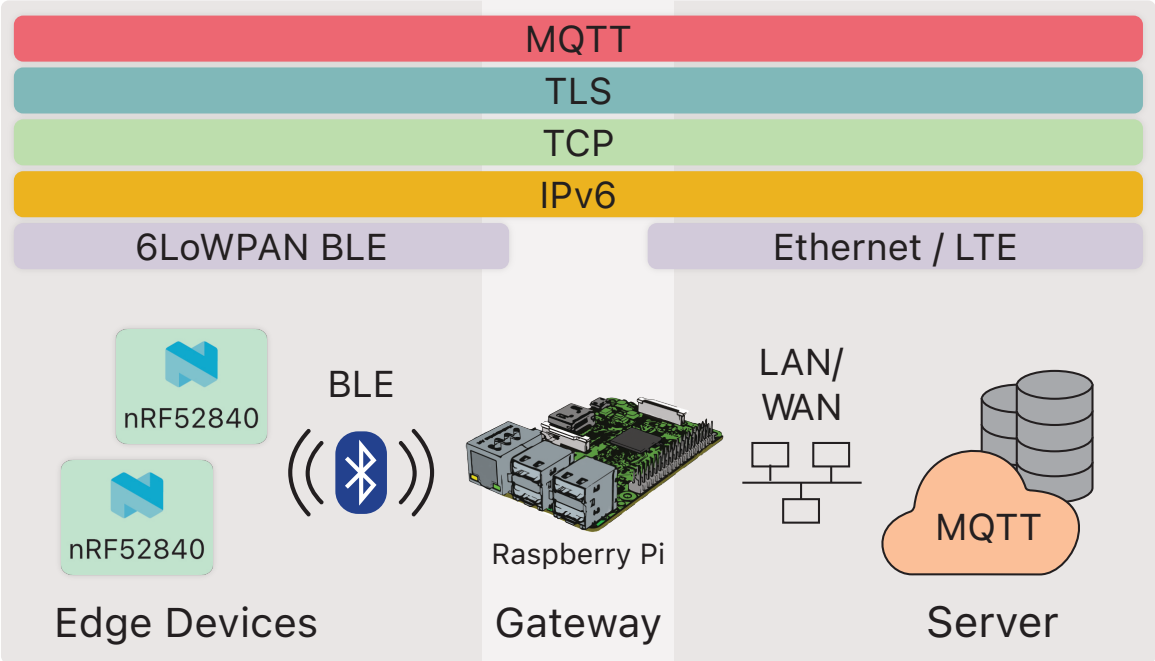

Figure 2.2: (Protocol-)Structure of the Industrial IoT System

Figure 2.2 illustrates the general system design and protocol structure. The three main components are the low-power sensor devices, in the following referred to as edge devices, the gateway, and a generic server that provides a MQTT broker. As already discussed in Subsection 2.2.3, the main computational unit of the edge device consists of the nRF52840 SoC by Nordic Semiconductor. The gateway is a Raspberry Pi 3 running Debian as its operating system. It is connected via the internet to an IPv6-enabled server, which provides an MQTT broker using the common Eclipse Mosquitto, message broker * software. The distinctive feature of this system is illustrated by the protocol structure in Figure 2.2 (top). Since IPv6 is used throughout the system, the gateway serves merely as a bridge between the different physical and link layers

(transparent gateway). This is made possible by the use of BLE and the 6LoWPAN standard between the edge device and the gateway. This standard allows IPv6 packets to be transmitted directly over BLE. By using a corresponding IP stack (in this case LWIP [14]) and a TLS library (in this case MbedTLS [15]), a classic TLS end-to-end encryption can be established between the edge device and the server. As an application layer, MQTT is used as an example, but this can easily be changed to other protocols if required by the target application, as the data security-related parts are handled by the underlying TLS layer.

Since, according to the use case, the edge device is not permanently connected to the server but only establishes a secure connection, for example, every 15 minutes, it can enter a deep sleep mode during the remaining time. Depending on the selected deep sleep mode, the SoC may be woken up by an internal timer or may even need to be woken up by an external source, such as an external real-time clock. Figure 2.3 illustrates this behavior in more detail. For security reasons, the respective connection set-ups are completely independent of each other and, therefore, always employ *Perfect Forward Secrecy* (PFS). Furthermore, strictly certificate-based authentication is used to eliminate many security problems of *Pre-shared Key* (PSK)-based authentication algorithms.

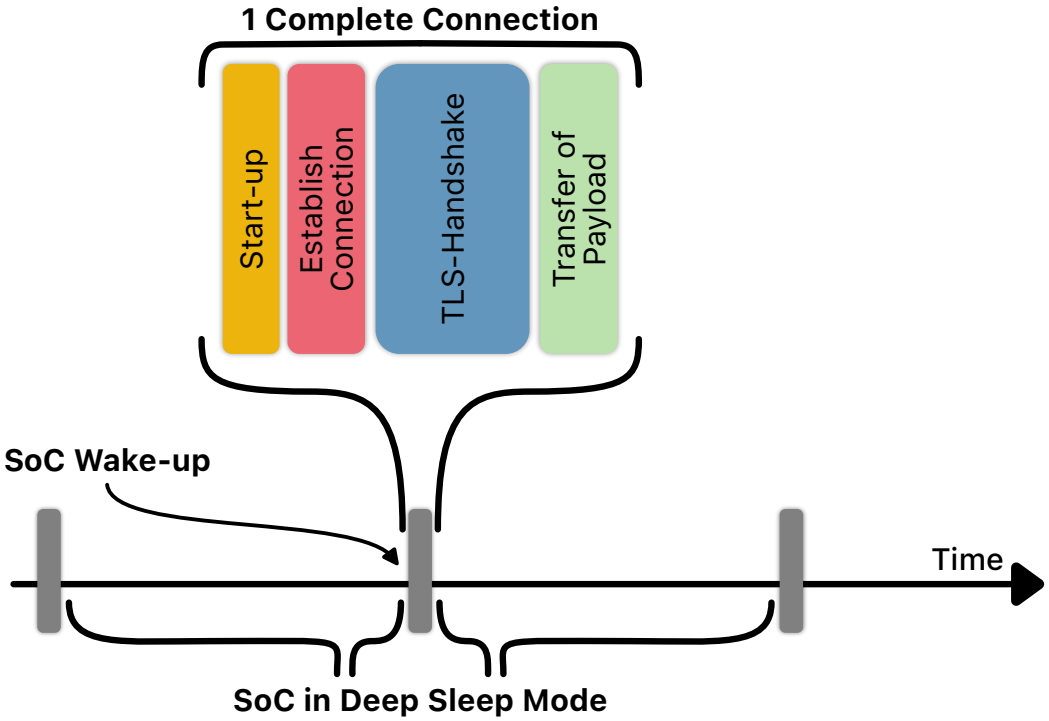

Figure 2.3: An Illustration of the Connection Interval between Edge Device and Server

[14] https://savannah.nongnu.org/projects/lwip/, accessed April 28, 2023
[15] https://www.trustedfirmware.org/projects/mbed-tls/, accessed April 28, 2023

2.4 Utilization of Hardware Accelerators

In the previous sections, a state-of-the-art Industrial IoT network system for the secure transmission of sensor data between edge devices and the cloud was proposed. In order to secure the data connection, the TLS protocol is used. However, the TLS protocol is practically non-existent in the low-power IoT domain. One reason is the relatively large amount of data that has to be transmitted to establish a secure connection; additionally, the required cryptographic calculations are considered too computationally intensive for embedded devices with limited resources [20–23, 93]. The utilization of a state-of-the-art SoC and dedicated cryptographic hardware accelerators, however, opens up new possibilities in contrast to the current state-of-the-art. The following section evaluates the general feasibility of the presented setup as well as the influence of specific cryptographic hardware accelerators.

2.4.1 Related Work

Related studies have analyzed the impact of various cryptographic algorithms, isolated without a network connection, on different microcontrollers, both with and without hardware accelerators: [100] examines the computing performance of three different microcontrollers with varying symmetric and asymmetric operations. Two of them employ internal hardware accelerators, but the analysis only covers time and not energy. In [101], the energy and time required to apply AES are analyzed on two different platforms, one of which includes a CHA. [102] compares the energy and computation performance of four different secure elements.

Other papers investigated cryptographic operations and protocols in combination with WLAN modules: [97] and [103] evaluated the complete TLS handshake with different ciphers based on RSA and ECC in terms of energy and time. [104] analyzes many different symmetric and asymmetric operations on various microcontrollers and external CHAs. [105] evaluates the performance of different crypto operations as well as the impact of a DTLS handshake on different microcontrollers in combination with a WLAN module. They report that the use of the integrated crypto accelerator has minimal impact on the application in terms of execution time and energy consumption.

2.4.2 Setup

For the evaluation, the setup described in Section 2.3 was used. The current consumption of the edge device was recorded with a Keithley DMM7510 digital multimeter. For the measurements, a sampling rate of 20 kHz and 0.1 µA resolution is used. The timings were measured and synchronized with the current measurements by using a high-speed logic analyzer. Furthermore, two different CHAs were used:

- ATECC508A [16]: This CHA from Microchip integrates all the necessary cryptographic functions for ECDSA and *Elliptic Curve Diffie-Hellman* (ECDH) Key Agreement. It supports the *National Institute of Standards and Technology* (NIST) standard P256 elliptic curve, SHA-256 hashing, and offers an internal random number generator. The device is connected to the edge device (nRF52840 SoC) via a standard *Inter-Integrated Circuit* (I2C) interface.
- Arm TrustZone CryptoCell-310 [17]: This security subsystem by Arm is directly integrated into the edge device (nRF52840 SoC). It offers a CHA for RSA public key cryptography as well as ECDH and ECDSA support utilizing different curves. Furthermore, other functions like SHA-2 hashing, a true random number generator, and AES symmetric encryption are provided by the accelerator.

To obtain the highest security level, as already described, the concept of PFS was applied with ephemeral encryption keys by employing the cipher suite *TLS ECDHE ECDSA AES 128 GCM SHA256* for all measurements. This means that each new connection is independent of previous ones and all necessary session data is generated from scratch. CHAs performed the following functions during the tests:

- ECDHE: Generation of a new key pair; Calculation of the shared secret
- ECDSA: Signing and Verification
- SHA-2: Hashing (CryptoCell only; Hashing is done in the software when using the ATECC508A)

2.4.3 Evaluation and Results

The results are segmented into three groups: plain software solution (SW), external hardware acceleration with the ATECC508 (HW_{AT}), and internal hardware acceleration using the CryptoCell (HW_{CC}). Figure 2.4 shows the time and energy overhead caused by the TLS handshake. Here, only the time and energy from sending the first message to establish the TLS connection to successfully establishing the secured connection was considered. The total handshake time is reduced to almost a quarter of the software-only solution when using one of the CHAs. In addition, the use of the external CHA (HW_{AT}) reduced the energy required by a factor of 10 compared to the software-only solution. When using the integrated CHA (HW_{CC}), the energy could even be further reduced by almost a factor of 2 compared to the external CHA.

Figure 2.5 shows different battery lifetime estimations of the sensor edge device, depending on the ECC implementation type and the number of MQTT connections

[16] https://www.microchip.com/en-us/product/atecc508a, accessed April 28, 2023
[17] https://www.arm.com/products/silicon-ip-security/crypto-cell-300, accessed April 28, 2023

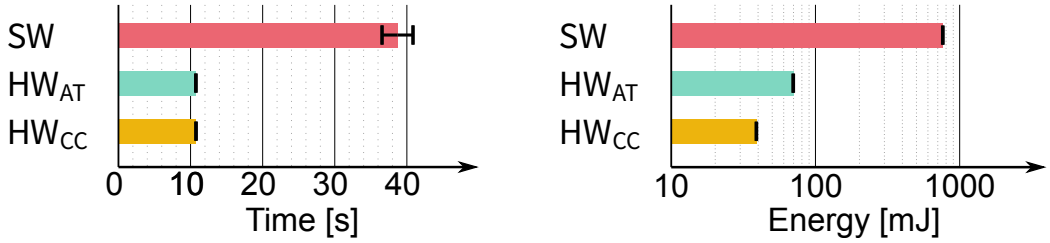

Figure 2.4: Handshake Overhead

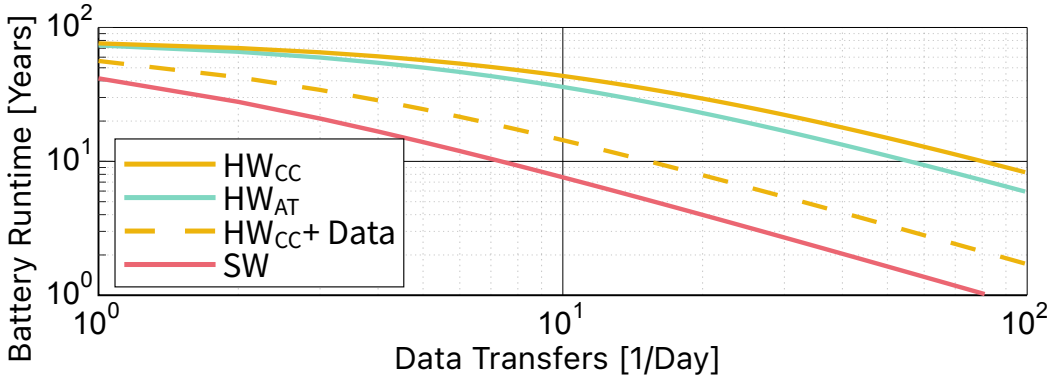

Figure 2.5: Battery Runtime Estimation

per day (see setup in Figure 2.3). Besides the handshake process, each connection includes a data transfer of 128 byte. The sleep current is 2.5 µA. An AA Lithium cell (thionyl chloride, 3.6 V, 2.6 A h) is employed as the battery, and 70% of its capacity is considered usable. Since the edge device in a real-world scenario usually requires additional energy for sensor value acquisition and processing, a corresponding example is added. The dashed line graph includes the sampling and preprocessing of vibration sensor data that takes about 20 s (consuming 300 mJ), prior to the connection establishment. Assuming a connection interval of 30 minutes, i.e. 48 connections per day, the theoretical battery runtime of less than one year can be increased to 10 years using the integrated CHA.

In summary, the results show that by using CHAs, the energy of the edge device used for a complete TLS handshake can be drastically reduced. Additionally in this setup, the integrated CHA is able to achieve significantly better results, which is partly due to the communication overhead for transmitting the data via I2C.

Moreover, it has been demonstrated that, in contrast to the state-of-the-art, TLS is already feasible for many applications by using a modern SoC in combination with a CHA.

2.5 Holistic Analysis Approach

In Section 2.4, it was shown that CHAs make TLS-based security feasible for battery-powered IoT edge devices. However, the expectable performance improvement utilizing CHAs for cryptographic computations is expected to be at least one order of magnitude [106], which is significantly higher than the achieved results that have been reported for TLS. The reason is that the cryptographic computations have been assessed and optimized in isolation and not in context with the overall TLS handshake procedure. Thus, neither further limitations of internal procedures like data handling and memory management nor interdependencies between the system components like gateway and server have been investigated. The following comprehensive analysis of the IoT network system leads to three new, main contributions. First, a detailed comparison of the software-only versus the hardware-accelerated implementation of the Industrial IoT network system. Secondly, the identification of further limiting factors and the corresponding optimizations led to a significant reduction in latency and energy consumption of the edge device. Thirdly, the analysis methods shown can be used to make a precise statement about the impact on energy and handshake duration of different cryptographic procedures (demonstrated here with the example of 3 different key lengths).

2.5.1 Procedure and Methodology

In the analysis of the system, the following methods and techniques are used to allow a holistic analysis of the system. Furthermore, common reference points are used to synchronize the different analyses in time to gain further insights into the system.

- ***General Purpose Input/Output* (GPIO) Pins and Logic Analyzer**
  By setting and clearing GPIO pins at significant points in the program and logging these with an external logic analyzer, very precise statements can be made about timings within the program. Since writing a GPIO pin requires only a few CPU cycles, the impact on the program is extremely small and in addition, the time measurements are very accurate. For the experiments, a *Logic Pro 16* logic analyzer by Saleae[18] is used.

- **Current Measurement**
  Since the main goal of this analysis is to reduce the energy demand of the edge device, the accurate measurement of the required energy is very important. This allows the detection of energy-intensive sections in the program and increased energy consumption in standby mode. In addition, by comparing the energy values with specifications from the manufacturer, it is possible to determine the operating mode of the microcontroller and the enabled peripherals.

[18] https://www.saleae.com, accessed January 16, 2023

This allows the identification of unused but activated peripherals. The synchronization with the logging of the GPIO pins allows an even deeper insight into dependencies and reveals precise information about the energy consumption of certain program passages, e.g. the generation of a key pair or the signing of a message. In the experiments, a Power Profile Kit II by Nordic Semiconductor[19] and a Keithley DMM7510 digital multimeter[20] are used.

- **System Logs**
  On the edge device as well as on the server and the gateway, log outputs can be used to inform about errors and system status. This can be used to detect problems such as timeouts or protocol errors. However, the output of text, e.g. via an *Universal Asynchronous Receiver Transmitter* (UART) connection, particularly on the edge device, can have a significant impact on energy consumption and timing. Therefore, the use of this function on the edge device is only advisable in the early phases of optimization and analysis.

- **Network Analyzer**
  A network analysis tool such as Wireshark[21], which runs on the gateway or an external device and captures the entire network traffic, is extremely useful for examining connection establishment, IP address management, and message flow. This allows, for example, retransmissions of messages or delays in corresponding reactions to be tracked.

2.5.2 Types of Optimizations

Based on the aforementioned analysis methods, several optimization options were identified that have a major impact, especially after the acceleration of cryptographic computations with a CHA.

1. **Application Code Optimization**
   Dynamic memory management offers various advantages in many applications. Especially for resource-limited devices with limited RAM size, static memory allocation is often not suitable. However, the system can benefit significantly from sporadic, permanently allocated static memory areas (memory reuse) in the case of constantly recurring memory allocations. Another optimization in the area of application code is the strict avoidance of active polling, e.g. while activating a resource, switching on clocks, or similar.

[19] https://www.nordicsemi.com/Products/Development-hardware/Power-Profiler-Kit-2, accessed January 16, 2023
[20] https://www.tek.com/de/products/keithley/digital-multimeter/dmm7510, accessed January 16, 2023
[21] https://www.wireshark.org, accessed January 16, 2023

Through the use of sporadic memory reuse and the reduction of active polling during startup, both the required energy and the duration of the handshake could be reduced.

2. **Device Specific Optimization**
   As SoCs continue to become more complex with additional features and components, it is getting increasingly difficult to enable only the necessary hardware resources. Unused but activated peripherals such as counters, clocks, or interfaces can, however, have a considerable influence on the energy consumption of the SoCs.

   In this case, deactivating unused resources and timers led to a further reduction in the energy required.

3. **Optimization of System Interdependencies**
   Especially in network-dependent systems, the coordination between the network participants can have a considerable influence on the overall performance of the system. A standard server, for example, expects by default a very fast response to sent IP packets. However, a resource-constrained edge device may not always be able to achieve fast responses due to its significantly lower computing power. Retransmissions and a resulting higher data and energy demand are the consequences.

   By improving the coordination and adjusting the server-side retransmission timeout, multiple retransmissions were avoided, resulting in significant energy and time savings.

4. **Optimization of Connection Parameters**
   The parameters of the network connection, such as the BLE connection interval or transmit power, have a significant impact on latency and data throughput. However, the increased activity of the radio can also directly influence energy consumption. A detailed study of the effect of BLE connection parameters was conducted by my colleague Carl C. Rheinländer and published in [26].

2.5.3 Evaluation and Results

The comparison between the purely software-based solution (SW) and the in Section 2.4 presented hardware accelerated solution (HW iso.) shows the significant influence of the CHA on the cryptographic operations (Figure 2.6 top). In relation to the total handshake time, the impact of the cryptographic operations can be significantly reduced (a decrease from approximately 80% of 38.5 s to about 1.6% of 10.5 s). By addressing the cryptographic operations in isolation, the total duration of the handshake could be improved by a factor of 3.5. The identified optimization potentials resulted in a reduction of the overall TLS handshake latency by about one order of

magnitude, i.e. a factor of about 30 between the original software-only solution (SW) and the optimized hardware-accelerated solution (HW hol.).

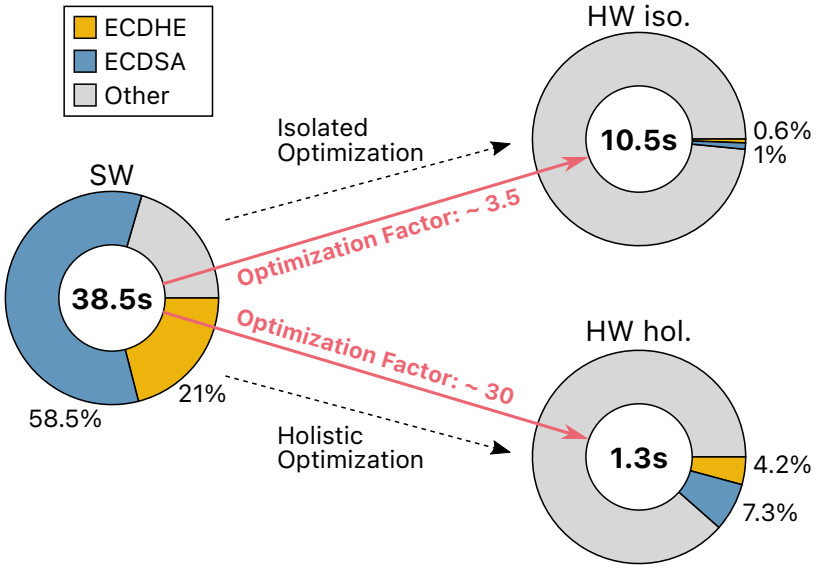

Figure 2.6: Optimization Approaches of the TLS Handshake Latency, split up in DSA and DHE Execution Times [26]

The energy demand in the isolated optimization approach, shown in Figure 2.7 on the left, is already reduced by more than one order of magnitude compared to the software-based solution (SW). This is mainly due to the fact that most of the energy in the software-based implementation is caused by the CPU being fully occupied during the cryptographic computations. By using a CHA to perform them, the CPU utilization can be drastically reduced. The holistic approach, moreover, resulted in an even further reduction of more than 60 %.

The precise system analysis of the edge device during the TLS handshake also enables an evaluation in terms of energy and time, of the influence of the selected cryptographic procedures. Figure 2.8 shows the influence of different key lengths (secp256r1, secp384r1, secp512r1) as one example. The right part of Figure 2.8 reveals that both, the computational effort (CHA Active) and the time required to transfer and process the larger keys (included in Other) increase significantly. Analyses of many other parameters and methods, primarily with respect to post-quantum secure cryptography, based on the same setup have been published by my colleague Maximilian Schöffel in [28] and [29].

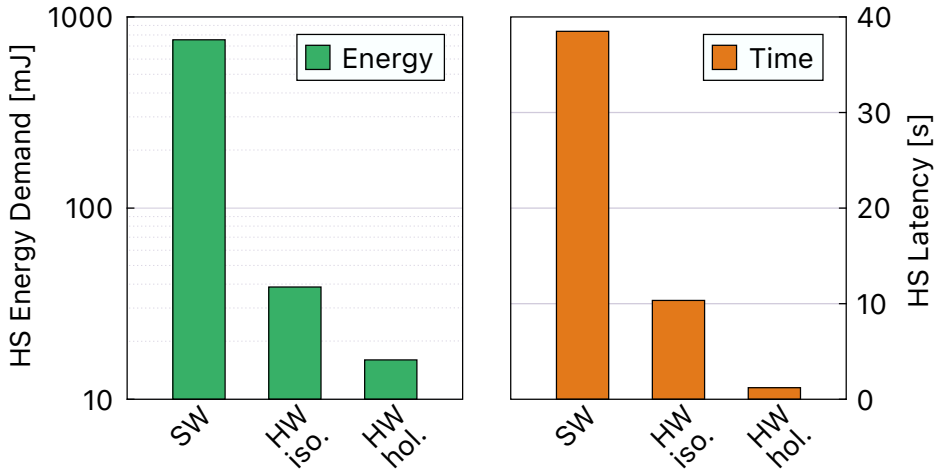

Figure 2.7: Energy Demand and Latency for the TLS Handshake Procedure in Comparison [26]

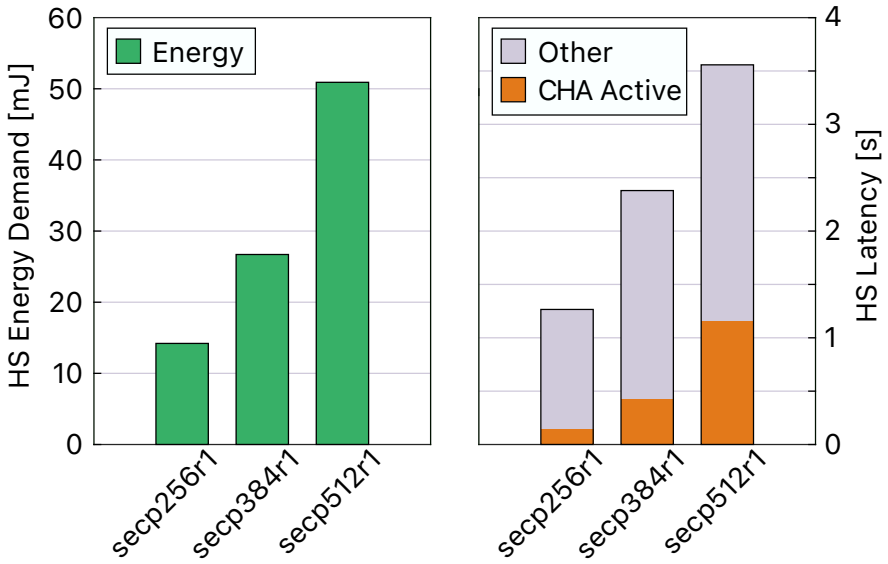

Figure 2.8: ECC Curve-Related Energy and Latency for the TLS Handshake Procedure [26]

2.6 Challenges of the Utilization of TEGs

The previous sections have focused on the systematic analysis and enhancement of the Industrial IoT system. The results are a significant reduction in the energy consumption of the edge device and a deep understanding of the temporal and energy impact of the different phases of connection establishment. These accomplishments could potentially facilitate the elimination of regular maintenance intervals caused by battery replacement by using energy harvesting solutions instead. Solar-powered wireless sensor nodes have already been shown to be a viable and practical solution for many applications. In direct sunlight, solar cells can quickly generate over 20 mW/cm^2, which is why even very small solar modules are often already feasible for powering a sensor node. However, the use of solar cells severely limits the operating environment to locations with sufficient light. This restriction also applies to the predictive maintenance use case described in Section 2.1, as these pumps are often installed in buildings, basements, or deep within process plants. However, there are many other energy harvesting solutions such as electromagnetic energy harvesting, piezoelectric crystals, or TEGs. In particular, TEGs, which convert a temperature gradient into electrical energy, are a viable option for the stated use case. Here, the radiated heat from the pump motor can potentially be used to power the edge device. However, due to their intrinsic thermal connectivity and the absence of active cooling, only low-temperature gradients can be expected, resulting in only a low energy yield. The conditions under which TEGs are suitable for operating the in 2.3 presented, representative Industrial IoT edge devices as well as the influence of different intermediate storage technologies are examined in more detail below.

The results and findings as well as isolated text passages in this section have already been published by me and my colleagues in the conference paper titled "Exploration of Thermoelectric Energy Harvesting for Secure, TLS-based Industrial IoT Nodes.“ presented at "International Conference on IoT (ICIOT 2022)" [27].

2.6.1 Related Work

Energy harvesting describes the conversion of energy from environmental sources into usable electrical energy. Commonly used energy sources are light (photoelectric effect), kinetic energy, chemical energy, radio frequencies, and thermal energy [107]. A TEG uses the Seebeck effect to transform thermal energy into electrical energy. This effect describes the phenomenon in which a voltage difference is created by the temperature difference between two different electrical conductors or semiconductors. Both the structure and the employed materials have an essential influence on the properties of the TEG [108–110]. The voltage generated by a TEG is usually in the range of millivolts. In order to utilize this small voltage difference, special boost converters are applied to generate a voltage level that can be used for embedded devices. The design of these booster circuits and their adaptation to the characteristics

of the TEGs have a considerable influence on the efficiency of the system [111–113]. Therefore, off-the-shelf modules consisting of a TEG and a precisely matched booster circuit are available to achieve maximum efficiency at a given operating point [114]. In the past, small-scale thermoelectric energy harvesting has been presented to supply wearable sensor devices [115, 116] and IoT applications [117–119].

Another important key component of the system is an energy storage element. The output power of small TEGs is mostly insufficient to directly power a microcontroller with an active radio, especially at low-temperature gradients. Therefore, the energy is typically initially collected in a storage element until enough energy is available to operate the unit for a specified time [120, 121]. The type of storage element is strongly application-specific. Thus, size, capacity, lifetime, leakage current, pulse-current capability, and cost are only a few of the decisive factors [120]. Typically, either small rechargeable batteries or supercapacitors are used.

2.6.2 Setup

In the following, an overview of the system setup that is used in the remainder of this chapter is presented. This includes the software components on the edge device, the energy harvesting module used, and the energy storage solutions considered in the study.

Edge Device Software

Similar to the previous sections, the Industrial IoT setup already presented in Section 2.3 was used. In this case, however, the software of the edge device is based on the RIOT operating system [122] and its default GNRC Network Stack. The use of this very resource-efficient and modular build operating system enables a more generic software application due to the additional abstraction layer, compared to the previously used bare metal software stack without an operating system. After a holistic system analysis and corresponding optimization as described in Section 2.5, the energy and latency values achieved with the RIOT-based software were comparable to those of previous measurements. The use of mbedTLS as a TLS library and a simple MQTT client as an application layer remains unchanged.

Energy Harvesting Module

As already mentioned in the related work 2.6.1, the matching between TEG and the booster circuit has a significant impact on the overall performance of the energy harvesting module. Therefore, a class-leading, off-the-shelf energy harvesting module called Prometheus by Matrix Industries [114] is used in the system. The compact module consists of a TEG (MATRIX Gemini) and an energy-harvesting boost converter

(MATRIX Mercury). Although the power expected at a given temperature is well documented in the Prometheus module datasheet for larger temperature differentials, it is not documented for small temperature gradients. In the targeted use case, however, only small temperature gradients (<5 K) can be expected, mainly due to the fact that the environmental temperature will be close to the temperature that the industrial appliances, which are to be monitored, emit. Section 2.6.3, therefore, presents an analysis of the performance of the TEG at small temperature differentials.

Energy Storage Technologies

The property that the system only establishes a connection at certain intervals and enters a deep sleep mode in between, allows the use of a significantly less powerful energy harvester and significantly lower temperature differences. This involves scheduling an energy storage element between the harvester and the edge device to accumulate the energy required to establish a full connection in the time between two connections. The capacity of the energy storage device, however, must be precisely matched to the application. It must be high enough to power the device during the lowest power incomes from the harvester, and low enough to quickly reach the minimum operation voltage even with little charge energy. This is particularly essential in systems with extended periods without active energy harvesting by the harvester.

Energy storage elements differ in their capacity, energy density, cost, maximum current output, and losses due to leakage and aging. To define the most suitable storage technology for the targeted IoT system the following energy storage technologies are evaluated in this work:

- ***Multi Layer Ceramic Capacitor* (MLCC):**
  This capacitor consists of a ceramic material that serves as a dielectric and is capable of delivering very high peak currents. Usually, the capacitance of a single capacitor is limited to a few tens to hundreds of microfarads, which is why several capacitors must be connected in parallel if larger capacitances are required. For this setup, twenty MLCCs from the manufacturer Taiyo Yuden, with a capacity of 220 µF each, connected in parallel for a total of 4.4 mF, are used.

- **Supercapacitor:**
  Conventional capacitors usually have a relatively high leakage current, which leads to unwanted energy losses. Supercapacitors, however, are optimized to have low leakage currents and feature a significantly higher capacitance density. But, they typically have a relatively high internal resistance, which causes the voltage to drop significantly at high current pulses. For this setup, one 100 mF supercapacitor by Eaton (KR-5R5V104) is used.

- **CeraCharge:**
  The CeraCharge is a solid-state SMD battery by TDK. Its capacity is around 200 mF at a maximum voltage of 1.8 V. The leakage currents to be expected are extremely low, but high peak currents are not possible due to the high internal resistance. An advantage over capacitors is the non-linear curve in terms of voltage and discharge capacity, which means that theoretically more usable energy is available until the voltage drops below a certain point. However, in this setup, a 440 µF MLCC had to be added in parallel to the CeraCharge in order to compensate for the high peak currents and to prevent large voltage drops which would result in a power-on reset of the SoC. Since the edge device runs with a maximum voltage of 3.6 V, two CeraCharge cells are connected in series.

The energy output of the TEG is expected to be relatively low due to its intrinsic thermal connectivity and lack of active cooling, resulting in a rather low-temperature gradient. Consequently, the energy storage component experiences many charge and discharge cycles. Classical electrochemical storage technologies such as Li-ion batteries are less suitable for this purpose as they suffer from severe aging effects, which is why they have not been included in this work.

2.6.3 Evaluation and Results

In this section, first, the requirements of the edge device are defined in more detail. Next, the amount of energy that can be expected from the energy harvesting system is analyzed. This is followed by a detailed investigation of different energy buffers and their trade-offs in this application. Finally, the results are summarised in a graph showing the minimum time between two connections to harvest the required energy as a function of the temperature gradient and the storage technology used.

Energy Requirements of the Edge Device

To determine the energy demands of the edge device during a single connection, precise current measurements were taken from the first power-up of the SoC until the successful transfer of the payload. Due to the modularity of the TLS handshake, two further key exchange methods were included as examples of post-quantum safe methods for further analysis, making a more general statement about the energy consumption of the edge device possible. The values of the handshakes using KYBER512 are based on the work of my colleague Maximilian Schöffel. A more detailed description and a much larger selection of post-quantum safe procedures have been published by us in [28, 29].

The application running on the edge device can be divided into the following functional sections, 2.9:

- start-up of the microcontroller (1)
- establishment of a BLE connection to the gateway (2)
- execution of the TLS handshake with the MQTT server, including the cryptographic calculations (3)
- transmission of 100 bytes of user data (4)

The resulting current profile of such a connection at a supply voltage of 3.6 V is shown in Figure 2.9. Each functional area is marked with the corresponding number.

In Table 2.1 the average duration and energy requirement of a complete connection, broken down by the different key exchange methods used, are listed. ECDHE-ECDSA represents the conventional state-of-the-art solution based on elliptic curves. KYBER512-ECDSA deploys the recently standardized post-quantum key encapsulation method, signed by conventional elliptic curve cryptography. KYBER512-DILITHIUM2, thus establishing a fully post-quantum secure connection based on KYBER [123] and DILITHIUM [124].

The system enters a deep sleep mode between connections and is woken up by an external real-time clock (e.g. RV-3028-C7 from Micro Crystal[22]). This allows the current required during this time to be less than 500 nA.

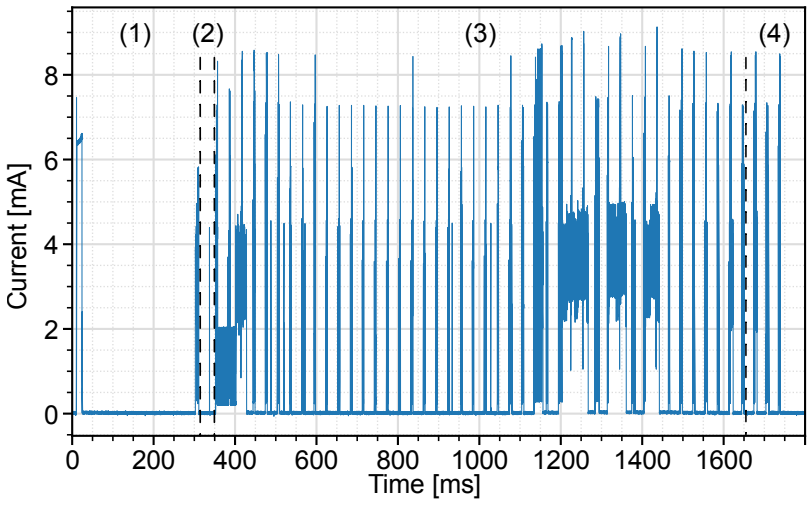

Figure 2.9: Current Profile of a Complete Connection [27]

[22] https://www.microcrystal.com/en/products/real-time-clock-rtc-modules/rv-3028-c7, accessed April 28, 2023

Table 2.1: Energy and Time Requirements of Different Key Exchange Methods (Mean Values of 10 Measurements)

Key Exchange Method	Energy [mJ]	Time [s]
ECDHE-ECDSA	5.90	1.71
KYBER512-ECDSA	6.44	2.18
KYBER512-DILITHIUM2	17.98	6.51

Energy Harvesting Module

The analyses of the TEG module were performed by my colleague Carl C. Rheinländer and published in [27]. As the results of the maximum power output as a function of the temperature difference are an essential part of the subsequent analysis of the overall system performance, the results are included here for the sake of completeness.

Figure 2.10 shows the measurement setup for measuring the energy at certain temperature differences. The temperatures are controlled on one side by a heated water bath and on the other side by a heat sink exposed to the environmental temperature. The resulting graph of the maximum output power of the TEG at a given temperature difference is shown in Figure 2.11.

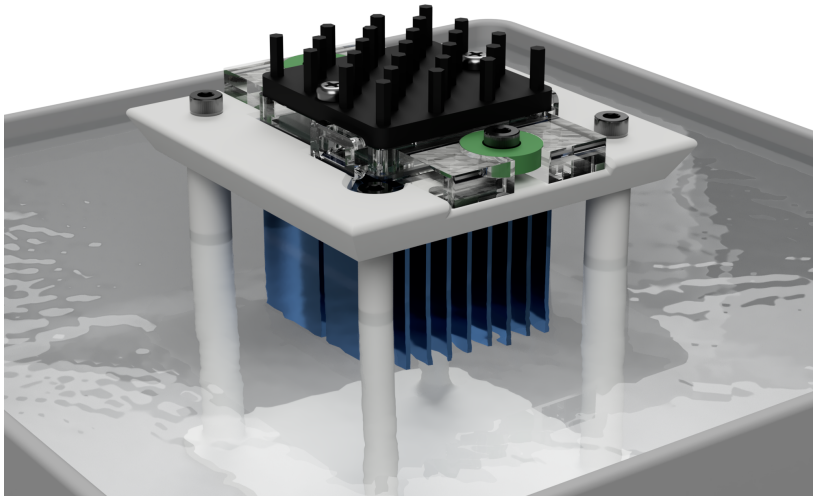

Figure 2.10: Test Setup for the Evaluation of the TEG Module [27]

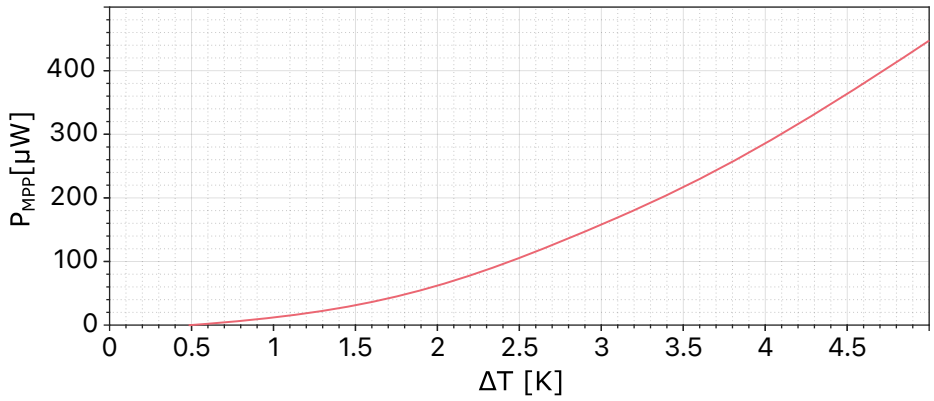

Figure 2.11: Maximum Output Power of the TEG Module [27]

Energy Storage Technologies

In order to determine how much of the energy stored in the storage devices can actually be used by the edge device, the respective discharge profiles were captured without a harvesting system connected. Therefore, the storage units were charged to 3.6 V in order to supply the IoT application. A minimum operating voltage V_{min} for the presented IoT application of 1.8 V was defined, which was derived from the minimum operating voltage specified in the datasheet of the employed BLE SoC plus a headroom of 100 mV. For the sake of simplicity, a high-duty cycle of the IoT application was chosen for this analysis with a new connection every 10 s. This way the losses through leakage will be low and can be neglected for the calculation, but at the same time, a good statement can be made about the usable energy in the buffer.

Figure 2.12 shows the discharge curves of the MLCC. Its capacitance of 4.4 mF of the MLCC is sufficient for 2 complete connections. It is noticeable that due to the low

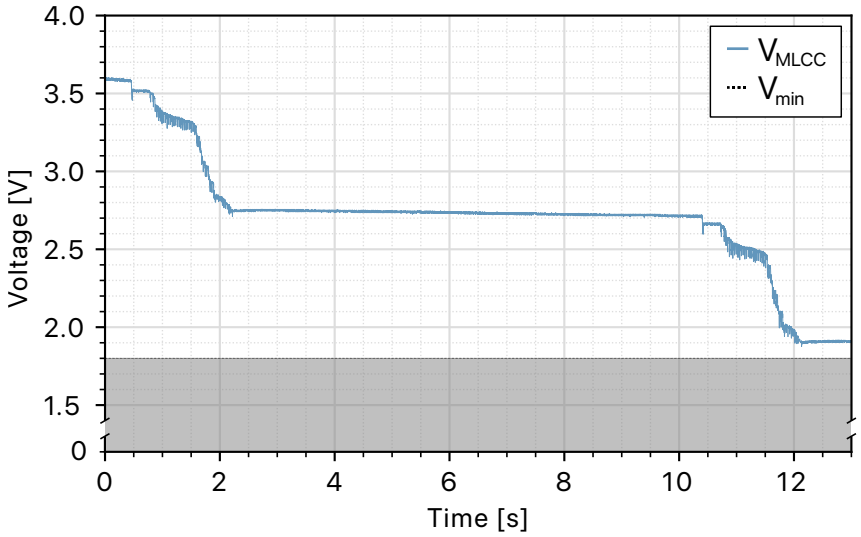

Figure 2.12: Discharge Curves of the MLCC; New Connection every 10 s [27]

internal resistance, there are practically no voltage drops caused by the peak currents, but only a linear drop in relation to the drawn energy. This means that the energy stored in the MLCC can be used very efficiently up to the defined minimum operation voltage of 1.8 V.

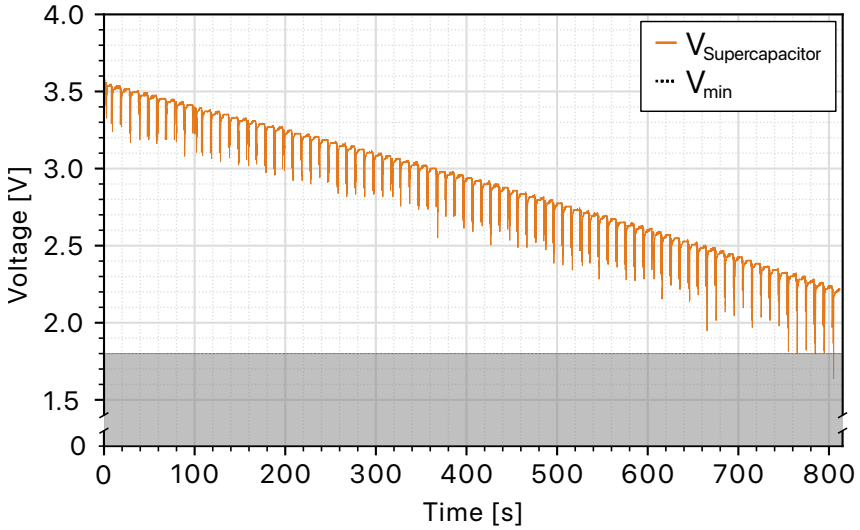

Figure 2.13: Discharge Curves of the Supercapacitor; New Connection every 10 s [27]

Figure 2.13 shows the discharge curve of the supercapacitor. With its capacity of 100 mF, it provided the energy for 83 successful connections. The high peak currents cause voltage drops that increase significantly with decreasing storage voltage to almost 0.6 V at a remaining storage voltage of 2.2 V. As a result, the supercapacitor can only reliably supply the application down to a remaining open loop voltage of 2.2 V, compared to the MLCC, which can be used down to 1.8 V.

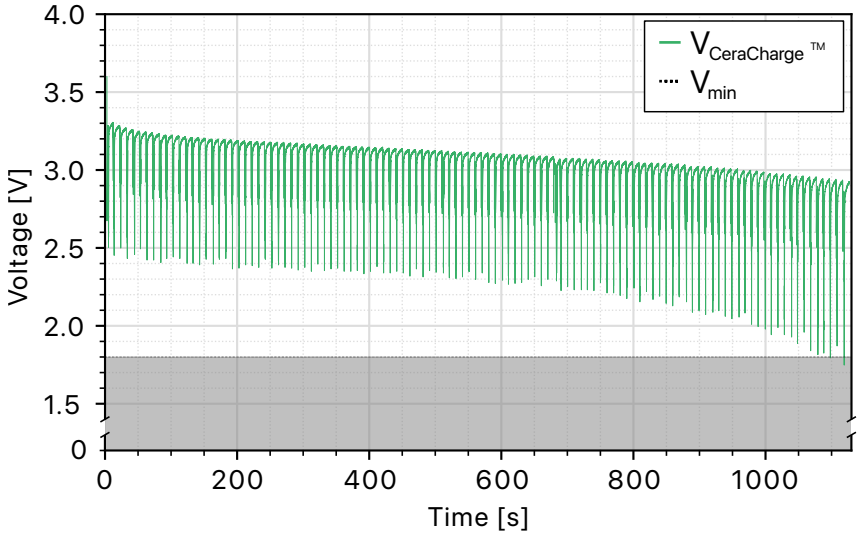

Figure 2.14: Discharge Curves of the CeraCharge with a 440 µF MLCC in parallel; New Connection every 10 s [27]

Compared to the supercapacitor, the CeraCharge has an even higher internal resistance and was not able to supply the peak currents required in the setup on its own. Therefore, two 220 µF MLCCs were connected in parallel to slightly absorb the peak currents. This allowed the CeraCharge, whose discharge curve is shown in Figure 2.14 to successfully supply the energy for 113 connections before the voltage drops below 1.8 V by a remaining open loop voltage of 2.9 V. In contrast to the MLCC and supercapacitor, the voltage curve of the CeraCharge is not linear with respect to the energy consumed but instead drops much slower, which, in principle, leads to a larger usable range. However, the strong voltage drops caused by the high internal resistance outweigh this advantage.

Based on the energy of the fully charged storage device and the residual energy at the point of the determined minimum open-circuit voltage, the maximum theoretically usable energy of the storage technology, E_{usable}, can be calculated as follows:

$$E_{usable} = E_{chg} - E_{res} = 0.5 \cdot C \cdot ((3,6V)^2 - V_{OLmin}^2) \quad (2.1)$$

Where E_{chg} is the stored energy of the respective buffer at the point where it is fully charged to 3.6 V and E_{res} is the residual energy in the buffer at the point where the minimum voltage under load conditions can be guaranteed. V_{OLmin} is the respective open loop voltage at this point. Regarding the MLCC, this reveals that about 75 % of the stored energy is usable by the IoT application. As far as the supercapacitor is concerned, about 55 % are usable. The CeraCharge reaches a rate of approximately 51 % of usable energy, whereby it must be noted that, as previously mentioned, a 440 µF MLCC had to be connected in parallel for this. This value for the CeraCharge is only an approximate value because the usable capacity strongly depends on the quantity and duration of the load. As shown above, the IoT system load consists of many different current pulses, which makes it almost impossible to theoretically determine the exact usable capacity. Furthermore, the open-circuit voltage of the CeraCharge dropped significantly after applying the load for the first time, which makes it more difficult to compare to other storage technologies.

Another important parameter of the various storage technologies is the leakage current, which is dependent on a variety of parameters. While the design of the storage unit and the materials used certainly have a major influence, parameters like, for instance, the ambient temperature, age, cycle count, and installation parameters can also have a significant impact. In this case, the values from the data sheets are used as a rough guideline for comparison. The values that are applied for subsequent calculations are thus 2 µA per MLCC (i.e. 40 µA for the twenty MLCCs connected in parallel), 0.6 µA for the supercapacitor, and 0.1 µA for the CeraCharge. For the CeraCharge, however, the leakage of the two MLCCs connected in parallel must also be taken into account, which increases the leakage to 4.1 µA in this case. Figure 2.15 shows the results for the different storage technologies deployed in this study.

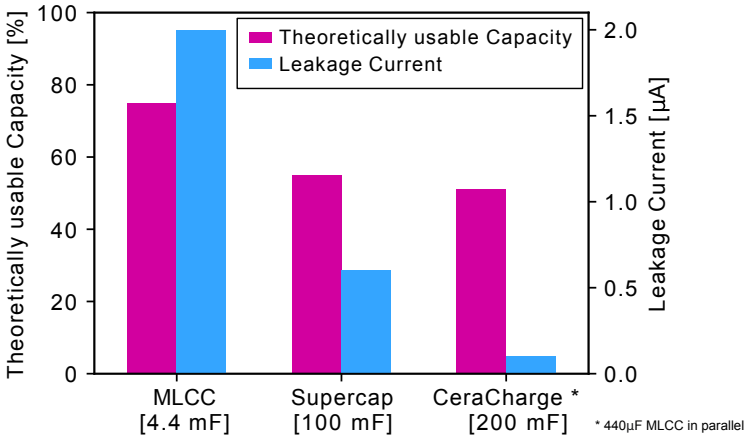

Figure 2.15: Comparison of the different Storage Technologies with respect to the theoretically usable Capacity and the Leakage Current [27]

For a qualitative comparison of the storage technologies in general, Figure 2.16 illustrates the different typical characteristics. All axes are arranged in such a way that the preferred path points outwards, e.g., low costs, high endurance, and high pulse current capability. The values only serve as a rough classification of the storage technologies and show the general advantages and disadvantages. MLCCs are ideal for absorbing large current peaks, have exceptional endurance, and can even be charged with large currents. The supercapacitors, on the other hand, are a good compromise in many areas with the advantage of their low cost in relation to capacity and their very high endurance. The outstanding features of the CeraCharge are the extremely low leakage current and the comparably high density. But in return, the CeraCharge is not capable of handling large pulse currents. In addition, the handling of the CeraCharge is more complex due to specific characteristics such as limited charge current.

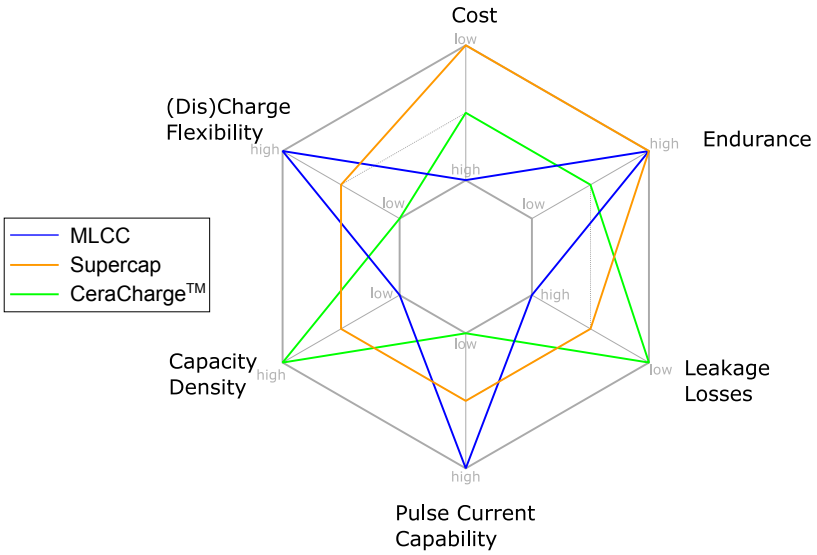

Figure 2.16: Overview of the Properties of the different Energy Storage Technologies [27]

Results in the System Context

By combining all the optimizations, insights, and results from the previous chapters, the minimum time required to generate the energy for one connection can be calculated as a function of the temperature gradient at the TEG (Figure 2.17). The leakage of the respective storage technologies is thereby also taken into account. Thus, the graphs indicate a lower bound at which the charge of the energy storage technologies remains constant over a long period of time. The dots at the right ends of the graphs indicate the minimum temperature gradient to overcome the leakage of energy storage technologies. Due to the very similar energy requirements of ECDHE and the post-quantum-safe KYBER512, the curves are almost congruent. The post-quantum secure signature method DILITHIUM2 has a significantly greater influence due to the large keys and signatures which strongly increases the amount of data being exchanged between client and server. The results clearly indicate the influence of the leakage current of the individual storage technologies. For example, in order to generate the energy for establishing a connection in 20 min, a temperature gradient of 3 K is required when using MLCCs, whereas a temperature gradient of only 1 K is required when using a supercapacitor.

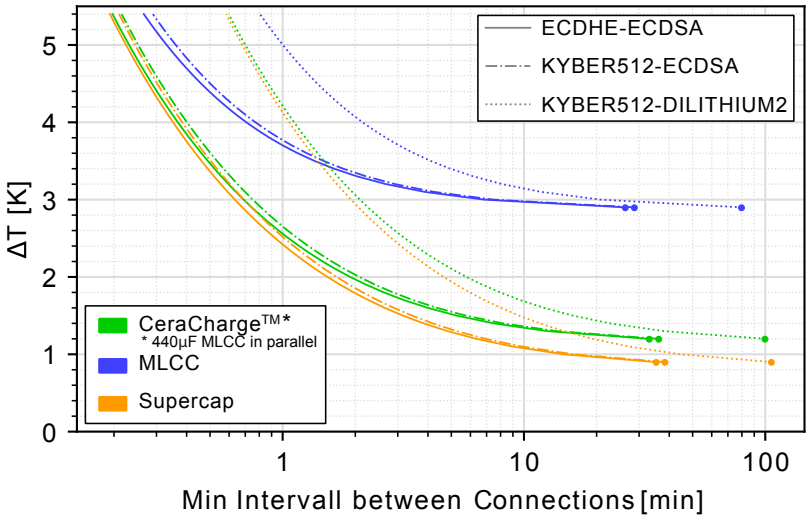

Figure 2.17: Temperature Gradient vs. minimal Time between Connections [27]

This chapter demonstrates that thermal energy harvesting, in combination with an appropriate intermediate storage device, is a reliable method for establishing a secure data connection to the cloud, even at low-temperature differences of just a few Kelvin. The use of energy harvesting instead of batteries or dedicated wiring significantly reduces the installation and maintenance effort and thus creates significant added value both in Industrial IoT and in other application areas such as smart homes.

2.7 Limitations

It is essential to mention that the consideration of the security aspect here only refers to applying the TLS protocol. Even though this protocol contains mechanisms for identification, authentication, confidentiality, and integrity, numerous other aspects must be taken into account to achieve the maximum possible security for the system. Nevertheless, the use of the TLS protocol provides an extremely versatile foundation which, when properly implemented in combination with mechanisms such as, for example, secure boot, an appropriate PKI infrastructure, and secure software updates, can provide a practice-oriented system that meets high-security standards.

2.8 Further Scientific Research Based on this System

Due to the modular structure of the software stack and the systematic use of standards, the system serves as an excellent platform for further research. The deep diagnostic and analysis techniques are a further advantage for the evaluation and analysis of new components. The system is therefore also used in research about post-quantum secure algorithms on embedded systems with very limited resources. This research, conducted by my colleague Maximilian Schöffel, serves for in-depth investigation of PQC algorithms on low-power embedded devices and adds significant value to ongoing standardization processes such as that of the US NIST. In [28], the system presented here was extended by potential post-quantum key-encapsulation mechanisms, and their impact in terms of energy and latency was analyzed and compared. In [29], additional potential post-quantum digital signature algorithms were implemented and also evaluated in terms of energy and latency.

Chapter 3

Data Acquisition - Educational IoT

In recent years, there has been a significant shift from traditional, basic learning environments to the dynamic and innovative realm of smart learning environments. This transformation is driven by the increased connectivity and the integration of advanced sensor technology into the individual objects of learning environments. Hence, this concept is also referred to as Educational IoT. Learning environments are commonly utilized, e.g., in STEM education, to impart not just facts to students but also ways of thinking and conceptual connections. This is often accomplished through the use of inquiry learning, in which students use experiments and research processes to construct knowledge [125]. While physical and hands-on laboratory experiments that focus on inquiry learning offer distinctive experiences, pure physical laboratories may not always lead to successful learning outcomes [126–130]. Complex research procedures and experiments can cause cognitive overload for the learner, hampering the learning process. Nonetheless, personalized guidance and suitable pedagogical support can mitigate this issue [131, 132].

In this context, modern, intelligent learning platforms can provide significant added value and open up completely new possibilities. Embedded sensors and networking enable the capture of detailed information about both the learner and the learning platform itself. This enables much more complex, immersive, and sophisticated learning platforms, in-depth analysis, and new study design, as well as highly personalized support methods. Additionally, the accessibility of this data stream serves as the foundation for using AI-based methods and analytics. In addition to the need to capture specific parameters and states, there are also various requirements for accuracy, latency, robustness, usability, and cost depending on the application. Consequently, such an intelligent learning environment transforms into a complex multi-sensor platform with sophisticated networking features, which poses considerable challenges for its design and development.

The further course of this chapter is structured as follows: First, the scientific key contributions proposed in this chapter are listed. This is followed by a short overview of the theoretical background of learning theories with a focus on *Cognitive Load*

Theory (CLT), *Cognitive Theory of Multimedia Learning* (CTML), and learning with *Multiple External Representations* (MER). Section 3.2 subsequently introduces the first of the two learning platforms. This consists of smart sensors for electrical experiments for primary use in AR environments. The focus here was set on the installed sensor solutions consisting of a measuring system for current and voltage, a cable tracking system, and a 2D positioning system for tracking the experiment components. In addition to the functionality of the sensor solutions, an evaluation of the solution is presented in the respective sections. Furthermore, the data transmission between the devices is explained. In Section 3.3 a smart measurement platform for photometric experiments for use at schools and universities is presented. Unique to this system is the integrated photometric measurement unit and the ability to accurately track all moving objects on the learning platform. After the functional description of the sensor technology, an evaluation of the measurement system follows. In Section 3.3.6, the corresponding digital twin is presented.

This chapter proposes the following new key contributions:

- A smart sensor system for educational STEM experiments in electrical circuits focused on usage in an AR environment is presented. It consists of sensors for voltage and current measurement, position identification with a focus on a 2D plane, and cable identification for circuit reconstruction.
- A portable photometric measuring system with smart electronics and various sensors for inquiry-based learning in STEM lessons called *Smart Education Photometer* (SmaEPho) is introduced.
- An energy-efficient and robust data connection between the system components through the use of the widely utilized BLE standard is presented.
- An evaluation of the installed sensor systems in terms of accuracy and precision.

3.1 Theoretical Background on Learning Theories

The learning environments presented in the following sections were primarily developed and used to address research questions related to CLT, CTML, and learning with MER. This work will focus on the technical concept and the associated challenges. To provide a better understanding of the individual design decisions and requirements, however, a brief and limited overview of the learning theory background is given in the following. Further comprehensive insights can be found in the distinct papers and the dissertation of Sebastian Kapp [133].

3.1.1 Cognitive Load Theory

The fundamental premise of the *Cognitive Load Theory* (CLT) [134, 135] is that learners have a restricted working memory. Within this working memory, learners must process all information associated with the learning process in the form of elements and integrate them into their long-term memory, which is assumed to be unlimited. In the CLT, the learning process that is continuously related to cognitive load is classified into three types:

- *Intrinsic Cognitive Load* (ICL) is caused by the inherent complexity of the learning content itself. Any learning material used has an inherent level of difficulty and complexity that places a mental load on the learner [136]. The content to be learned can be seen as individual elements. Element interactivity, therefore, describes, on the one hand, the number of elements that must be kept active in working memory at the same time in order to fully understand a particular content, and on the other hand, the number of references between these elements. Accordingly, a high element interactivity indicates a high ICL. However, learners' prior knowledge significantly influences their learning process. Individuals with extensive background knowledge can combine many independent, previously acquired elements into chunks for processing. By reducing the number of discrete elements, the cognitive load is reduced, which in turn makes the cognitive load dependent on the learner's prior knowledge.

- *Extraneous Cognitive Load* (ECL) refers to cognitive load that is not relevant to learning, caused by suboptimal design of learning materials. The combination of relevant and irrelevant content within the learning material places additional demands on the learner by requiring the learner to first differentiate and classify the content. Appropriately optimized learning materials, utilizing design principles such as for example the split-attention-effect [137–139], can significantly contribute to reducing ECL.

- *Germane Cognitive Load* (GCL) is considered to be a positive load for the learner. It reflects the load on the learner's actual learning process in order to understand the information presented and to form schemas in long-term memory. A conscious reduction of ICL and ECL can support this process.

To assess cognitive load in educational laboratory settings, for instance, a questionnaire developed by Thees et al [140] can be used.

3.1.2 Cognitive Theory of Multimedia Learning

Cognitive Theory of Multimedia Learning (CTML) posits that a learner processes information through two distinct channels: verbal or textual representation, and graphical or visual presentation. By presenting information simultaneously through multimedia content, the content can be better processed and learned. Additionally, there is a broad alignment with CLT. As with CLT, CTML presupposes that learners have limited working memory and near-unlimited long-term memory. Additionally, it distinguishes between three types of cognitive processes: essential processing (similar to ICL), extraneous processing (similar to ECL), and generative processing (similar to GCL). A principle developed in the context of CTML to reduce extraneous processing is the multimedia principle [141, 142], which states that learning with a combination of images and text is superior to learning with text alone. Another concept is the principle of temporal and spatial coherence [143], which refers to the joint presentation of content to be processed together.

3.1.3 Multiple External Representations

The term *Multiple External Representations* (MER) refers to the expression of a scientific concept or problem in diverse forms and representations. The use of MERs in learning across multiple domains has been extensively documented [144–146]. Ainsworth's DeFT framework [147, 148] characterizes MERs in the context of learning scenarios in terms of design, function, and task. Similar to CTML, MERs consist of numerous representations that need to be simultaneously processed during learning. Specifically, three core functions are identified by Ainsworth [147]:

- Complementary Roles: The usage of representations that contain complementary information or support complementary cognitive processes.
- Constrain Interpretation: The mutual influence of the use or interpretation of the representations involved.
- Construct Deeper Understanding: The encouragement of learners to construct a deeper understanding of a situation.

3.2 Smart Sensors for Augmented Electrical Experiments

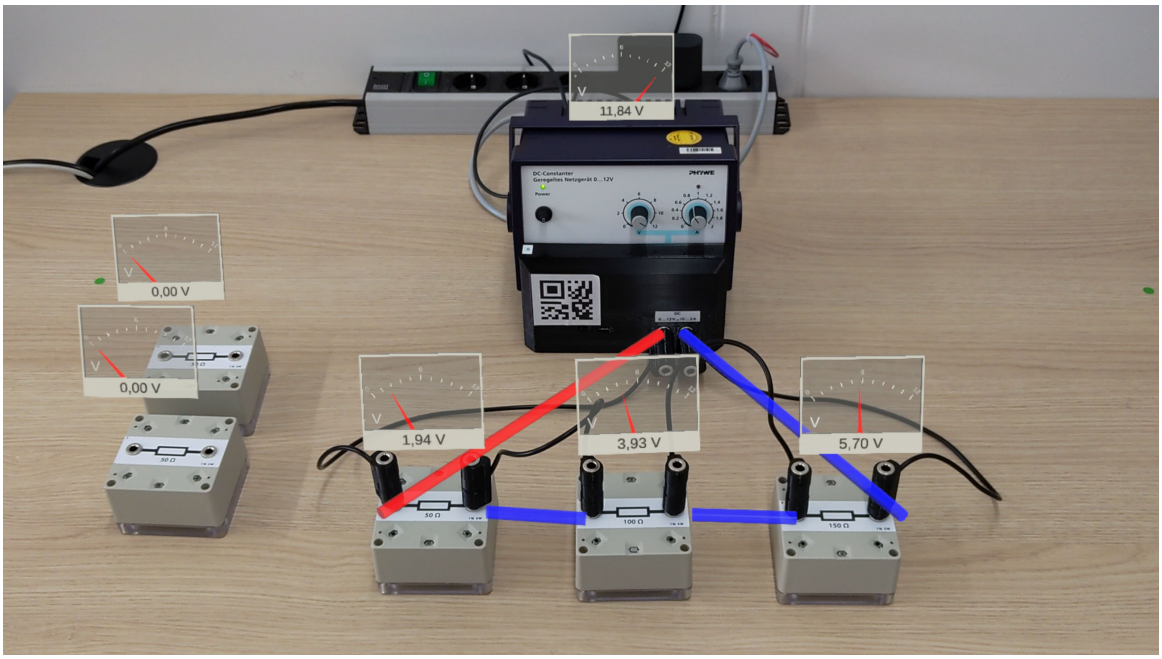

Figure 3.1: Example of a Visualization of the Electrical Potential in AR; Screenshot Captured on a HoloLens 2 [30]

Especially in the context of STEM education, learning platforms are an essential part of education, as students learn not only the facts but also the ways of acquiring knowledge. In inquiry-based learning, students use experiments to gain new knowledge or to deepen what they have learned. A crucial point here is the targeted guidance as well as appropriate educational support to avoid situations such as cognitive overload. The use of smart learning platforms can add considerable value here. By analyzing the learner, targeted assistance or additional questions can be triggered depending on the specific experiment. This can significantly enhance the learning experience while at the same time reducing the workload for teachers. The data obtained also serve as the foundation for many research questions, including *Artificial Intelligence* (AI)-assisted learning.

In this chapter, therefore, a smart sensor system for educational STEM experiments in electrical circuits is presented. It consists of individual components such as resistors or switches that can be connected with cables to form various circuits. The integrated sensors offer considerable added value for the user and for addressing various research questions. Both the electrical parameters like voltage and current, as well as the interconnection of the components by the user, are captured and can be transmitted wirelessly in real-time to other devices. In addition, the exact positions of the components on the table are tracked, for example, to recognize certain

arrangements, but also to ensure the fundamental prerequisite for the use of AR systems. Especially AR applications set high demands on the accuracy and latency of the different systems, since, for example, too strong temporal deviations between the real and the digital environment quickly have a negative impact on the user experience.

An application of the finished smart learning environment is shown in Figure 3.1. In this case, it consists of 4 boxes, each with different resistors and the corresponding connections for wiring. In addition, a laboratory power supply unit is used to power the circuit. With the help of the sensors integrated into the boxes, the wiring of the boxes, the electrical parameters, and the individual positions can be detected. This information is evaluated in the AR-App, and a corresponding visualization of the voltage drop at the resistor, as well as the connection of the boxes, are projected into the user's field of view.

3.2.1 Related Work

The characteristic feature of an AR environment is the visual blending of digital objects into the real world. In order to create an interactive experience, the visualizations are dependent on real-time sensor data giving information about the status of objects or values in the environment. Due to the direct integration into the field of view, however, accuracy, latency, and robustness are decisive factors for a good user experience. The sensor technology used in an AR application can be roughly divided into two groups.

The sensors of the first group are responsible for the detection of the environment and for general localization. The sensors of the first group are responsible for the detection of the environment and for general localization. They are usually installed directly in the device which is used to provide the AR application. A *Head-Mounted Display* (HMD) such as the Microsoft HoloLens [1] has sensors for detecting its own position in space and technology for recognizing surfaces or optical markers that can be used to align and anchor virtual objects. Many modern HMDs also have, for example, built-in eye-tracking sensors, hand gesture recognition, or microphones. The second group consists of application-specific sensors that acquire as much additional information as possible from the relevant application context. For example, in a physics experiment in an electric circuit, the current and voltage at various points in the circuit are important parameters. But also the wiring or the status of different components can be of great interest. The availability of all this specific information opens up completely new possibilities for interaction and can lead to a highly immersive experience.

M. Thees et al. [149] presented an AR environment for physics experiments on heat conduction in metals. A Microsoft HoloLens forms the HMD and uses the integrated sensors to localize and track special markers placed on the experiment. The

[1] https://www.microsoft.com/de-de/hololens, accessed January 16, 2023

application-specific physical measurements in the form of a temperature profile along the investigated metal rod are captured by a thermal imaging camera. The acquired data is processed with the help of an additional computer and sent to the HoloLens where it is visualized. D. Sonntag et al. [150] also used a HoloLens to create AR environments for a capacitor experiment, an electron beam deflection tube experiment, and an experiment with Teltron tube and Helmholtz coils [151]. The positioning of the objects is established at the beginning by an automatized visual comparison of camera images with a stored CAD model, with the possibility to make manual corrections. Application-specific measurement values are recorded by multimeters connected via USB to a Raspberry Pi *, which makes the data available to the HoloLens via a web server.

Both of the solutions presented have their limitations. By using classic of-the-shelf measuring instruments such as multimeters or thermal imaging cameras, an additional computer is needed to process the data and make it available to smart glasses. The marker detection used by M. Thees et al. [149] provides sufficient accuracy in most cases and responds to subsequent changes during the experiment, but requires very prominent markers that are directly in the field of view of the user and, therefore, quickly disturbing. The solution of G. Albuquerque et al. [151] does not use markers, but the mention and implementation of a manual correction of the position, however, indicate a rather low accuracy. In addition, changes in position are not tracked during the experiment.

3.2.2 Voltage and Current Measuring System

A key component of the experimentation boxes is the measurement system for current and voltage. It measures the voltage across and the current through the electrical component. In order to be suitable for a wide range of experiments, the following requirements were defined in advance:

1. Measurement range: The physical experiments to be performed are related to electrical circuits operating at touch-safe voltages and powered by a laboratory power supply which is limited to a maximum voltage of 15 V and a maximum current of 500 mA. Since the boxes do not have a defined polarity from the outside, the measuring system must cover the measuring range $V_{IN} = -15\,\text{V} ... + 15\,\text{V}$ and $I_{IN} = -500\,\text{mA} ... + 500\,\text{mA}$.

2. Measurement accuracy: The experiment boxes form a learning instrument and should therefore keep the inconsistencies as low as possible since a high measurement deviation inevitably creates a distraction for the learner. This may be intended in certain experiments to further explore the topic of measurement inaccuracies, but usually, it is a hindrance and tends to confuse the learner. In this case, a maximum voltage deviation of $\pm 0.3\,\text{mV}$ and a maximum current

deviation of $\pm 10\,\mathrm{mA}$ were specified for the measurement system. Through a suitable study design, where, for example, the measurement of very small currents is avoided, it is possible to almost completely hide measurement errors.

3. Sampling rate: The required sampling rate for current and voltage measurement depends strongly on the application. For experiments with direct current, high sampling frequencies are usually not necessary, which is why an additional low-pass filter in software is used to ensure a smooth data output. For experiments with alternating current or, for example, experiments regarding the charging and discharging of capacitors, a higher sampling frequency is an advantage. With regard to the planned experiments, the maximum sampling rate is limited to 250 Hz, and an adjustable digital low pass filter is added in the software.

4. Protection circuits: To ensure reliable operation in every possible use case and to make the sensor boxes robust against improper use and unwanted negative effects, various protective circuits are required. Therefore, the installed electronic component (e.g.: resistor, light bulb), as well as the internal electronics, had to be protected against currents and voltages outside the specified range and possible electrostatic discharges.

To meet all these requirements, the circuit shown in Figure 3.2 was designed. To protect the integrated electronics from external electrostatic discharge, three *Transient Voltage Suppressor* (TVS) diodes were included. A *Voltage-triggered Bidirectional Thyristor* (VBT) and a *Polymeric Positive Temperature Coefficient* (PPTC) were added to protect the circuit against voltages and currents outside the specified range. To measure the voltage, a voltage divider formed by two precision resistors R_{V1} and R_{V2} is used to map the applied voltage range to the differential input range of the *Analog to Digital Converter* (ADC) ADC_V. The current measurement is realized by measuring the voltage across the shunt resistor R_S. This voltage is amplified by two anti-parallel instrumentation amplifiers and routed to the differential inputs of ADC_I. As instrumentation amplifiers, current shunt monitors have been used which are characterized by a large range of bidirectional common-mode voltage.

Analysis and Evaluation

To determine the accuracy of the current and voltage measurement unit, a set of five identical sensor boxes was considered. To explore the full range of the electrical specification, resistor values of 25 Ω, 50 Ω, and 150 Ω were employed as incorporated electrical components. Two calibrated precision multi-meters were used as measuring instruments for current and voltage measurement. The measurement results were generated by setting a laboratory power supply to the corresponding desired value, controlled by the reference multimeter.

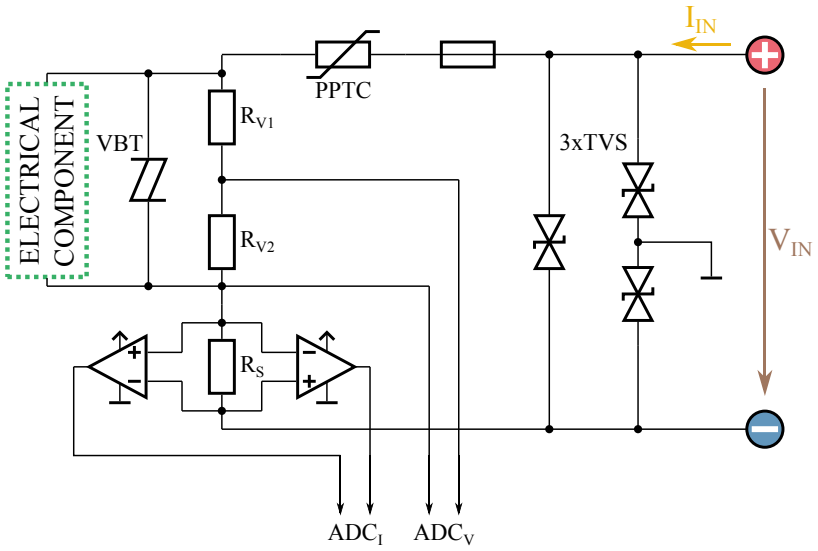

Figure 3.2: Circuitry of the Voltage and Current Measurement [30]

The tests show that the voltage measurement meets the specifications. Over the entire measurement range, a maximum deviation of 0.2 mV is not exceeded (Figure 3.3). At the same time, the inaccuracy decreases significantly as the voltage decreases. Figure 3.4 illustrates this even more clearly and shows a relative deviation of around one percent over the measurement range. The results of the analysis of the current measurement show a maximum deviation of about ± 7 mA (Figure 3.3), which is below the required maximum deviation of 10 mA.

In summary, the measurement system was able to meet the required specifications in a laboratory test environment. The measuring system was also able to fulfill the requirements when used in several studies and laboratories in schools and universities.

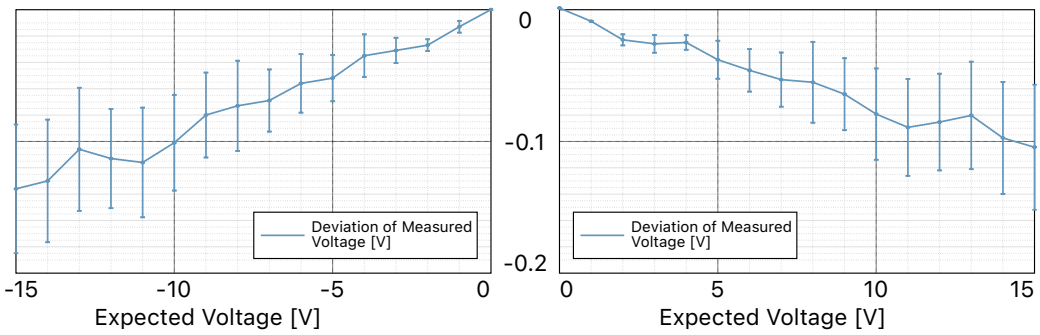

Figure 3.3: Absolute Deviation of the Voltage as Measured by the Sensor Box with Regard to the Expected Value [30]

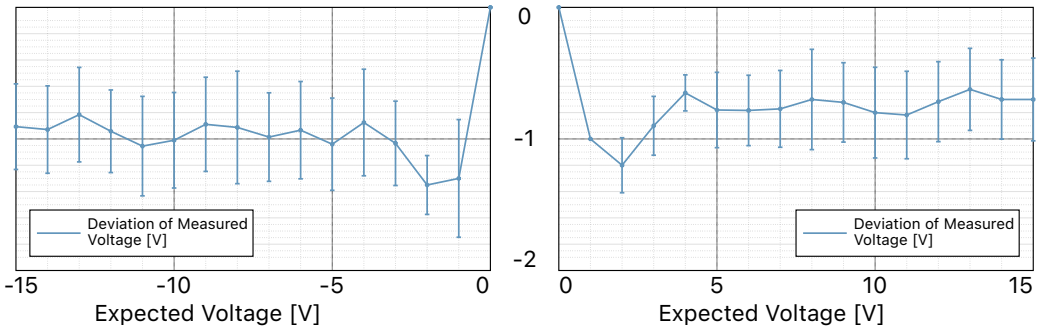

Figure 3.4: Relative Deviation of the Voltage as Measured by the Sensor Box with Regard to the Expected Value [30]

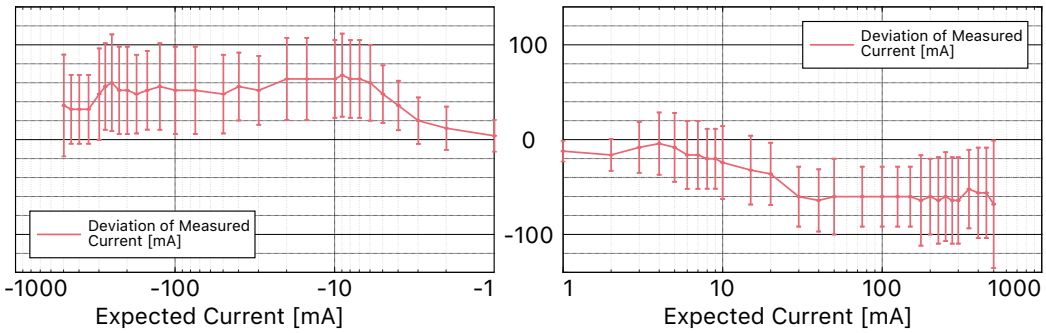

Figure 3.5: Absolute Deviation of the Current as Measured by the Sensor Box with Regard to the Expected Value [30]

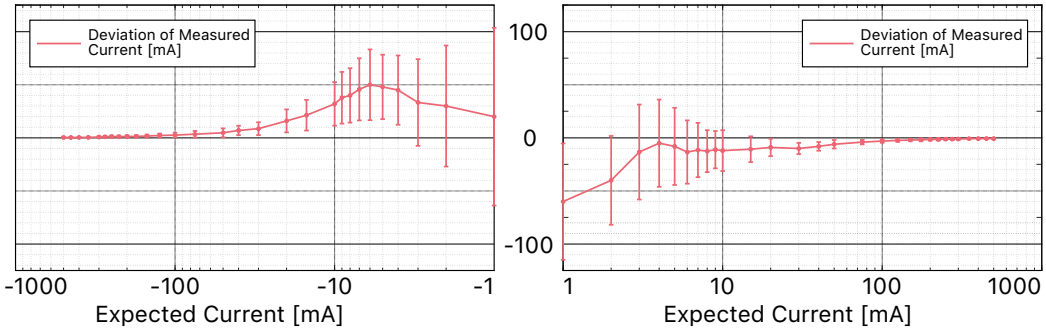

Figure 3.6: Relative Deviation of the Current as Measured by the Sensor Box with Regard to the Expected Value [30]

3.2.3 Cable Tracking

Since the interconnection of the individual boxes via cables is an essential part of the planned experiments in the electrical circuit, it must also be tracked. An important prerequisite here is the clear identification of the cables in the various sockets. In addition, an optically similar-looking solution to the previously used laboratory plugs, as well as the function of "multi-stacking plugs" (Figure 3.7), as is known from laboratory plugs, is required. The tracking of the cables enables the software to generate a connection graph in real-time, which can then be used, for example, to reconstruct the structure in the form of a circuit diagram or to check the current circuit against a predefined solution.

Figure 3.7: Multi-Stacked Laboratory Plugs

Figure 3.8: Multi-Stacked Smart Plugs

To achieve this functionality, several approaches were evaluated. Distinguishing the plugs by different color markings would have the advantage that the previously used cables can continue to be used. The disadvantage, however, is the mandatory color differentiation of the cables, which is not necessarily desired in every experiment. In addition, a sensor system with color sensors poses a major challenge, especially for the "multi-stacking plugs". A camera-based sensor system, however, would be an option, but it increases the installation effort and is influenced by light conditions and possible obscurations. Furthermore, camera-based systems are often not considered for use in schools due to the high data protection requirements.

Another system for cable identification is presented in [152]. Here, instead of the usual lab plugs, three-pin 3.5 mm *Tip Ring Sleeve* (TRS) audio plugs are used. The two additional contacts of each plug are connected to a resistor located inside the plug. The resistance of this resistor can be determined by a corresponding measuring electronic inside the box. By choosing different resistors for each plug, the plugs can be identified uniquely. The disadvantages of this system are, on the one hand, the limited number of plugs due to the resolution of the ADC used and the accuracy of the employed resistors. On the other hand, the identification of "multi-stacking plugs" is still very challenging and only possible with a further significantly reduced number of plugs.

Since none of the above solutions fully met all the requirements of the project, a new solution was developed. The standard lab connectors are replaced by 6.35 mm TRS audio jacks. They offer sufficient stability for continuous use and are widely available in a three-contact form factor. One contact is still used for the actual cable connection, and the other two for the identification of the connectors. The identification is based on the one-wire protocol which uses two physical connections to create a bus structure for data transmission. Every plug forms a one-wire slave with a unique 64 bit identifier, whereas each socket represents a one-wire master. Due to the one-master/multi-slave structure, the master can read out all identifiers of the connected slaves and even select them specifically for communication. This allows the realization of "multi-stacking plugs" (Figure 3.8) by connecting the corresponding data lines as shown in Figure 3.9. Technically, there is a 1 kbit EEPROM chip (DS2431 from Maxim) integrated into each plug, shown in Figure 3.10, whereas currently, only the 64 bit identifier of the 1-Wire interface on the DS2431 is used to identify the plug. The actual memory can be used in the future for additional information and statistics about the plug. The one-wire master is implemented directly on the main microcontroller, but can also be implemented on a *Field Programmable Gate Array* (FPGA) as done in 3.3.4.

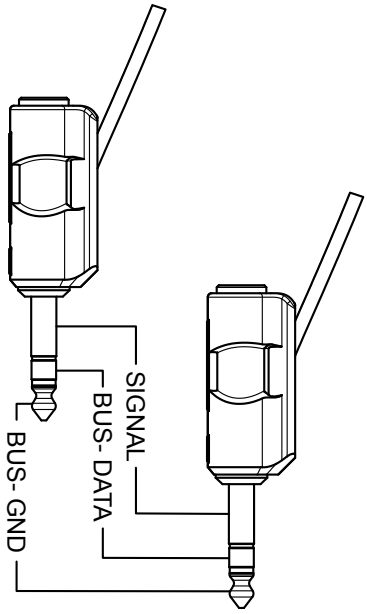

Figure 3.9: Signal Description of Multi-Stacked Smart Plugs

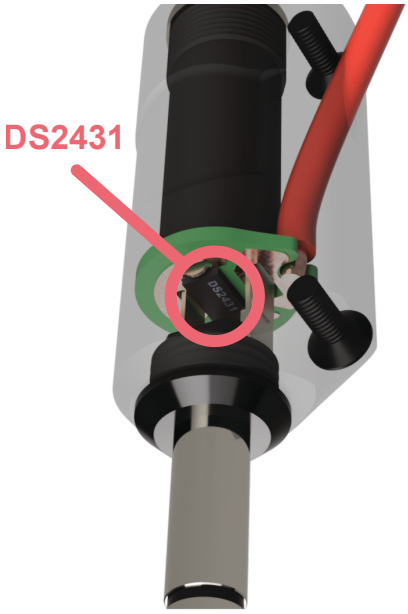

Figure 3.10: Identification Chip inside the Smart Plug

Analysis and Evaluation

This solution for the detection of connectors suffers from a few disadvantages due to its design. It requires special cables and three-pin connectors to enable data exchange. In particular, the multipole connectors may raise additional questions for advanced learners, which need to be addressed during the introduction. Furthermore, connections of cables without a connection to the box cannot be tracked. In other words, if plugs are stacked, but the lowest plug is not plugged into a box, this connection cannot be tracked.

However, the solution also offers major advantages, particularly in comparison with other available systems. The digital interface enables precise identification of each individual connector through the 64 bit long identifier and also the reliable identification of multiple connectors in one socket due to the bus structure. The additional memory in each connector can be used to describe the cable more precisely. When a master reads an identifier for the first time, it can read the information stored in the memory to get the identifier of the connector on the other side of the cable as well as information about the length and color of the cable. This way, the pair of plugs does not have to be registered as a cable in the software beforehand. The time it takes to read an identifier essentially determines the latency in which a change is available in the software. Reading a single plug identifier on the bus only takes about 15 ms. For practicality reasons, the stacking of plugs is limited to a maximum of five in software, which results in a maximum time to read all IDs of $5 \cdot 15\,\text{ms} = 75\,\text{ms}$. Thus a very responsive behavior can be guaranteed.

3.2.4 2D Positioning System

The position of an object is very important information for many types of learning environments. Anchoring information in an AR environment necessarily requires some sort of positioning system, but even in non-AR environments, the position of objects is necessary or can provide additional, important insights for learning analytics.

Since the requirements for a positioning system used in a learning environment are strongly dependent on the intended use, there are various approaches. In the field of AR learning environments, smartphones or tablets are often used. Here, the camera image is analyzed with special algorithms that recognize certain predefined markers. Depending on these markers, simulated objects can then be positioned. Surface structure AR works in a similar way, with the structures of the available surfaces replacing the markers. Both technologies are usually assisted by additional data from accelerometers and gyroscopes, which lead to a significantly better overall result. This technology is particularly characterized by the low initial barrier. In general, a modern smartphone is sufficient to obtain at least acceptable results.

For an even more immersive and hands-free experience, AR glasses such as Microsoft's HoloLens 2 are used. The tracking system of the HoloLens 2 consists of a number of individual cameras and *Light Detection and Ranging* (LIDAR) systems that are used to track objects as well as the position of the glasses themselves in the environment. Cameras are also frequently used in non-AR environments. Here, either marker can be used or objects and structures can be recognized directly. A well-known example is a motion-capturing system that uses several infrared cameras to detect special reflective markers and calculate their positions based on the different viewing angles. This system is regularly used in learning environments in the field of sports due to its high tracking frame rate capabilities.

Another popular tracking system is the SteamVR Tracking 2.0 which was developed by VALVE. It uses rotating infrared light beams emitted by one or more base stations, allowing the objects themselves to calculate their position relative to the base station(s). This approach differs significantly from the systems described so far, as the position of objects is not calculated by an external device, but by the object itself. Through the use of multiple sensors together with an accelerometer and a gyroscope, it is possible to detect very fast movements with low latency. The objects then transmit their position via a data connection to a central device, which then processes it further. This system is mainly used in conjunction with virtual reality glasses developed by the same manufacturer.

In addition to the systems mentioned above, there are a number of other approaches for capturing the position of objects in learning platforms, such as the system presented in [152], which is based on RFID tags. However, in order to reliably track the boxes of our physics experiment platform, the tracking system had to meet the following requirements.

1. The system is intended to be a fully functional tracking system that works together with devices such as the HoloLens 2, but can also be used independently.

2. The accuracy of the system must be suitable for use in AR systems. Therefore, it is sufficient for us to determine the position and rotation on a regular table. A 3D positioning, as well as the tracking of very fast movements, is not required.

3. The system must be reliable and robust against external interferences.

4. A camera-based system is not desired due to possible data protection concerns when used in schools.

5. Since the complete system should also be produced in larger quantities for use in studies, the system should be relatively cost-effective and, if possible, utilize existing components of the overall system.

The system closest to meeting the requirements is version 2.0 of the Steam VR-tracking system. However, the available original tracker (VIVE Tracker 3.0[2]) is challenging to integrate into boxes due to its form factor and furthermore exceeds the costs of one of our experimental boxes without tracking system several times. In addition, the tracker is designed for fast-tracking in 3D, which is not needed in our case.

Therefore we have developed our own tracking system where we use the Base Stations 2.0 of the SteamVR tracking system (in the following referred to as "SteamVR BaseStation 2.0"), but have created a fully custom tracking device.

This project was carried out in collaboration with Sebastian Kapp working at the Physics Education Research Group at the Technische Universität Kaiserslautern. Figure 3.11 illustrates my contribution to the overall system. It starts with the reception of the light pulses from the SteamVR BaseStation 2.0 and ends with the transmission of the filtered and preprocessed raw data via BLE. The further processing of the raw data as well as the calculation of the final position and conversion into the coordinate system of the HoloLens 2 was implemented by Sebastian Kapp. In the following subsection 3.2.4, I will only give a very brief overview of the entire system and afterward go into more detail on my part of the system. A more general overview of the entire system was published in [30] as well as in [153].

[2] https://www.vive.com/de/accessory/tracker3/, accessed January 16, 2023

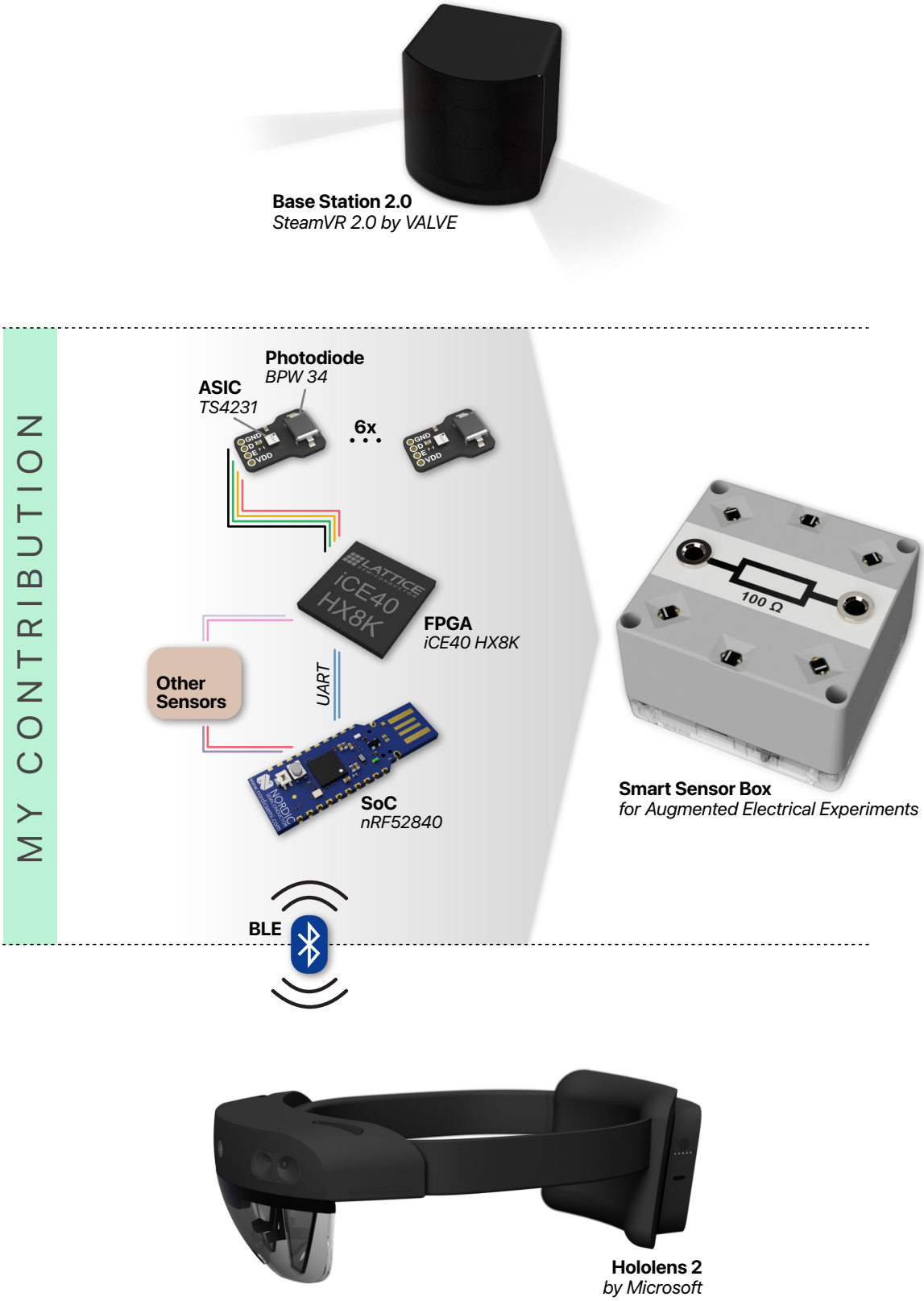

Figure 3.11: Tracking System Contribution

System Overview and Functionality

This paragraph first describes the general idea and functionality of the position tracking system. More detailed implementation parameters and specifications will follow in the next paragraph. A base station equipped with a rotor that emits two light beams moving through space serves as the basic reference point. Figure 3.12 schematically shows an open base station with the spinning rotor emitting the two light beams and Figure 3.13 shows a sequence of images illustrating the movement of a light beam. It is important to note that the light beams must be offset on the rotor as well as angled relative to each other. The exact alignment used on the SteamVR BaseStation 2.0 will be explained in Figure 3.17. Mathematically, the two light beams can be described by plane equations depending on the rotor position. The first plane is defined by the normal vector $\vec{n}_1(\phi)$ and the second plane by the normal vector $\vec{n}_2(\phi)$. The angle ϕ describes the angle covered on one revolution of the rotor starting from a fixed starting position ($0° \leq \phi < 360°$).

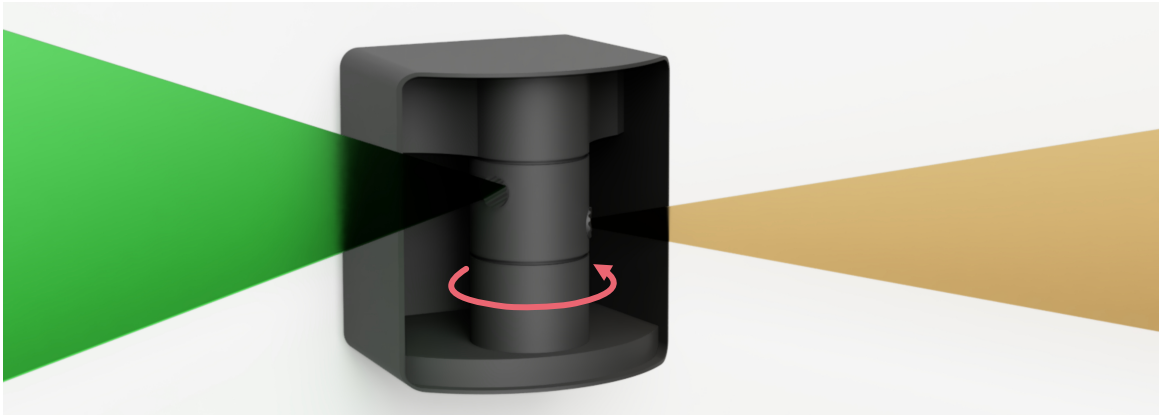

Figure 3.12: Simplified Representation of a Basestation 2.0 Without Front Cover [3]

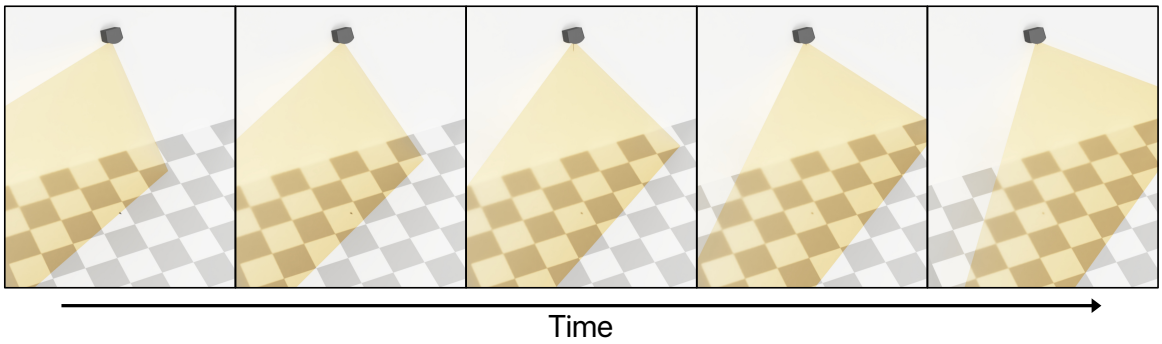

Figure 3.13: Image Sequence to Illustrate the Movement of a Light Beam[3]

The actual positioning takes place exclusively on the tracked object itself. An additional communication channel besides the light beam emitted by the base station, as well as the predefined system parameters, is not necessary. Starting from the tracked

object, considering exactly one rotation of the rotator ($0° \leq \phi < 360°$), there are two significant events:

1. $\phi = \alpha$ (Figure 3.14 (a)): At this point, the first of the two light beams hits the phototransistor of the tracked object. The phototransistor must, therefore, be located in the plane with the normal vector $\vec{n}_1(\phi = \alpha)$.

2. $\phi = \beta$ (Figure 3.14 (b)): At this point, the second of the two light beams hit the phototransistor of the tracked object. The phototransistor must, therefore, also be located in the plane with the normal vector $\vec{n}_2(\phi = \beta)$.

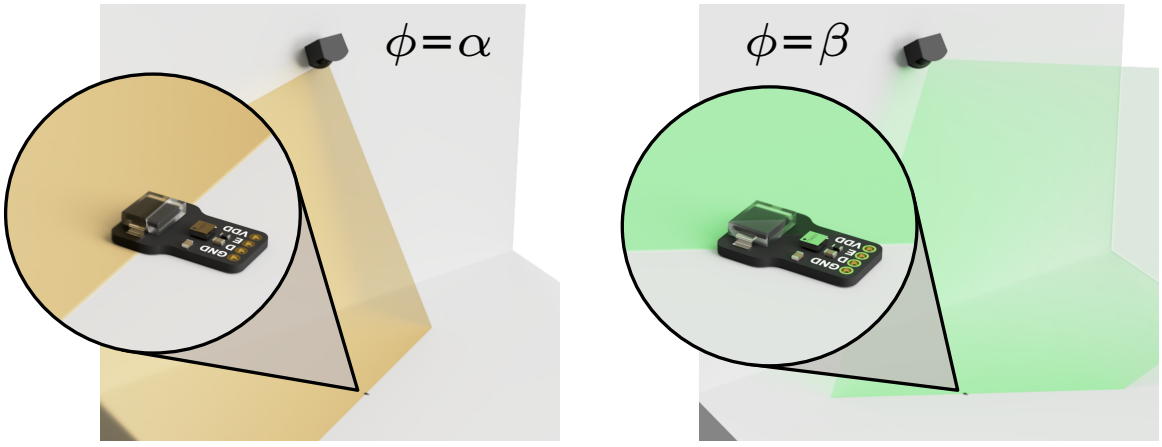

Figure 3.14: Detailed Views of the Moment when a Light Beam Hits a Sensor[3]

Knowing that the phototransistor must be located on both planes, it must also be located on the intersection line of the two planes: $\vec{s} = \vec{n}_1(\alpha) \times \vec{n}_2(\beta)$. Thus with only one sensor a straight line starting from the base station can be determined on which the sensor must be located. With several sensors and a carefully chosen arrangement of the sensors, even positioning in three-dimensional space can be realized. In our case, however, only the position and rotation of the object on a predefined plane E_{table} (the table surface on which the experiments are performed) shall be tracked. For this purpose, the intersection lines $\vec{s}_n$ of several sensors are intersected with the plane E_{table} to obtain the exact positions of the individual sensors.

The essential point of the system is the determination of the angles α and β. For this purpose, a system-wide known sequence $(s_i)_{i=1,\ldots,n}; s \in \{0, 1\}$ is defined in advance. This is continuously transmitted by the base station across the light planes.

[3] The color of the light beams is only for illustration purposes, in reality, they are located in the infrared range and therefore not visible to the human eye.

It is important to note that the sequence always starts at the rotor position $\phi = 0°$ and is transmitted at a fixed frequency. This results in a fixed dependence between the rotation angle ϕ and the position i within the sequence (s_i). The tracked object receives a small part of the sequence while the phototransistor is hit by each of the light beams ($(a_j)_{j=1,...,m}$ for the first light beams; $(b_k)_{k=1,...,p}$ for the second light beams). The lengths m and p of the received sequences depend on the orientation and distance of the phototransistor as well as the transmission frequency of the sequence. The sequence (s_i) was chosen in advance so that each contiguous subsequence with a minimum length of l_{min} is present exactly once in the sequence. Thus, if $m \geq l_{min}$ and $p \geq l_{min}$, the positions of the received sequences (a_j) and (b_k) on (s_i) can be determined. By knowing the rest of the system parameters, the angles α and β can then also be calculated.

The description of the actual implementation techniques and parameters on the SteamVR BaseStation 2.0 is based on measurements and observations (reverse engineering) since there are no official documents explaining the exact construction. Furthermore, we have not done any hardware or software modifications to the SteamVR BaseStation 2.0. The two light beams projected by the lenses placed on the rotor inside the SteamVR BaseStation 2.0 are offset by 120° on the rotor and at the same time angled by ±30° to the rotor axis. Figure 3.17 visualizes the arrangement in more detail, with the yellow line representing the first light beam and the green line representing the second light beam. In order to use several base stations in a common environment, there is a total of 16 different predefined channels that can be selected by software. Depending on the selected channel, the emitted sequences change as well as the rotor speed, which is in the range of around 50 Hz to around 54 Hz. To generate the different sequences, an 17 Bit width *Linear Feedback Shift Register* (LFSR) (description in Figure 3.15) clocked at 6 MHz is used.

Due to the plain structure of LFSRs, they can be implemented in an extremely resource-efficient way and are very easy to reconfigure. The required sequences, which are around 114 000 bit long, can each be fully defined with a polynomial of degree 17 (start value always fixed to 1). To transmit the sequence generated by the LFSR, the signal is first encoded using a *Biphase-Mark-Code* (BMC) (description in Figure 3.16) encoder with a clock frequency of about 12 MHz. This signal is then used for the modulation of the laser to generate the light beams. An overview of the structure of the SteamVR BaseStation 2.0 components required for this work is shown in figure 3.18. A control unit takes over the task of resetting the LFSR when the rotor is in the appropriate position. It is also responsible for the systematic reconfiguration of the LFSR. Each channel of the base station does not have one specific polynomial, as might be expected at first, but actually has two polynomials assigned to it. By selectively switching between these two polynomials, additional information is transmitted from the base station to the tracked objects. One polynomial represents a binary 0, the other a 1. This technique is used to transmit so-called *Omnidirectional Optical Transmitter* (OOTX) data, which consists of a preamble, a CRC32 checksum,

and a payload of 43 byte. In addition to information such as the serial number, the payload also contains important factory-measured calibration data of the base station.

***Linear Feedback Shift Register* (LFSR)**

A LFSR consists of a series of flip-flops connected in a shift register configuration, where the output of one flip-flop is fed back into the input of the next flip-flop in the chain. The output of the last flip-flop in the chain serves as the general output of the LFSR. Furthermore, it is combined along with other intermediate taps with an XOR gate and fed back as the input of the first flip-flop. The taps of this feedback path are defined by the linear feedback function, which gives the shift register its name. There are generally two different types of implementations of LFSRs, the Fibonacci-LFSR and the Galois-LFSR. In this thesis, I will only refer to the Fibonacci implementation whose structure and corresponding Feedback Polynomial are illustrated below.

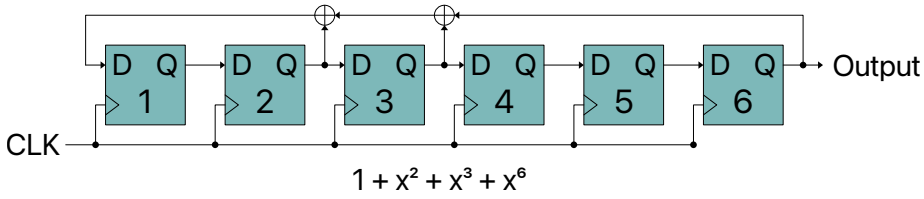

Figure 3.15: Description of a LFSR

***Biphase-Mark-Code* (BMC)**

BMC is often used when only one data line is available since data and clock are transmitted together. However, this leads to twice as many signal transitions being required compared to the actual data signal. The encoded signal (red) toggles at each rising edge of the clock signal (yellow) and additionally at each falling edge of the clock signal if a logical 1 is to be transmitted.

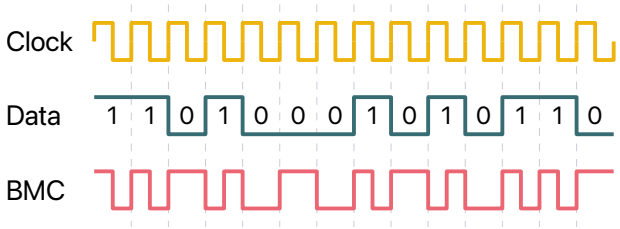

Figure 3.16: Description of a BMC

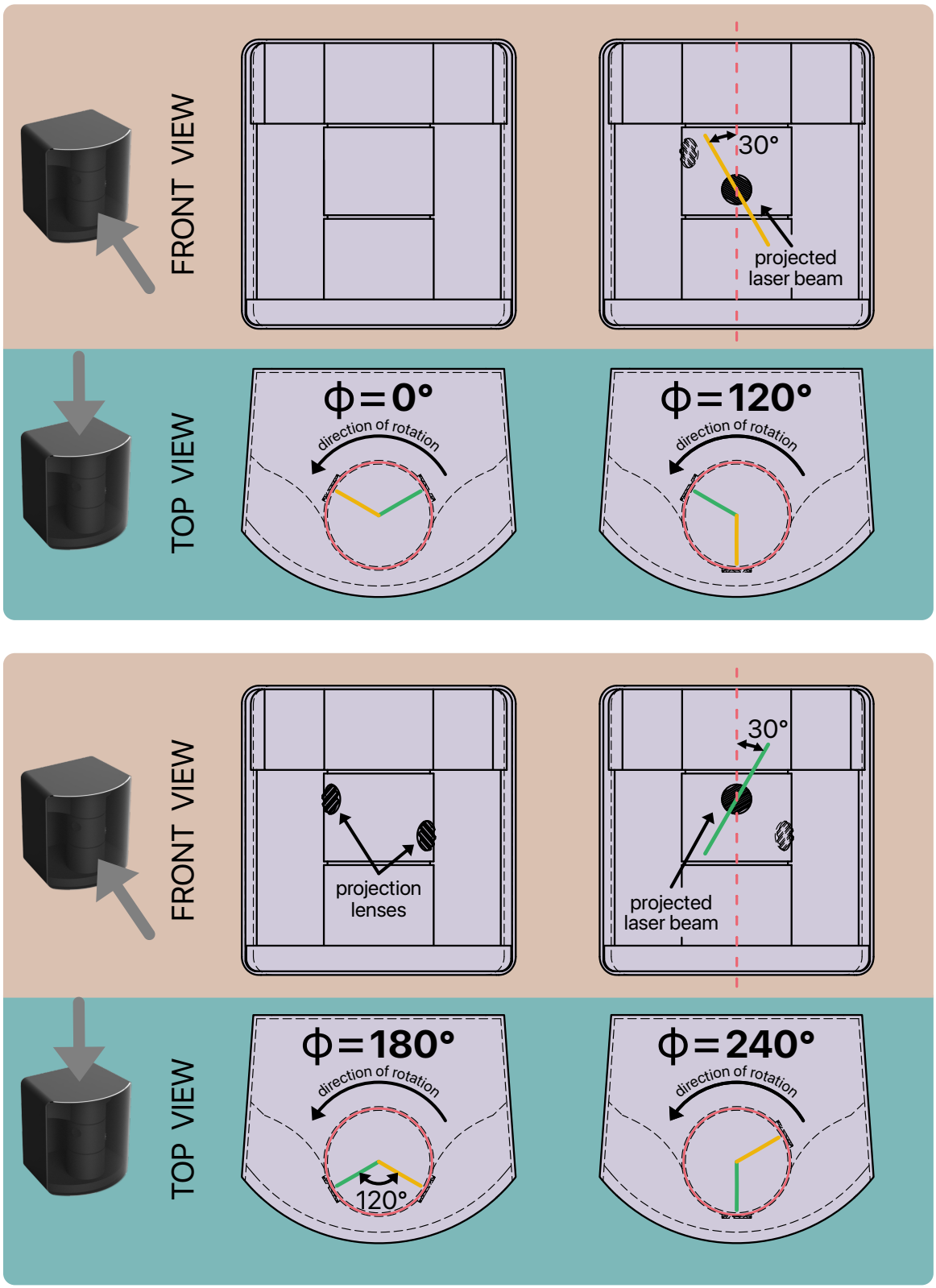

Figure 3.17: Detailed Description of the Arrangement and Alignment of the Light Beams on the Rotor of the SteamVR Base Station 2.0;

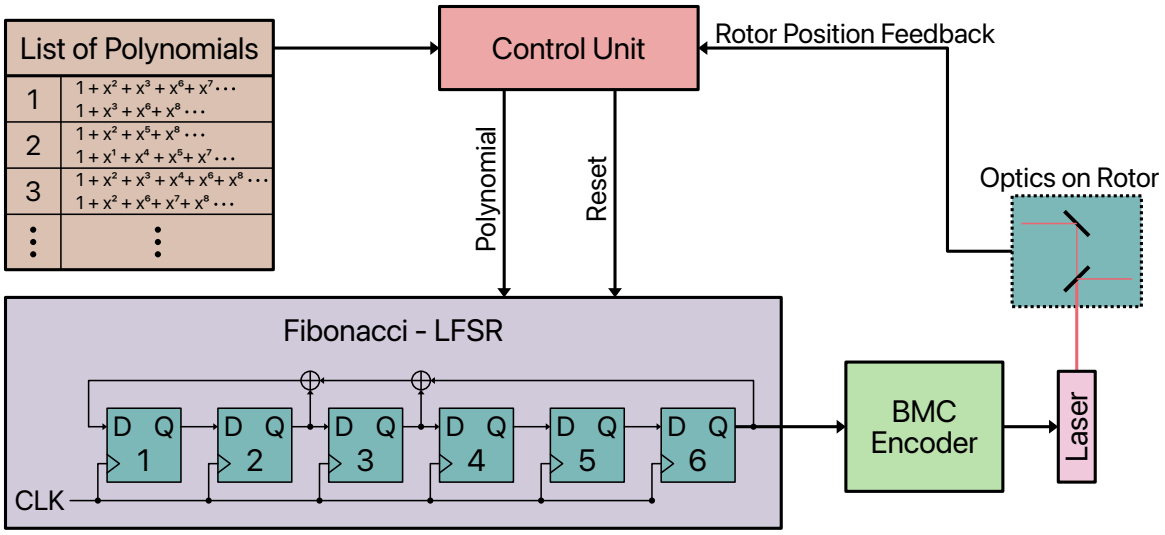

Figure 3.18: Overview of the Structure of the SteamVR BaseStation 2.0 Components Required for this Work

Hardware-Software-Co-Design of the Tracked Objects

Each of the tracked objects consists of six photodiodes for receiving the light beams, a FPGA for processing the time-critical and parallel data streams, and a SoC for filtering and transmitting the received data. The six photodiodes are evenly distributed on the top of the smart sensor box to allow reliable position tracking even when individual sensors are obstructed. Each photodiode is directly connected to a TS4231 *Application-Specific Integrated Circuit* (ASIC) from Triad Semiconductor[4], which was specially developed for this application and converts the received signal into two 1-bit digital signals. One signal serves as an envelope signal and the other as a data signal which reflects the received light intensity. The resulting data streams from the six ASICs are processed identically and completely in parallel on the FPGA. The envelope signal operates as a kind of enable signal, whose start and length are measured. The data signal is first decoded with the help of a BMC decoder and then passed on to the *PolynomChecker-Block*. This block checks if the received data stream has been generated by a LFSR configured with one of the 32 stored polynomials (16 channels x 2 polynomials). If a hit is found, the result is forwarded to the *PositionFinder-Block*, which calculates the position on the sequence. The calculated information is packed together with other measurement data into individual data packets per sensor and per light beam event and sent to the SoC via the UART interface. A single data packet contains the following information:

- **StepCount**: Distance in steps on the LFSR generated sequence from reset to sampled value at *TimeStamp*
- **TimeStamp**: Timestamp of an internal timer in the moment of sampling the last bit for the *PolyValue*
- **PolynomID**: ID of the polynomial used in this sequence
- **SensorID**: ID of the receiving sensor/phototransistor
- **EnvelopeWidth**: Width of the envelope signal pulse
- **SignalStrength**: Number of bits where the received sequence is following the calculated values using the internal LFSR
- **SignalOffset**: Offset between the start of the envelope signal and *TimeStamp*

All data packets are first cached in a *First In First Out* (FIFO)-Buffer on the SoC and then processed consecutively. The main tasks are sorting and summarizing the data, filtering out disturbances, and carrying out plausibility tests. The goal is a data packet consisting of the two positions for the angle determination as well as the sensor/phototransistor ID and a fixed packet ID. Therefore, the packets are sorted by

[4] https://triadsemi.com/product/ts4231/, accessed January 16, 2023

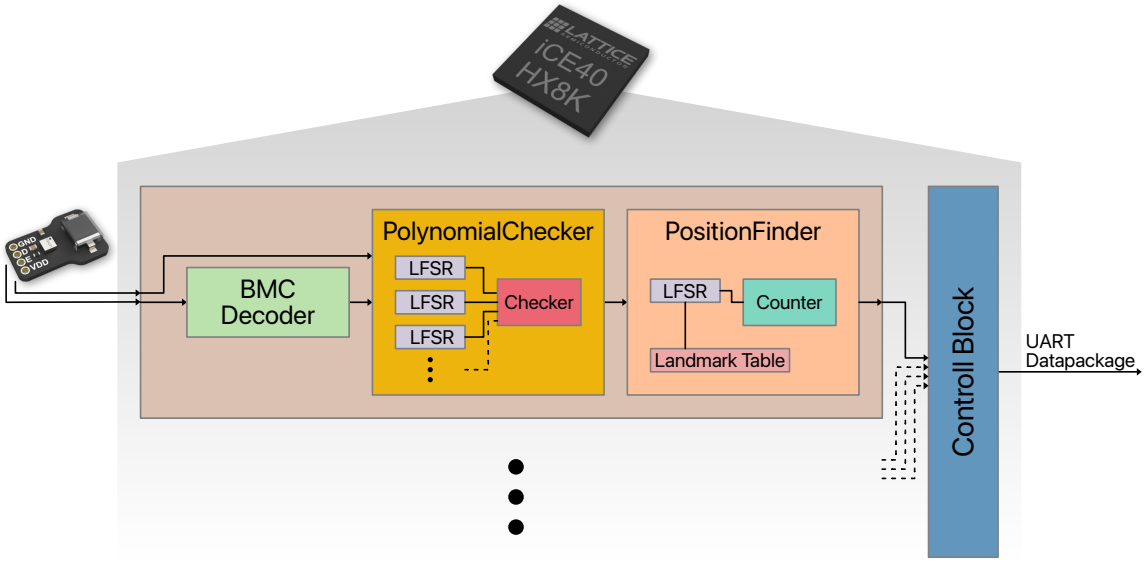

Figure 3.19: Structural Overview of the Hardware Blocks on the FPGA for Processing the Data Received by the Light Beams

sensor/phototransistor ID and verified against multiple plausibility checks concerning timing, pulse length, and sorting. In addition, time dependencies of data from different sensors/phototransistors are checked to detect incorrect data. The reviewed data packets are then transferred to the BLE interface.

In addition to the position data, the OOTX data is also sent via BLE. This is usually done once after the start of the system, as soon as a valid OOTX data packet is available. For this purpose, the use of the different polynomials is evaluated on the SoC, and the resulting data packet is validated with the help of the CRC32 checksum. Afterward, the data is sent via BLE in a predefined format.

Position tracking in the coordinate system of the HoloLens 2

Further data processing and final position determination were realized on the HoloLens 2 by Sebastian Kapp [30]. In addition to the mathematical operations for calculating the intersection lines and applying the calibration data available in the OOTX data, the merging of the relative position data from the tracking system to the coordinate system of the HoloLens 2 is a major challenge. For the current implementation, a single smart sensor box was first localized in the HoloLens 2 coordinate system using a QR code on the table. Next, the position of the base station in the HoloLens 2 coordinate system can be calculated by using the positioning information provided by the tracking system. As soon as the position of the base station in the HoloLens 2 coordinate system is known, the tracking system is ready for use. A more detailed description of this procedure can be found in [30] and [153].

Analysis and Evaluation

The analysis and evaluation of the system consist of two parts. On the one hand, the accuracy and validity of the raw data collected by the tracking system must be checked extensively. This includes the hardware/software on the FPGA and SoC. On the other hand, the overall system must be tested for accuracy, interference tolerance, and latency.

The accuracy of the overall system depends heavily on the determined positions of the received sequences (a_j) and (b_k) on the main sequence (s_i). Ideally, the determined positions which are later used to calculate the angles α and β should be located exactly in the middle of the hit event. Especially in real environments, interferences cannot be excluded. These range from completely reflected signals, e.g. due to reflective surfaces, to small changes in the temporal course of the signal that can lead to incorrect decoding. Therefore, during the development of the system, many test scenarios were created to provoke interference and reflections intentionally. The signal outputs from the ASICs during the tests were recorded in order to use them as a stimulus for the system simulation in software. As a result, various validity criteria and optimizations were developed to detect and filter out the provoked errors. By applying these rules while processing the raw data packets from the FPGA on the SoC, incorrect data is filtered out reliably. Another source of interference was detected when used together with the HoloLens 2. Since the HoloLens 2 also uses infrared burst signals for its own positioning in space, there are always very short overlaps during which our system is practically blind. However, the interferences can be reliably detected and filtered out, which means that the system does, at least, not detect and pass on any incorrect positions.

The performance of the entire system was tested by Sebastian Kapp by performing a static accuracy measurement and during use in a usability evaluation together with the other features of the smart sensor box. In summary, the standard deviation of the position of the smart sensor box in the selected setup was less than 2 mm. The positions on the sequence used to calculate the angles have a standard deviation of less than 2 bit in the same setup. The system also performed very well in the usability evaluation. The exact results and setups can be found in [30].

3.2.5 Data Communication

Since all system components are connected to each other, the wireless data connection plays a very decisive role in the overall system. First of all, the transmission technology must be capable of transferring the amount of data required by the application within the corresponding latency. At the same time, the system must be resistant to interference and thus enable robust data transmission. Dropouts or even incorrect data can have a significant impact on the user experience or even lead to the entire system becoming unusable. Since almost all components of the system are battery-powered, attention must also be paid to the energy efficiency of the data transmission. This avoids excessive recharging times of the system components and thus increases the usability of the overall system. In addition to the requirements during system operation, the setup phase must also be taken into account. The connection setup of the boxes must be achievable for untrained persons and should ideally be automated.

As a solution for wireless data communication between our smart sensor boxes and the HoloLens 2, the BLE technology was chosen due to offering a very energy-efficient way of wireless data transmission and providing a robust connection through techniques such as frequency hopping. It is also supported by many devices, especially smartphones, and tablets. In terms of data throughput, BLE offers an over-the-air data rate of up to 2 Mbit/s. In the practical environment, however, and due to the necessary protocol structure, the actually transmitted payload is significantly lower. Since all sensor devices (smart sensor boxes) in our application are only connected to the HoloLens 2, the BLE module installed in the HoloLens 2 limits the throughput and the maximum number of connected devices. Making a precise statement about the exact maximum data throughput of BLE in our scenario is relatively difficult, as this depends heavily on external interference factors as well as the actual BLE modules used. At the same time, the data rate required by our application is variable and can be adjusted to a certain degree. After the first estimations and the evaluation of several test setups with up to eight simultaneous connections, it can be concluded that the data rate of BLE is sufficient for our application.

To ensure maximum flexibility and compatibility with other tools such as phyphox [154], the communication protocol used is relatively simple. The first byte of a packet is, by definition, always a packet identifier and thus determines the further structure and function of the packet. In this way, it can be quickly decided in the software whether a packet is relevant, and if so, a parser according to the packet identifier can be selected. Figure 3.20 shows an example of the structure of a data packet as used in our positioning system.

In addition to the transmission of measurement and status data from the smart sensor boxes, the HoloLens 2 can also send configuration parameters to the smart sensor boxes. Hence, it is possible to select different filters for current and voltage measurement or ignore certain base station channels in our tracking system. The

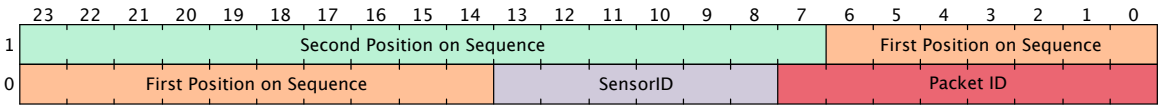

Figure 3.20: Example of the Structure of a Data Packet as Used in the Positioning System

use of packet identifiers also enables continuous expansion without affecting older structures. This is especially useful because the system should also be compatible with other future sensors and modules.

In summary, the data transmission technology proved to be very reliable and completely sufficient for the required amount of data. Even when using several sets of our smart sensor boxes in a classroom with ultimately more than 40 individual boxes, the system performed very well. In addition, the connection setup could be automated by means of pre-configured setups, which is a significant advantage in everyday use.

3.3 Smart Measurement Platform for Photometry in Education

Figure 3.21: Smart Measurement Platform for Photometry in Education (SmaEPho) and its Digital-Twin

Photometry is a very important measurement method in a variety of experiments in the field of STEM education. It is based on the measurement of the absorption or transmission of radiation from a solution. It is often used in the field of analytics in biology for the determination of, for example, ions in water samples, food components, or photopigments. But it can also be used for growth analysis, for example. Due to everyday and tangible applications of photometry and the simple understandable physical basics of the measurement method, the subject is an integral part of school education in STEM subjects. It is also part of the elemental knowledge in many advanced training classes and university lectures. In both areas, the focus is not only on carrying out measurements and using the obtained data but also on the measurement method and the way it works. The disclosure of the measuring method and measuring technique provides a deeper understanding of the technical realization of a measuring device on the one hand and, on the other hand, leads to a more

informed handling of the measuring device itself, which in turn results in a better understanding and evaluation of the measured value.

Due to the widespread application of photometric measurements, this topic is ideally suited for the use of a smart learning platform. On the one hand, this enables research-based learning, i.e. the experimental acquisition of scientific principles, problem-solving, research, and learning skills in real-world contexts [155]. On the other hand, smart features such as the tracking of user interactions or the additional interaction possibilities with the learner can deliver an even better learning experience. Moreover, such smart learning platforms are the prerequisite for addressing a wide range of research questions on topics like the understanding of the learning process or the application of AI-based analysis and feedback processes.

From a technical point of view, a smart learning platform of a photometric measurement system represents another instance of a complex integrated sensor system for data acquisition with a focus on usability, reliability, and accuracy.

In cooperation with the Chair of Bioprocess Engineering at the Technical University of Kaiserslautern, we developed a smart learning platform for inquiry-based learning. It is called SmaEPho and is designed to illustrate the functionality of a photometric measurement system as well as to provide a fully functional photometric measurement system with sufficient accuracy for use in schools. At the same time, similar to the smart sensor boxes presented in Section 3.2, special attention was given to the integrated sensor system to track, all user interactions and measurement data. Furthermore, this information is forwarded to a digital twin of the SmaEPho where it is analyzed and stored.

This project was carried out in collaboration with Lena Geuer working at the Chair of Bioprocess Engineering at the Technical University of Kaiserslautern, who was responsible for the methodological and didactic planning of the SmaEPhos as well as the later evaluation in e.g. usability studies. My contribution was the technical planning, development, and implementation, as well as the direct evaluation of the integrated sensor technology. The complete system, together with a first usability study as well as isolated text passages in this section, have already been published in the Journal of Education Sciences [31].

3.3.1 Related Work

Professional photometric measuring systems are usually fully enclosed, making them less suitable for demonstrating the basic photometric measuring method. In addition, the acquisition costs are typically far outside the tight available budget for schools. Self-built photometers using instructions from public sources do offer some advantages in this respect. Their construction is often much simpler and, therefore, easier to understand, and furthermore, the components used are much cheaper. However, teachers usually do not have the time to build and provide a class set of such self-built low-cost photometers.

Here, a modular photometer from desklab[5], in the following referred to as desklab photometer, offers a low-cost alternative that is already widely used in German education. Desklab describes its modular photometer as "new possibilities for experimentation and research in science and technology lessons with a focus on interdisciplinary and problem-oriented tasks and issues" [1]. The desklab photometer is modular in three parts (microcontroller, breadboard, measurement chamber) that were 3D printed and can be assembled with magnetic connections. Desklab explains that the magnetic connections allow a flexible assembly of the photometer and a specific alignment to the individual components. The measurement setup can thus be supplemented step by step with the required components and still remain clearly arranged. The widespread use of the system in German schools demonstrates the usefulness of such a system for research-based learning.

However, the system also has some limitations in order to keep costs low. For example, there are no protection circuits to safeguard the electronic components like the LED, which is why the circuit must always be checked by a teacher or other trained person before it is switched on. This is time-consuming and can restrict the experimentation creativity. In addition, the system does not offer the possibility of digitally logging further information about the system status, such as circuit structure, the status of the measurement system, or errors. Studies are, therefore, limited to externally measured values and surveys, which is why many research questions cannot be adequately investigated with this system. Especially due to the increasing use of artificial intelligence, accurate and comprehensive data for the analysis of processes is essential.

Today, such precise recording of process parameters is primarily found in industrial processes, particularly in connection with digital twins. In the field of education, learning platforms in AR or VR environments are frequently used, which are commonly expanded by additional sensor technology such as eye tracking or other body measurements. However, at the time of development of the SmaEPho, I was not aware of any comparable non-virtual intelligent learning platform for research-based learning in photometry.

[5] https://desk-lab.de, accessed January 16, 2023

3.3.2 Smart Learning Platform for Photometry - SmaEPho

In general, the SmaEPho is built on the same principles as the Desklab photometer presented in section 3.3.1 and has, therefore, some similarities regarding design and color scheme. The visual resemblances facilitate the collaborative use of the two systems for studies and research purposes. However, the overall goals in the development of the SmaEPho are quite different from those of the desklab photometer. In addition to integrating the object tracking system, protecting the electrical components, and connecting it to the digital twin with all the resulting possibilities, the aim was to develop a much larger and more robust device that could also function as a demonstrator in larger groups. In addition, all measurement data should be transferred in real-time to a digital twin, which, on the one hand, serves as an additional virtual representation and, on the other hand, can be used for the evaluation and analysis of the data. More about the features and implementation of the digital twin can be found in Subsection 3.3.6. Figure 3.22 shows the hardware platform of the SmaEPho which can be divided into three main components:

- The microcontroller with the display on the left side provides a voltage supply of 5 V and an analog input for voltage measurement. The display allows easy interaction with the user without the need to use an additional device or the digital twin.
- The breadboard in the middle is used to build up the electrical circuit. The sockets of the upper and lower two rows are connected horizontally. The remaining sockets in the middle are connected vertically. During the construction and design of the breadboard, attention was paid to the similarity to a commercially available breadboard.
- The right side consists of a replaceable LED, a replaceable phototransistor, a diffuser, and a recess to hold the cuvettes. Further details can be found in subsection 3.3.3.

Figure 3.22: Hardware Platform of the SmaEPho

3.3.3 Photometric Measuring Setup

The measurement setup of the SmaEPhos is based on the design of the desklab photometer. The measuring chamber consists of a 3D-printed housing with a socket for placing an *Light-Emitting Diode* (LED) on one side and a socket for a phototransistor on the opposite side. A diffuser and a recess for the cuvette containing the sample are located in between. The cover, which blocks the ambient light, can be removed so that the entire setup and beam path can be viewed and thus better understood (Figure 3.23). In contrast to the desklab photometer, the inside of the measurement setup is black in order to reduce possible influences from reflections. In addition, special sockets have been integrated which, in conjunction with the corresponding circuit boards, allow the LEDs and the phototransistor to be changed quickly and easily. The boards also contain an identification chip that is required for the object tracking system as well as parts of the protective circuit to protect the LED/phototransistor.

The necessary circuit that needs to be built on the breadboard that connects the components placed in the measurement chamber to the microcontroller can be divided into two parts. The simple power supply of the LED with a fixed series resistor of 220 Ω and the measuring circuit which converts the current through the phototransistor into a voltage difference with the help of a variable 25 kΩ resistor (potentiometer). This voltage difference is then measured by an external 10 bit ADC (MCP3021 from Microchip[6]) which is connected to the microcontroller. The exact circuit diagram is shown in Figure 3.24.

The voltage measured by the ADC can, depending on the selected mode, either be output directly on the display of the SmaEPhos or used to calculate the optical

[6] https://www.microchip.com/en-us/product/MCP3021, accessed January 16, 2023

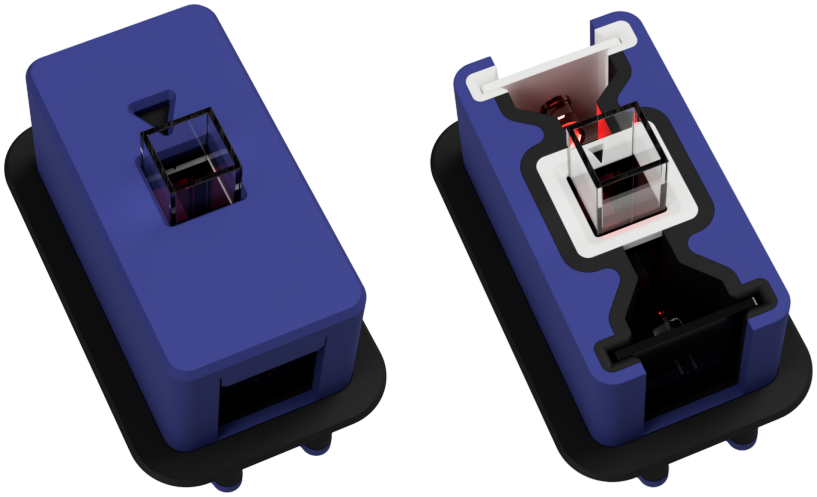

Figure 3.23: Measuring Chamber of the SmaEPho; With and Without Cover

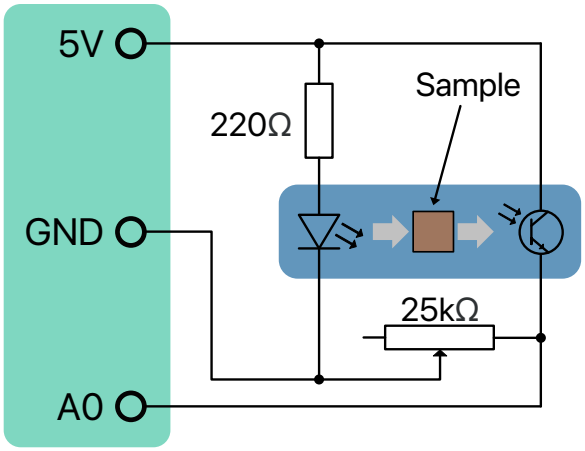

Figure 3.24: Circuit Diagram of the Photometric Measuring Setup

density. Therefore, the zero point must first be set using the blank. The blank sample should include all the components that go into the measurement of the sample, with the sole exception of the substance to be analyzed. After insertion, the resistance of the potentiometer is adjusted so that the voltage across the potentiometer is exactly 3.9 V. This value was defined during the development and is used in the calculation of the optical density in the software of the SmaEPho. Starting from this zero point, the optical density of the following samples is calculated. In order to obtain usable measurement results for an educational environment despite the simple structure of the photometric measurement unit, a quadratic regression to previously determined measurement values was chosen for the calculation of the optical density in SmaEPho. For this purpose, a number of samples for each LED were measured

with the SmaEPho as well as with a professional laboratory photometer (Agilent Technologies, Cary 60). The voltage values measured on the SmaEPho were then normalized by the specified blank value of 3.9 V and adjusted to the optical density measured by the laboratory photometer using a quadratic approximation. This procedure makes it possible to directly compensate for inaccuracies and non-linearities in the measurement setup but also involves considerable effort due to the large series of measurements required for calibration.

Analysis and Evaluation

The aim of the photometric measuring system is clearly to demonstrate the basic operation of a photometric measuring device. Therefore, when designing the measuring system, more emphasis was placed on a simple circuit and standard components than on absolute accuracy. As light sources with a limited range in wavelengths, standard LEDs with various peak wavelengths are used in our case to cover the different measurement ranges (470 nm, 530 nm, 590 nm, 620 nm, 660 nm). The spectral full width at half maximum (FWHM) of the LEDs are approx. 60 nm, which results in a much wider scattered light than what is used in modern laboratory photometers. The latter operates in the range of a few nanometers in width. A standard phototransistor (SFH 300 from Osram) with a preferably linear behavior between irradiance and current is used to measure the luminous intensity. The phototransistor is connected in series to an adjustable resistor and the voltage dropping across the resistor is measured by the ADC. In this way, a direct correlation can be established between the measured voltage irradiance.

To calibrate the measuring system, the reference point must first be set using a blank sample, including all dissolved components in the sample solution, with the exclusion of the substance to be analyzed. After inserting the blank sample into the measuring chamber, the resistance of the potentiometer is adjusted so that the voltage across the resistor is exactly 3.9 V, or the value of *Optical Density* (OD) is 0.00. This value was specifically defined in the development and is stored in the calculation of the optical density in the software of the SmaEPhos.

As described in chapter 3.3.3, a quadratic approximation on pre-determined measurements with a laboratory photometer was used to determine the optical density in order to compensate for possible non-linearities and inaccuracies in advance. To evaluate the system, a series of measurements were again performed in comparison with the laboratory photometer. A colorimetric detection reaction was used to evaluate the OD of a standard series with 12 different phosphates (PO_4) concentrations in mg L^{-1} (0.01; 0.05; 0.1; 0.2; 0.35; 0.5; 0.75; 1; 1.5; 2; 3.5; 5) in triplicates measured on the SmaEPho as well as on the laboratory photometer for each of the LEDs. Figure 3.25 shows the mean values of the difference, i.e., the potential error of the optical density between SmaEPho and the laboratory photometer for each concentration of the measured samples. The SmaEPho displays the optical density to two decimals

only. This means that the display error is in the range of ± 0.01 for almost all of our measurements. However, the results also show higher deviations in the limit range at higher and lower concentrations at wavelengths 620 nm and 660 nm. Here, optimization possibilities remain open. For simple measurements in the educational field, such as the determination of the concentration of nitrate, nitrite, or phosphate ion to examine water samples, or for the determination of growth curves of an algae culture, the results are more than sufficient.

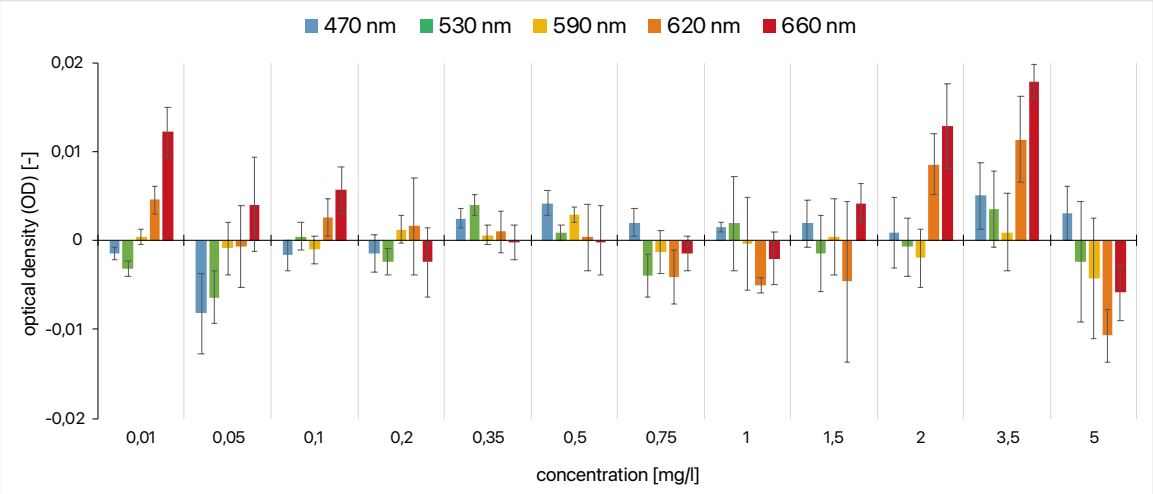

Figure 3.25: Shown are the Mean Values of the Difference in Optical Density between SmaEPho and the Laboratory Photometer for the Concentrations of Phosphate Ions in mg L^{-1} (0.01; 0.05; 0.1; 0.2; 0.35; 0.5; 0.75; 1; 1.5; 2; 3.5; 5) Measured in Triplicates by a Colorimetric Detection Reaction; The Error Bar Corresponds to the Standard Deviation [31]

3.3.4 Cable and Component Tracking

A key feature of the SmaEPhos is the tracking of each pluggable component. This includes not only the cable connections but also the components such as the resistor, the phototransistor, and the various LEDs. Each component can be uniquely identified and mapped to a corresponding position. This not only enables precise synchronization of the digital twin but also various analyses and evaluations. The technology that is used for this purpose is based on the cable tracking system presented in 3.2.3. The one-wire protocol[7] is still used as the communication protocol. Also, the 64 bit ID of a 1 kbit *Electrically Erasable Programmable Read-Only Memory* (EEPROM) chip (DS2431 from Maxim) which is installed in each component serves as unique identification (Figure 3.26). However, the implementation of the master that reads the ID on each socket has been modified. On the SmaEPho a total of 73 sockets have to be monitored (three on the microcontroller part, 64 on the breadboard, four next to the measurement chamber, one for the LED, and one for the phototransistor).

[7] https://www.analog.com/en/product-category/1wire-devices, accessed January 16, 2023

To still achieve a reasonable response time, a total of nine masters were implemented in parallel on the small field-programmable gate array (FPGA; iCE40HX8K from Lattice Semiconductor Corporation). Each master is multiplexing over eight respectively nine sockets and reports detected changes to the microcontroller. The detection of multiple clients per socket, which is used if plugs can be stacked on top of each other, is not required on the SmaEPho and is therefore disabled in the software.

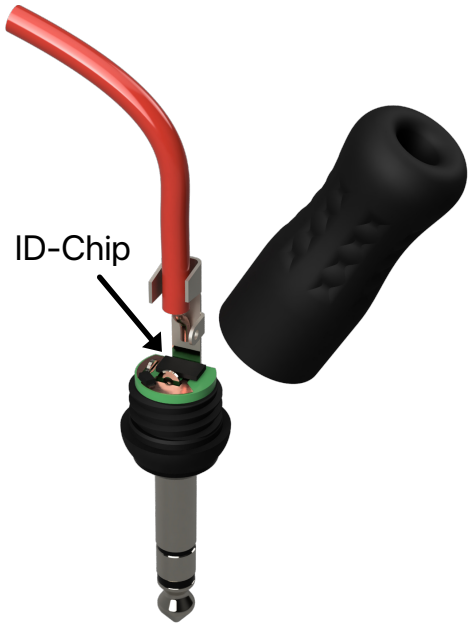

Figure 3.26: Open Cable Plug with Integrated ID-Chip

Evaluation

In addition to the actual ID of the EEPROM chip installed in each component, a *Cyclic Redundancy Check* (CRC) is transmitted. This ensures the reliable detection of transmission errors. Through the use of a single master interface to query up to nine slots one after the other, the maximum latency between two queries in the same slot is around 135 ms. For processing and transmission of the data to the digital twin, a maximum latency of 25 ms could be determined.

3.3.5 Reliability

Reliability is also an important factor in the development of the SmaEPho. Especially when used in studies, which often have a tight schedule, the device must operate with no errors. Since the focus of the SmaEPhos is on experimental research, situations that could potentially lead to a defect in the hardware, e.g. due to a short circuit provoked on the breadboard, are unavoidable and often even deliberate. To protect the hardware, such faults must be reliably intercepted and, at best, also detected in the software so that the appropriate reaction can be executed. Therefore, digital isolators (Si8600AB-IS from Skyworks[8]) were used to isolate any connection between the internal sensor electronics and the externally accessible contacts. Furthermore, numerous circuits for monitoring and preventing excessive currents and potentially dangerous voltages were installed. Potential faults such as a short circuit or excessive current at the LED are detected by the hardware, interrupted and a corresponding message is forwarded directly to the software or the digital twin. Figure 3.27 shows the robust transport case of the SmaEPho with custom-made foam inserts and storage solutions to protect the SmaEPho and the necessary accessories during transport.

Figure 3.27: SmaEPho with Transport-Case and Accessories

[8] https://www.skyworksinc.com/en/Products/Isolation/Si86xx-Digital-Isolators/Si8600AB-IS, accessed January 16, 2023

3.3.6 Digital Twin/Shadow

The app, which forms the digital twin of the SmaEPho, runs on an iPad. It is based on Apple's ARKit[9] and is connected to the physical SmaEPho via the BLE interface. The protocol is identical to the one used in 3.2.5, but with different packet identifiers. The received data is used to display the exact state of the SmaEPho using a three-dimensional model of the SmaEPho and all its components. In addition, warnings are issued in the event of short circuits, for example. Furthermore, the data is also stored in special log files for later analysis and further processing. Configurations on the SmaEPho can also be changed via the app. This applies, for example, to different measurement modes such as voltage ranges or direct conversion to optical density. In its current state, the digital twin serves more as a digital shadow. It represents the current state of the physical SmaEPho and can, for example, be used in a teaching-learning context in the form of an additional presentation level, as a demonstrator. In the future, additional representation modes will be added, e.g. a more detailed evaluation of the measurement results with automatically generated diagrams. In addition, it is planned to add the possibility of interaction on the digital twin in order to use it independently of the physical SmaEPho for remote learning settings.

The expansion and extensive use of the data of the digital twin is planned in future research projects. The platform presented in this section, consisting of the physical SmaEPho and the wirelessly connected digital twin, forms a fundamental cornerstone for the planned research work based on it. An initial study to evaluate the usability of the SmaEPho in which 21 students evaluated the SmaEPho has already been completed by Ms. Lena Geuer and published in [31]. In this study, the SmaEPho hardware achieved an excellent system usability score. Furthermore, very positive feedback from the community has already been obtained at several trade fairs and conferences.

[9] https://developer.apple.com/augmented-reality/arkit/, accessed January 16, 2023

Chapter 4

Conclusion and Future Work

The IoT, with its diverse and constantly growing sub-areas, continuously raises new challenges for the involved components. The systems and methods presented in this thesis contribute significantly to new developments in the segments of the Industrial IoT and the Educational IoT.

In the first part of the thesis, a system for secure communication of ultra-low power edge devices in the Industrial IoT context was presented, analyzed, and optimized in terms of latency and energy. The fundamental approach of using the well-established TLS protocol as a security layer brings many advantages in terms of compatibility, future-proofing, and flexibility of the underlying cryptographic problems. However, the primary goal in the development of the TLS protocol was to achieve high-security requirements rather than to be used on resource-constrained devices. As a result, it is often not considered for solutions using devices with very limited resources.

An initial software solution implemented on a low-power edge device confirmed this opinion, by taking about 40 s to establish a single connection, which modern computers or smartphones can do in a few hundred milliseconds or even less. However, in Section 2.4 it was shown that by using state-of-the-art hardware accelerators, which are already integrated into many modern SoCs, the time required to establish a connection could be reduced to almost a quarter of the time required by a pure software solution. Furthermore, the energy required has even been reduced by a factor of 10. The use of specialized hardware accelerators, though, focuses purely on optimizing cryptographic algorithms. In the next step (Section 2.5), a holistic analysis and optimization of the entire system focused on energy and latency reduction was carried out. This reduced the required time by a factor of 8 and the energy by more than a factor of 2.5. The resulting system can operate for many years on a single AA lithium cell, with one connection establishment every hour, and still leave plenty of energy for the operation and data processing of the actual sensor.

In fact, the system is so energy-efficient that it can be powered by a thermoelectric energy harvester utilizing temperature differences of only a few degrees Kelvin.

Chapter 2.6 therefore evaluates possible energy storage devices in the system context in more detail. These energy storage devices are used to collect the energy provided by the TEG over a longer period so that it can then be used to establish a connection. It was shown that both the leakage current and the internal resistance, with its resulting ability to deliver larger current peaks, are essential parameters for the selection of the storage device. Further analysis provided an estimation between the temperature difference available at the TEG and the resulting minimum time between successive connections, i.e. the interval at which a connection can be established, differentiated for each type of storage device.

In conclusion, after holistic analyses and optimizations, the TLS protocol is also suitable for use on ultra-low-power edge devices powered by a TEG to secure data transmission in the Industrial IoT. Furthermore, the system shows that limited energy budgeting should not be used as an excuse for insufficient or weakly protected data transfer. Hence, the system design and the methods for optimizing energy efficiency shown in this thesis should also serve as a starting point for further applications in scientific research (Section 2.8) as well as in other areas of the IoT.

In the second part of the thesis, two innovative learning platforms are presented, each of which is setting new standards for smart learning platforms in their respective thematic domains. Both platforms combine a dedicated experimentation environment with application-specific sensors to measure a wide range of parameters, providing new possibilities for analysis and scientific research. These include sensors for determining electrical current and voltage or a measuring chamber for photometric measurements. In addition, special connectors and a customized tracking system are used to capture further environmental parameters.

The use of the "Sensors for Augmented Electrical Experiments" in numerous scientific studies and publications [30, 32–35, 37, 156] emphasizes the added value for the scientific community. Furthermore, the continuous use in schools and universities, as well as further planned research projects based on the presented hardware, show the benefit of the developed solution. Additional research projects are also planned with the Smart Measurement Platform for Photometry in Education (SmaEPho). Here, particular emphasis will be placed on the expansion of the digital twin and its interaction with the learner. Moreover, the already available, recorded user interaction data from the usability study will form the basis for an extended analysis and evaluation approach. Both systems provide a deeper and more targeted insight into the learning process and thus enable the investigation of many complex questions in educational research. They also build an essential foundation for KI-supported analysis of the learning process and extend established systems for experimental research with smart components.

Chapter 5

Zusammenfassung

Die enormen Mengen an digitalen Daten, die in der Welt vorhanden sind, bestehen schon lange nicht mehr aus lediglich gezielt von Menschen veröffentlichten Informationen wie Fotos, Nachrichten oder Blogs; vielmehr werden die Daten von Servern vollautomatisch gesammelt, verarbeitet und gespeichert. Darüber hinaus werden immer mehr Geräte "intelligent" gemacht, indem sie über Netzwerkschnittstellen Teil eines lokalen Netzwerks oder des Internets werden, in dem Daten ausgetauscht, gespeichert und genutzt werden. Dieses Konzept der vernetzten Dinge und Geräte wird als "Internet of Things" (IoT) bezeichnet. Das Anwendungsgebiet erstreckt sich hierbei ausgehend von kleinsten Gadgets bis hin zu hochkomplexen Industrieanlagen, die mit entsprechenden Sensoren und Aktoren ausgestattet sind.

Im Laufe der Zeit haben sich verschiedene Bezeichnungen für die unterschiedlichen Anwendungsbereiche etabliert. Im privaten Bereich wird zum Beispiel häufig vom "Consumer IoT" gesprochen, im industriellen Kontext spricht man wiederum vom "Industrial IoT" oder von "Industrie 4.0". Abwandlungen wie "Educational-IoT" oder "Internet of Medical Things" (IoMT) stehen wiederum für vernetzte Geräte im jeweiligen Bereich. Eine Herausforderung, die sich über alle Bereiche des IoTs erstreckt, ist das Datenmanagement. Hierzu gehört die Erfassung der Daten, der Transport der Daten sowie die Auswertung und Nutzung der Daten. Im Kontext dieser Arbeit habe ich mich mit zwei dieser Bereiche befasst: der Übertragung der Daten und der Erfassung der Daten.

Datenübertragung - Bereich Industrial IoT (Kapitel 2)

Gerade im Kontext des Industrial IoTs werden häufig besondere Anforderungen an die Übertragung der Daten gestellt. Hierzu zählen unter anderem die Integrität und Verschlüsslung der Daten, wie auch Ansprüche an die Flexibilität der verwendeten Übertragungstechnologie und den resultierenden Energiebedarf des Gerätes. Ein Beispiel hierzu stellt das Feld der vorausschauende Wartung (engl. predictive maintenance) dar. Ziel ist es dabei, durch Sensor- und Prozessdaten, einen möglichst optimalen

und dynamischen Wartungsplan zu erstellen, um somit sowohl Wartungskosten als auch Ausfallzeiten zu reduzieren. Zur Gewinnung der nötigen Sensordaten werden bevorzugt flexible und möglichst von der Infrastruktur unabhängige Sensorgeräte genutzt, da diese auch ohne erhöhten Aufwand an bereits bestehenden Maschinen nachgerüstet werden können. Die Geräte sind demnach in der Regel batteriebetrieben und verfügen gleichzeitig über eine drahtlose Datenverbindung. Das limitierte Energiebudget steht allerdings in direktem Kontrast zu den durch die drahtlose Datenverbindung noch weiter gestiegenen Anforderungen an die Datensicherheit. Der zusätzliche Overhead zum sicheren Verbindungsaufbau und der Verschlüsslung der Daten ist für moderne Server, PCs oder Smartphones relativ gering. Für die ressourcenbeschränkten eingebetteten Systeme stellt dies jedoch eine große Herausforderung dar.

Kapitel 2 dieser Arbeit befasst sich daher mit der sicheren Datenübertragung im Kontext des Industrial IoTs mit dem Schwerpunkt der Energieeffizienz. Ausgehend von einem konkreten branchenbezogenen Anwendungsfall im Bereich der vorausschauenden Wartung werden in den Abschnitten 2.1-2.3 die damit verbundenen Anforderungen identifiziert und für eine anschließende Design Space Exploration genutzt, die mögliche Technologien, Setups und Lösungen evaluiert und bewertet. Die Ergebnisse werden in Form eines aggregierten Industrial IoT Netzwerksystems dargestellt, welches die Grundlage für die folgenden Untersuchungen bildet. Sowohl die Design Space Exploration als auch das daraus resultierende Industrial IoT Netzwerksystem können als Referenz für andere Anwendungsdomänen genutzt werden.

Die Verwendung von Kryptografischen Hardwarebeschleunigern zur Verbesserung der Geschwindigkeit und Energieeffizienz von kryptografischen Operationen ist ein gängiger Ansatz zur Optimierung eingebetteter Systeme. Im Abschnitt 2.4 wird die allgemeine Durchführbarkeit des zuvor definierten Aufbaus bewertet und die erwartete Batterielaufzeit dargestellt. Darüber hinaus werden die Auswirkungen einer isolierten Optimierung durch die Verwendung verschiedener Kryptografischer Hardwarebeschleuniger im TLS-basierten Industrial IoT Netzwerksystem mit geringem Stromverbrauch gezeigt.

Abschnitt 2.5 präsentiert einen ganzheitlichen Analyseansatz für das TLS-basierte Low-Power Industrial IoT Netzwerksystem, der limitierende Faktoren und entsprechende Optimierungen identifiziert. Das daraus resultierende System ist meines Wissens das erste System, das die Lücke zwischen der Verwendung etablierter Sicherheitsstandards und Geräten mit stark begrenztem Energie Budget im Bereich der Industrial IoT Netzwerksysteme schließt.

Abgeschlossen wird dieses Kapitel mit einer quantitativen Bewertung des Einsatzes von thermoelektrischem Energy Harvesting in einem TLS-basierten Industrial IoT Netzwerksystem unter Berücksichtigung verschiedener Speichertechnologien in Abschnitt 2.6. Die Ergebnisse ermöglichen eine direkte Korrelation zwischen der

nutzbaren Temperaturdifferenz des Energy Harvesters und dem daraus resultierenden minimalen Zeitintervall für die Akkumulation der Energie, die für den Aufbau einer neuen Verbindung zum Senden von Daten an die Cloud erforderlich ist.

Die Beiträge dieses Kapitels wurden bereits in wissenschaftlichen Fachzeitschriften- und Konferenzartikeln veröffentlicht (TLS-Level Security for Low Power Industrial IoT Network Infrastructures [25]; Analysis and Optimization of TLS-based Security Mechanisms for Low Power IoT Systems [26]; Exploration of Thermoelectric Energy Harvesting for Secure, TLS-based Industrial IoT Nodes [27]) Außerdem haben sie zu Veröffentlichungen im Bereich der Post-Quantum-Kryptographie beigetragen [28, 29].

Datenerfassung - Bereich Educational IoT (Kapitel 3)

Der zweite Teil meiner Arbeit beschäftigt sich mit der Datenerfassung im Kontext des Educational IoTs. Wie in vielen anderen Bereichen des Lebens hält die Technologie auch Einzug in unsere Lernumgebungen. Diese sogenannten "smarten" Lernumgebungen sind ein wesentlicher Beitrag zum modernen Lernen, zur Lernanalyse und zur Lernforschung. Sie bestehen aus einer einzelnen App, einer komplexen AR-Lösung oder einer kompletten VR-Umgebung. Die Qualität und die Menge der erfassten Sensordaten sowie die Benutzerfreundlichkeit stellen entscheidende Kriterien für den Nutzen der intelligenten Lernplattform dar. Eine AR-basierte Lernumgebung zeichnet sich beispielsweise durch die digitale Interaktion mit physisch vorhandenen Objekten aus. Eine notwendige Voraussetzung hierfür ist, neben der Kenntnis der physischen Position des AR-Gerätes im Verhältnis zur Umgebung, auch die Kenntnis der Position der Objekte, mit denen interagiert werden soll. Um das volle Potenzial einer solchen interaktiven Lernumgebung auszuschöpfen, müssen möglichst viele Informationen aus der physischen Welt digital verfügbar sein. So können dadurch zum Beispiel Messwerte in einem Experiment direkt mit den zugehörigen Objekten verknüpft dargestellt werden oder Aufgaben individuell an den Lernenden angepasst werden. Die Sensorik solcher Systeme stellt häufig eine große Herausforderung dar. Entscheidend ist, dass die integrierte Technologie weder das eigentliche Experiment noch die lernende Person negativ beeinflussen dürfen. Zugleich muss das System eine hohe Messgenauigkeit bieten und robust gegenüber äußeren und unvorhergesehenen Einflüssen sein. Weitere Herausforderungen sind die oft komplexen Multisensorsysteme, Budgetbeschränkungen, Latenz- und Reaktionszeiten, Datenschutzanforderungen, Stromversorgung sowie Datenkonnektivität. In der Folge werden die intelligenten Lernplattformen, welche einen wesentlichen Bestandteil der Bildungsforschung darstellen, selbst Teil wissenschaftlicher Fragestellungen im Bereich der Elektro- und Informationstechnik. Sie bilden einen speziellen Anwendungsfall für Multisensorsysteme im Kontext des IoTs, dessen Konzepte und Erkenntnisse auf viele andere Anwendungen übertragen werden können.

In dieser Arbeit werden zwei smarte Lernplattformen mit unterschiedlichen Themenschwerpunkten für den Einsatz in Schulen und Universitäten vorgestellt. Die erste Lernumgebung (Abschnitt 3.2) besteht aus mehreren mit Sensoren bestückten Boxen, die mit Hilfe spezieller Kabel miteinander verschaltet werden und so für Experimente im elektrischen Schaltkreis genutzt werden können. Die Plattform wurde hierbei gezielt für den Einsatz in einer AR-Umgebung entwickelt und bietet ein Messsystem für Strom und Spannung, ein Trackingsystem für Kabel und ein 2D-Positionierungssystem zur Lokalisierung der Experimentkomponenten auf der Tischoberfläche. Neben dem Aufbau der Sensorlösungen wird in den jeweiligen Abschnitten auch eine Bewertung der Lösung vorgestellt. Außerdem wird die Datenübertragung zwischen den Geräten näher erläutert.

Die zweite smarte Lernplattform (Abschnitt 3.3) besteht aus einer Messplattform für photometrische Experimente. Die Hauptbestandteile sind hierbei eine photometrische Messeinheit, ein elektrisches Steckbrett zum Aufbau der notwendigen Schaltung und eine Microcontroller-Einheit mit Display zur Auswertung und Anzeige der Messwerte. Zur Erfassung des Schaltungsaufbaus und zur Verfolgen aller beweglichen Objekte auf der Lernplattform wurde ein spezielles Trackingsystem entwickelt. Die zugehörige App, welche den digitalen Zwilling der Lernplattform bildet, ist dadurch in der Lage, den exakten Experimentierablauf zu erfassen und zu visualisieren. Weiter dienen die gewonnenen Daten zur Analyse des Lernprozesses und als Basis für weitergehende Forschungsfragen in diesem Bereich.

Beide Lernumgebungen wurden in mehreren Projekten und Studien mit Studenten und Schülern eingesetzt und erprobt. Sie bilden eine wichtige Basis zur Bearbeitung diverser Forschungsfragen in der Lern- und Didaktik-Forschung.

Die Beiträge dieses Kapitels wurden bereits in wissenschaftlichen Fachzeitschriften- und Konferenzartikeln veröffentlicht (Smart Sensors for Augmented Electrical Experiments [30]; SmaEPho–Smart Photometry in Education 4.0 [31]). Außerdem haben sie zu weiteren Veröffentlichungen im Bereich der Smarten Lernumgebungen beigetragen ([32–37]).

Acronyms

6Lo	IPv6 over Networks of Resource-constrained Nodes 23
6LoWPAN	IPv6 over Low power Wireless Personal Area Network 23, 25, 29
ADC	Analog to Digital Converter 58, 62, 82
AES	Advanced Encryption Standard 18, 20, 22, 26, 31
AFH	Adaptive Frequency Hopping 25
AI	Artificial Intelligence 55
AR	Augmented Reality 2, 3, 6, 11, 52, 55, 56, 112
ASIC	Application-Specific Integrated Circuit 73
BLE	Bluetooth Low Energy 11, 23–26, 29, 35, 42, 44, 52, 65, 74, 76, 88
BMC	Biphase-Mark-Code 69, 70, 73, 112
BSI	Bundesamt für Sicherheit in der Informationstechnik 15, 18
CAN FD	Controller Area Network Flexible Data-Rate 14
CHA	Cryptographic Hardware Accelerator 6, 9, 20, 30–36
CLT	Cognitive Load Theory 51, 53, 54
CPU	Central Processing Unit 26, 33, 36
CRC	Cyclic Redundancy Check 86
CTLS	Compact TLS 21
CTML	Cognitive Theory of Multimedia Learning 52–54
DH	Diffie-Hellman 18, 19
DIY	Do It Yourself 4
DSA	Digital Signature Algorithm 19, 22, 95
DTLS	Datagram TLS 26, 27, 30
ECC	Elliptic Curve Cryptography 19, 20, 26, 30, 31, 37, 111
ECDH	Elliptic Curve Diffie-Hellman 31
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral 22, 31, 48
ECDSA	Elliptic Curve DSA 22, 31

ECL Extraneous Cognitive Load 53, 54
eeDTLS Energy Efficient Datagram TLS 21
EEPROM Electrically Erasable Programmable Read-Only Memory 85, 86

FHSS Frequency Hopping Spread Spectrum 25
FIFO First In First Out 73
FPGA Field Programmable Gate Array 62, 73–75, 86, 112

GCL Germane Cognitive Load 54
GCM Galois/Counter Mode 22
GPIO General Purpose Input/Output 33, 34

HMD Head-Mounted Display 56

I2C Inter-Integrated Circuit 31, 32
IC Integrated Circuit 13
ICL Intrinsic Cognitive Load 53, 54
IETF Internet Engineering Task Force 21, 23
IoMT Internet of Medical Things 1, 5
IoT Internet of Things 1, 2, 4–7, 9–18, 20, 22, 23, 26–28, 30, 33, 38–40, 44, 46, 48, 51, 89, 90, 93, 111
IP Internet Protocol 20, 22, 23, 29, 34, 35
IPsec Internet Protocol Security 20
IPv4 Internet Protocol Version 4 23
IPv6 Internet Protocol Version 6 . . . . . 23–25, 28, 29, 95

LAN Local Area Network 24
LED Light-Emitting Diode 82–85, 87
LFSR Linear Feedback Shift Register 69, 70, 73, 112
LIDAR Light Detection and Ranging 64

MAC Message Authentication Code 21
MD5 Message-Diges Algorithm 5 19
MEMS Micro-Electro-Mechanical Systems 2
MER Multiple External Representations 52–54
MLCC Multi Layer Ceramic Capacitor 40, 41, 44–46, 48, 111
MQTT Message Queuing Telemetry Transport 27–29, 31, 39, 42

NFC Near Field Communication 26
NIST National Institute of Standards and Technology 31, 49

OD	Optical Density 84
OOTX	Omnidirectional Optical Transmitter 69, 74
PFS	Perfect Forward Secrecy 29, 31
PKI	Public Key Infrastruktur 19, 22, 26, 49
PPTC	Polymeric Positive Temperature Coefficient 58
PQC	Post-Quantum Cryptography 19–21, 26, 49
PSK	Pre-shared Key 29
RAM	Random-Access Memory 13, 14, 26, 34
RFID	Radio-Frequency Identification 1, 64
RSA	Rivest Shamir Adleman 19, 20, 26, 30, 31
SHA-2	Secure Hashing Algorithm 2 . . . . . 19, 20, 22, 26, 31
SHA-3	Secure Hashing Algorithm 3 19
SmaEPho	Smart Education Photometer 52, 78–88, 112, 113
SoC	System on Chip 14, 15, 18, 20, 25, 26, 28, 30–32, 35, 41, 44, 73, 75, 89
SSH	Secure Shell 20
STEM	Science Technology Engineering Mathematics 11, 51, 52, 55
TCP	Transmission Control Protocol 21
TEG	Thermoelectric Generator 6, 10, 38–40, 43, 44, 48, 90, 111
TLS	Transport Layer Security . 5, 9, 10, 20–23, 25–27, 29–33, 35–39, 41, 42, 49, 89, 90, 92, 93, 95, 96, 111
TRNG	True Random Number Generator 26
TRS	Tip Ring Sleeve 62
TVS	Transient Voltage Suppressor 58
UART	Universal Asynchronous Receiver Transmitter 34, 73
USB	Universal Serial Bus 14
VBT	Voltage-triggered Bidirectional Thyristor 58
VPN	Virtual Private Network 20
VR	Virtual Reality 2
WLAN	Wireless Local Area Network 4, 24, 25, 27, 30
WPAN	Wireless Personal Area Network 23

Bibliography

[1] D. R.-J. G.-J. Rydning, J. Reinsel, and J. Gantz. The digitization of the world from edge to core. *Framingham: International Data Corporation*, 16, 2018.

[2] G.-J. Hwang. Definition, framework and research issues of smart learning environments - a context-aware ubiquitous learning perspective. *Smart Learning Environments*, 1(1):4, Dec. 2014.

[3] Kinshuk, N.-S. Chen, I.-L. Cheng, and S. W. Chew. Evolution Is not enough: Revolutionizing Current Learning Environments to Smart Learning Environments. *International Journal of Artificial Intelligence in Education*, 26(2):561–581, June 2016.

[4] B. H. Limbu, H. Jarodzka, R. Klemke, and M. Specht. Can You Ink While You Blink? Assessing Mental Effort in a Sensor-Based Calligraphy Trainer. *Sensors*, 19(14):3244, July 2019.

[5] D. Di Mitri, J. Schneider, K. Trebing, S. Sopka, M. Specht, and H. Drachsler. Real-Time Multimodal Feedback with the CPR Tutor. In I. I. Bittencourt, M. Cukurova, K. Muldner, R. Luckin, and E. Millán, editors, *Artificial Intelligence in Education*, volume 12163, pages 141–152. Springer International Publishing, Cham, 2020. Series Title: Lecture Notes in Computer Science.

[6] D. Di Mitri, J. Schneider, M. Specht, and H. Drachsler. From signals to knowledge: A conceptual model for multimodal learning analytics. *Journal of Computer Assisted Learning*, 34(4):338–349, Aug. 2018.

[7] O. R. E. Pereira and J. J. P. C. Rodrigues. Survey and analysis of current mobile learning applications and technologies. *ACM Computing Surveys*, 46(2):1–35, Nov. 2013.

[8] O. Bodensiek, D. Sonntag, N. Wendorff, G. Albuquerque, and M. Magnor. Augmenting the fine beam tube: From hybrid measurements to magnetic field visualization. *The Physics Teacher*, 57(4):262–263, Apr. 2019.

[9] M. P. Strzys, M. Thees, S. Kapp, and J. Kuhn. Smartglasses in STEM laboratory courses – the augmented thermal flux experiment. In *2018 Physics Education Research Conference Proceedings*, Washington, DC, Jan. 2019. American Association of Physics Teachers.

[10] C. Lindner, A. Rienow, and C. Jürgens. Augmented Reality applications as digital experiments for education – An example in the Earth-Moon System. *Acta Astronautica*, 161:66–74, Aug. 2019.

[11] X. Zhou, L. Tang, D. Lin, and W. Han. Virtual & augmented reality for biological microscope in experiment education. *Virtual Reality & Intelligent Hardware*, 2(4):316–329, Aug. 2020.

[12] W.-K. Liou and C.-Y. Chang. Virtual reality classroom applied to science education. In *2018 23rd International Scientific-Professional Conference on Information Technology (IT)*, pages 1–4, Zabljak, Feb. 2018. IEEE.

[13] D. Hamilton, J. McKechnie, E. Edgerton, and C. Wilson. Immersive virtual reality as a pedagogical tool in education: a systematic literature review of quantitative learning outcomes and experimental design. *Journal of Computers in Education*, 8(1):1–32, Mar. 2021.

[14] R. Liu, L. Wang, J. Lei, Q. Wang, and Y. Ren. Effects of an immersive virtual reality-based classroom on students' learning performance in science lessons. *British Journal of Educational Technology*, 51(6):2034–2049, Nov. 2020.

[15] M. R. Mutizwa, F. Ozdamli, and D. Karagozlu. Smart Learning Environments during Pandemic. *Trends in Higher Education*, 2(1):16–28, Jan. 2023.

[16] M. Achouch, M. Dimitrova, K. Ziane, S. Sattarpanah Karganroudi, R. Dhouib, H. Ibrahim, and M. Adda. On Predictive Maintenance in Industry 4.0: Overview, Models, and Challenges. *Applied Sciences*, 12(16):8081, Aug. 2022.

[17] T. Gebremichael, L. P. I. Ledwaba, M. H. Eldefrawy, G. P. Hancke, N. Pereira, M. Gidlund, and J. Akerberg. Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges. *IEEE Access*, 8:152351–152366, 2020.

[18] U. Association, editor. *Proceedings of the Second Workshop on Real, Large Distributed Systems: December 13, 2005, San Francisco, CA, USA*. 2005.

[19] X. Jiang, M. Lora, and S. Chattopadhyay. An Experimental Analysis of Security Vulnerabilities in Industrial IoT Devices. *ACM Transactions on Internet Technology*, 20(2):1–24, May 2020.

[20] H. Hellaoui, M. Koudil, and A. Bouabdallah. Energy-efficient mechanisms in security of the internet of things: A survey. *Computer Networks*, 127:173–189, Nov. 2017.

[21] M. Frustaci, P. Pace, and G. Aloi. Securing the IoT world: Issues and perspectives. In *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, pages 246–251, Helsinki, Finland, Sept. 2017. IEEE.

[22] M. Frustaci, P. Pace, G. Aloi, and G. Fortino. Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. *IEEE Internet of Things Journal*, 5(4):2483–2495, Aug. 2018.

[23] O. Yerlikaya and G. Dalkiltc. Authentication and Authorization Mechanism on Message Queue Telemetry Transport Protocol. In *2018 3rd International Conference on Computer Science and Engineering (UBMK)*, pages 145–150, Sarajevo, Sept. 2018. IEEE.

[24] S. P. Gochhayat, C. Lal, L. Sharma, D. P. Sharma, D. Gupta, J. A. M. Saucedo, and U. Kose. Reliable and secure data transfer in IoT networks. *Wireless Networks*, 26(8):5689–5702, Nov. 2020.

[25] J. Mades, G. Ebelt, B. Janjic, F. Lauer, C. C. Rheinlander, and N. Wehn. TLS-Level Security for Low Power Industrial IoT Network Infrastructures. In *2020 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 1720–1721, Grenoble, France, Mar. 2020. IEEE.

[26] F. Lauer, C. C. Rheinlander, C. Kestel, and N. Wehn. Analysis and Optimization of TLS-based Security Mechanisms for Low Power IoT Systems. In *2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID)*, pages 775–780, Melbourne, Australia, May 2020. IEEE.

[27] F. Lauer, M. Schöffel, C. C. Rheinländer, and N. Wehn. Exploration of Thermoelectric Energy Harvesting for Secure, TLS-Based Industrial IoT Nodes. In B. Tekinerdogan, Y. Wang, and L.-J. Zhang, editors, *Internet of Things – ICIOT 2022*, volume 13735, pages 92–107. Springer Nature Switzerland, Cham, 2023. Series Title: Lecture Notes in Computer Science.

[28] M. Schöffel, F. Lauer, C. C. Rheinländer, and N. Wehn. On the Energy Costs of Post-Quantum KEMs in TLS-based Low-Power Secure IoT. In *Proceedings of the International Conference on Internet-of-Things Design and Implementation*, pages 158–168, Charlottesvle VA USA, May 2021. ACM.

[29] M. Schöffel, F. Lauer, C. C. Rheinländer, and N. Wehn. Secure IoT in the Era of Quantum Computers—Where Are the Bottlenecks? *Sensors*, 22(7):2484, Mar. 2022.

[30] S. Kapp, F. Lauer, F. Beil, C. C. Rheinländer, N. Wehn, and J. Kuhn. Smart Sensors for Augmented Electrical Experiments. *Sensors*, 22(1), 2022.

[31] L. Geuer, F. Lauer, J. Kuhn, N. Wehn, and R. Ulber. SmaEPho–Smart Photometry in Education 4.0. *Education Sciences*, 13(2):136, Jan. 2023.

[32] S. Kapp, M. Thees, F. Beil, T. Weatherby, J.-P. Burde, T. Wilhelm, and J. Kuhn. The Effects of Augmented Reality: A Comparative Study in an Undergraduate Physics Laboratory Course:. In *Proceedings of the 12th International Conference on Computer Supported Education*, pages 197–206, Prague, Czech Republic, 2020. SCITEPRESS - Science and Technology Publications.

[33] S. Kapp, M. Thees, F. Beil, T. Weatherby, J.-P. Burde, T. Wilhelm, and J. Kuhn. Using Augmented Reality in an Inquiry-Based Physics Laboratory Course. In H. C. Lane, S. Zvacek, and J. Uhomoibhi, editors, *Computer Supported Education*, volume 1473, pages 177–198. Springer International Publishing, Cham, 2021. Series Title: Communications in Computer and Information Science.

[34] K. Altmeyer, S. Kapp, M. Thees, S. Malone, J. Kuhn, and R. Brünken. The use of augmented reality to foster conceptual knowledge acquisition in STEM laboratory courses—Theoretical background and empirical results. *British Journal of Educational Technology*, 51(3):611–628, May 2020.

[35] M. Thees, K. Altmeyer, S. Kapp, E. Rexigel, F. Beil, P. Klein, S. Malone, R. Brünken, and J. Kuhn. Augmented Reality for Presenting Real-Time Data During Students' Laboratory Work: Comparing a Head-Mounted Display With a Separate Display. *Frontiers in Psychology*, 13:804742, Mar. 2022.

[36] H. Javaheri, F. Lauer, L. Lauer, K. Altmeyer, R. Brünken, M. Peschel, N. Wehn, and P. Lukowicz. Smart Teaching Materials with Real-Time Augmented Reality Support for Introductory Physics Education. In *Proceedings of the 2022 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pages 53–54, Cambridge United Kingdom, Sept. 2022. ACM.

[37] M. Thees, S. Kapp, K. Altmeyer, S. Malone, R. Brünken, and J. Kuhn. Comparing Two Subjective Rating Scales Assessing Cognitive Load During Technology-Enhanced STEM Laboratory Courses. *Frontiers in Education*, 6:705551, July 2021.

[38] M. V. Natale, M. Jung, K. Kraft, F. Lauer, J. Feldmann, C. Sudarshan, C. Weis, S. Krumke, and N. Wehn. Efficient Generation of Application Specific Memory Controllers. In *The International Symposium on Memory Systems*, pages 233–247, Washington DC USA, Sept. 2020. ACM.

[39] C. C. Rheinlander, F. Lauer, and N. Wehn. A New Method for Predictive Checkpointing in Transiently-Powered IoT Sensor Devices with Thermal Energy Harvesting. In *Conference on Technologies for Sustainability (SusTech)*, accepted but not yet published, 2023. IEEE.

[40] C. Arnold, D. Kiel, and K.-I. Voigt. HOW THE INDUSTRIAL INTERNET OF THINGS CHANGES BUSINESS MODELS IN DIFFERENT MANUFACTURING INDUSTRIES. *International Journal of Innovation Management*, 20(08):1640015, Dec. 2016.

[41] P. Lade, R. Ghosh, and S. Srinivasan. Manufacturing Analytics and Industrial Internet of Things. *IEEE Intelligent Systems*, 32(3):74–79, May 2017.

[42] M. S. Hossain and G. Muhammad. Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring. *Computer Networks*, 101:192–202, June 2016.

[43] Y. Yin, Y. Zeng, X. Chen, and Y. Fan. The internet of things in healthcare: An overview. *Journal of Industrial Information Integration*, 1:3–13, Mar. 2016.

[44] M. A. Iqbal and M. Bayoumi. Secure End-to-End key establishment protocol for resource-constrained healthcare sensors in the context of IoT. In *2016 International Conference on High Performance Computing & Simulation (HPCS)*, pages 523–530, Innsbruck, Austria, July 2016. IEEE.

[45] A. Rey, E. Panetti, R. Maglio, and M. Ferretti. Determinants in adopting the Internet of Things in the transport and logistics industry. *Journal of Business Research*, 131:584–590, July 2021.

[46] G. S. S. Chalapathi, V. Chamola, A. Vaish, and R. Buyya. Industrial Internet of Things (IIoT) Applications of Edge and Fog Computing: A Review and Future Directions. In W. Chang and J. Wu, editors, *Fog/Edge Computing For Security, Privacy, and Applications*, volume 83, pages 293–325. Springer International Publishing, Cham, 2021. Series Title: Advances in Information Security.

[47] P. K. Malik, R. Sharma, R. Singh, A. Gehlot, S. C. Satapathy, W. S. Alnumay, D. Pelusi, U. Ghosh, and J. Nayak. Industrial Internet of Things and its Applications in Industry 4.0: State of The Art. *Computer Communications*, 166:125–139, Jan. 2021.

[48] G. E. Moore. Cramming More Components Onto Integrated Circuits. *Electronics*, pages 114–117, Apr. 1965.

[49] P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. 1995. Publisher: arXiv Version Number: 2.

[50] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni. A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities. *IEEE Communications Surveys & Tutorials*, 22(4):2489–2520, 2020.

[51] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access*, 7:82721–82743, 2019.

[52] J. M. Mcginthy and A. J. Michaels. Secure Industrial Internet of Things Critical Infrastructure Node Design. *IEEE Internet of Things Journal*, 6(5):8021–8037, Oct. 2019.

[53] N. I. of Standards and Technology. Advanced Encryption Standard (AES), 2001.

[54] BSI. BSI Technische Richtlinie BSI TR-02102-1: Kryptographische verfahren: Empfehlungen und Schlüssellängen. BSI TR-02102-1, 2022. Type: techreport.

[55] J. W. Bos, D. A. Osvik, and D. Stefan. Fast Implementations of AES on Various Platforms, 2009. Published: Cryptology ePrint Archive, Paper 2009/501.

[56] S. Didla, A. Ault, and S. Bagchi. Optimizing AES for Embedded Devices and Wireless Sensor Networks. In *Proceedings of the 4th International ICST Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities*, Innsbruck, Austria, 2008. ICST.

[57] S. P. Jadhav and Faculty of Telecommunications, Technical University of Sofia, Bulgaria. Towards Light Weight CryptographySchemes for Resource ConstraintDevices in IoT. *Journal of Mobile Multimedia*, 15(1):91–110, 2020.

[58] S. Kumaran, N. Kailasanathan, and S. Mohan. Review of asymmetric key cryptography in wireless sensor networks. *International Journal of Engineering and Technology (IJET)*, 8:859–862, Jan. 2016.

[59] M. Fritter, N. Ould-Khessal, S. Fazackerley, and R. Lawrence. Experimental Evaluation of Hash Function Performance on Embedded Devices. In *2018 IEEE Canadian Conference on Electrical & Computer Engineering (CCECE)*, pages 1–5, Quebec City, QC, May 2018. IEEE.

[60] J. Balasch, B. Ege, T. Eisenbarth, B. Gérard, Z. Gong, T. Güneysu, S. Heyse, S. Kerckhof, F. Koeune, T. Plos, T. Pöppelmann, F. Regazzoni, F.-X. Standaert, G. Van Assche, R. Van Keer, L. van Oldeneel tot Oldenzeel, and I. von Maurich. Compact Implementation and Performance Evaluation of Hash Functions in ATtiny Devices. In D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, and S. Mangard, editors, *Smart Card Research and Advanced Applications*, volume 7771, pages 158–172. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013. Series Title: Lecture Notes in Computer Science.

[61] H. Cheng, D. Dinu, and J. Großschädl. Efficient Implementation of the SHA-512 Hash Function for 8-Bit AVR Microcontrollers. In J.-L. Lanet and C. Toma, editors, *Innovative Security Solutions for Information Technology and Communications*, volume 11359, pages 273–287. Springer International Publishing, Cham, 2019. Series Title: Lecture Notes in Computer Science.

[62] W. J. Dally, Y. Turakhia, and S. Han. Domain-specific hardware accelerators. *Communications of the ACM*, 63(7):48–57, June 2020.

[63] M. Schöffel, J. Feldmann, and N. Wehn. Code-based Cryptography in IoT: A HW/SW Co-Design of HQC. 2023. Publisher: arXiv Version Number: 1.

[64] P. Kietzmann, L. Boeckmann, L. Lanzieri, T. C. Schmidt, and M. Wählisch. A performance study of crypto-hardware in the low-end IoT, 2021. tex.howpublished: Cryptology ePrint Archive, Paper 2021/058.

[65] G. Panić, O. Stecklina, and Z. Stamenković. An Embedded Sensor Node Microcontroller with Crypto-Processors. *Sensors*, 16(5):607, Apr. 2016.

[66] M. Imran, Z. U. Abideen, and S. Pagliarini. An Experimental Study of Building Blocks of Lattice-Based NIST Post-Quantum Cryptographic Algorithms. *Electronics*, 9(11):1953, Nov. 2020.

[67] J. Xie, K. Basu, K. Gaj, and U. Guin. Special Session: The Recent Advance in Hardware Implementation of Post-Quantum Cryptography. In *2020 IEEE 38th VLSI Test Symposium (VTS)*, pages 1–10, San Diego, CA, USA, Apr. 2020. IEEE.

[68] L. Beckwith, A. Abdulgadir, and R. Azarderakhsh. A Flexible Shared Hardware Accelerator for NIST-Recommended Algorithms CRYSTALS-Kyber and CRYSTALS-Dilithium with SCA Protection. In M. Rosulek, editor, *Topics in Cryptology – CT-RSA 2023*, volume 13871, pages 469–490. Springer International Publishing, Cham, 2023. Series Title: Lecture Notes in Computer Science.

[69] D. Soni, K. Basu, M. Nabeel, and R. Karri. A hardware evaluation study of nist post-quantum cryptographic signature schemes. In *Second PQC Standardization Conference*. NIST, 2019.

[70] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. Technical Report RFC5246, RFC Editor, Aug. 2008.

[71] U. Banerjee, C. Juvekar, S. H. Fuller, and A. P. Chandrakasan. eeDTLS: Energy-Efficient Datagram Transport Layer Security for the Internet of Things. In *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, pages 1–6, Singapore, Dec. 2017. IEEE.

[72] A. Haroon, S. Akram, M. A. Shah, and A. Wahid. E-Lithe: A Lightweight Secure DTLS for IoT. In *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, pages 1–5, Toronto, ON, Sept. 2017. IEEE.

[73] E. Rescorla, R. Barnes, H. Tschofenig, and B. M. Schwartz. Compact TLS 1.3. Internet-draft draft-ietf-tls-ctls-06, Internet Engineering Task Force / Internet Engineering Task Force, July 2022. tex.pagetotal: 24.

[74] S. Sahoo, S. S. Sahoo, P. Maiti, B. Sahoo, and A. K. Turuk. A Lightweight Authentication Scheme for Cloud-Centric IoT Applications. In *2019 6th International Conference on Signal Processing and Integrated Networks (SPIN)*, pages 1024–1029, Noida, India, Mar. 2019. IEEE.

[75] P. Kanuch and D. Macko. Optimizing Energy Efficiency of Secured IoT Communication by OpenHip. In *2019 42nd International Conference on Telecommunications and Signal Processing (TSP)*, pages 174–177, Budapest, Hungary, July 2019. IEEE.

[76] G. Glissa and A. Meddeb. 6LowPSec: An end-to-end security protocol for 6LoWPAN. *Ad Hoc Networks*, 82:100–112, Jan. 2019.

[77] M. Vucinic, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti. OSCAR: Object security architecture for the Internet of Things. In *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014*, pages 1–10, Sydney, Australia, June 2014. IEEE.

[78] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt. Lithe: Lightweight Secure CoAP for the Internet of Things. *IEEE Sensors Journal*, 13(10):3711–3720, Oct. 2013.

[79] AWS IoT Developer Guide. Infrastructure security in AWS IoT, 2022.

[80] Cloud IoT Core. Requirements - Cloud IoT Core, 2022.

[81] S. Ziegler, C. Crettaz, L. Ladid, S. Krco, B. Pokric, A. F. Skarmeta, A. Jara, W. Kastner, and M. Jung. IoT6 – Moving to an IPv6-Based Future IoT. In A. Galis and A. Gavras, editors, *The Future Internet*, volume 7858, pages 161–172. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013. Series Title: Lecture Notes in Computer Science.

[82] S. Ziegler, A. Skarmeta, P. Kirstein, and L. Ladid. Evaluation and recommendations on IPv6 for the Internet of Things. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, pages 548–552, Milan, Italy, Dec. 2015. IEEE.

[83] J. Granjal, E. Monteiro, and J. S. Silva. Security in the integration of low-power Wireless Sensor Networks with the Internet: A survey. *Ad Hoc Networks*, 24:264–287, Jan. 2015.

[84] J. Nieminen, T. Savolainen, B. Patil, M. Isomäki, Z. Shelby, and C. Gomez. RFC 7668: IPv6 over BLUETOOTH(R) Low Energy. *IETF RFC*, Oct. 2015.

[85] K. Shahzad and B. Oelmann. A comparative study of in-sensor processing vs. raw data transmission using ZigBee, BLE and Wi-Fi for data intensive monitoring applications. In *2014 11th International Symposium on Wireless Communications Systems (ISWCS)*, pages 519–524, Barcelona, Spain, Aug. 2014. IEEE.

[86] P. Trelsmo, P. Di Marco, P. Skillermark, R. Chirikov, and J. Ostman. Evaluating IPv6 Connectivity for IEEE 802.15.4 and Bluetooth Low Energy. In *2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, pages 1–6, San Francisco, CA, USA, Mar. 2017. IEEE.

[87] J. Campos, S. Colteryahn, and K. Gagneja. IPv6 transmission over BLE Using Raspberry PI 3. In *2018 International Conference on Computing, Networking and Communications (ICNC)*, pages 200–204, Maui, HI, Mar. 2018. IEEE.

[88] C.-M. Kim, H.-W. Kang, S.-I. Choi, and S.-J. Koh. Implementation of CoAP/6LoWPAN over BLE Networks for IoT Services. *Journal of Broadcast Engineering*, 21(3):298–306, 2016.

[89] F. L. Coman, K. M. Malarski, M. N. Petersen, and S. Ruepp. Security Issues in Internet of Things: Vulnerability Analysis of LoRaWAN, Sigfox and NB-IoT. In *2019 Global IoT Summit (GIoTS)*, pages 1–6, Aarhus, Denmark, June 2019. IEEE.

[90] K. O. Adefemi Alimi, K. Ouahada, A. M. Abu-Mahfouz, and S. Rimer. A Survey on the Security of Low Power Wide Area Networks: Threats, Challenges, and Potential Solutions. *Sensors*, 20(20):5800, Oct. 2020.

[91] K.-L. Tsai, Y.-L. Huang, F.-Y. Leu, I. You, Y.-L. Huang, and C.-H. Tsai. AES-128 Based Secure Low Power Communication for LoRaWAN IoT Environments. *IEEE Access*, 6:45325–45334, 2018.

[92] M. Seliem and K. Elgazzar. IoTeWay: A Secure Framework Architecture for 6LoWPAN Based IoT Applications. In *2018 IEEE Global Conference on Internet of Things (GCIoT)*, pages 1–5, Alexandria, Egypt, Dec. 2018. IEEE.

[93] P.-Y. Ting, J.-L. Tsai, and T.-S. Wu. Signcryption Method Suitable for Low-Power IoT Devices in a Wireless Sensor Network. *IEEE Systems Journal*, 12(3):2385–2394, Sept. 2018.

[94] S. Pirbhulal, H. Zhang, M. E Alahi, H. Ghayvat, S. Mukhopadhyay, Y.-T. Zhang, and W. Wu. A Novel Secure IoT-Based Smart Home Automation System Using a Wireless Sensor Network. *Sensors*, 17(12):69, Dec. 2016.

[95] G. Restuccia, H. Tschofenig, and E. Baccelli. Low-Power IoT Communication Security: On the Performance of DTLS and TLS 1.3. In *2020 9th IFIP International Conference on Performance Evaluation and Modeling in Wireless Networks (PEMWN)*, pages 1–6, Berlin, Germany, Dec. 2020. IEEE.

[96] Y.-k. Lee, Y. kim, and J.-n. kim. Implementation of TLS and DTLS on Zephyr OS for IoT Devices. In *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, pages 1292–1294, Jeju, Oct. 2018. IEEE.

[97] A. H. Gerez, K. Kamaraj, R. Nofal, Y. Liu, and B. Dezfouli. Energy and Processing Demand Analysis of TLS Protocol in Internet of Things Applications. In *2018 IEEE International Workshop on Signal Processing Systems (SiPS)*, pages 312–317, Cape Town, Oct. 2018. IEEE.

[98] T. Prantl, L. Iffländer, S. Herrnleben, S. Engel, S. Kounev, and C. Krupitzer. Performance Impact Analysis of Securing MQTT Using TLS. In *Proceedings of the ACM/SPEC International Conference on Performance Engineering*, pages 241–248, Virtual Event France, Apr. 2021. ACM.

[99] G. Restuccia, H. Tschofenig, and E. Baccelli. Low-Power IoT Communication Security: On the Performance of DTLS and TLS 1.3. In *2020 9th IFIP International Conference on Performance Evaluation and Modeling in Wireless Networks (PEMWN)*, pages 1–6, Berlin, Germany, Dec. 2020. IEEE.

[100] C. Lachner and S. Dustdar. A Performance Evaluation of Data Protection Mechanisms for Resource Constrained IoT Devices. In *2019 IEEE International Conference on Fog Computing (ICFC)*, pages 47–52, Prague, Czech Republic, June 2019. IEEE.

[101] P. S. Munoz, N. Tran, B. Craig, B. Dezfouli, and Y. Liu. Analyzing the Resource Utilization of AES Encryption on IoT Devices. In *2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, pages 1200–1207, Honolulu, HI, USA, Nov. 2018. IEEE.

[102] T. Schläpfer and A. Rüst. Security on IoT devices with secure elements. *Embedded World Conference 2019 - Proceedings*, 2019. Medium: application/pdf Publisher: WEKA.

[103] R. A. Nofal, N. Tran, C. Garcia, Y. Liu, and B. Dezfouli. A Comprehensive Empirical Analysis of TLS Handshake and Record Layer on IoT Platforms. In *Proceedings of the 22nd International ACM Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems - MSWIM '19*, pages 61–70, Miami Beach, FL, USA, 2019. ACM Press.

[104] B. Pearson, L. Luo, Y. Zhang, R. Dey, Z. Ling, M. Bassiouni, and X. Fu. On Misconception of Hardware and Cost in IoT Security and Privacy. In *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, pages 1–7, Shanghai, China, May 2019. IEEE.

[105] T. Schläpfer and A. Rüst. Using secure microcontrollers in IoT applications. *Wireless Congress, Munich, 22 - 23 October 2019*, 2019. Medium: application/pdf Publisher: WEKA.

[106] ARM Developer. IP | TrustZone CryptoCell, 2020.

[107] D. Enescu. Thermoelectric Energy Harvesting: Basic Principles and Applications. In D. Enescu, editor, *Green Energy Advances*. IntechOpen, Feb. 2019.

[108] M. Haras, V. Lacatena, F. Morini, J.-F. Robillard, S. Monfray, T. Skotnicki, and E. Dubois. Thermoelectric energy conversion: How good can silicon be? *Materials Letters*, 157:193–196, Oct. 2015.

[109] A. J. Minnich, M. S. Dresselhaus, Z. F. Ren, and G. Chen. Bulk nanostructured thermoelectric materials: current research and future prospects. *Energy & Environmental Science*, 2(5):466, 2009.

[110] G. J. Snyder and E. S. Toberer. Complex thermoelectric materials. *Nature Materials*, 7(2):105–114, Feb. 2008.

[111] J.-M. Gruber and S. Mathis. P3.6 - Efficient Boost Converter for Thermoelectric Energy Harvesting. In *Proceedings Sensor 2017*, pages 642–645, Nürnberg, Germany, 2017. AMA Service GmbH, Von-Münchhausen-Str. 49, 31515 Wunstorf, Germany.

[112] Y. K. Ramadass and A. P. Chandrakasan. A batteryless thermoelectric energy-harvesting interface circuit with 35mV startup voltage. In *2010 IEEE International Solid-State Circuits Conference - (ISSCC)*, pages 486–487, San Francisco, CA, USA, Feb. 2010. IEEE.

[113] V.-K. Pham. A High-Efficient Power Converter for Thermoelectric Energy Harvesting. In *2020 5th International Conference on Green Technology and Sustainable Development (GTSD)*, pages 82–87, Ho Chi Minh City, Vietnam, Nov. 2020. IEEE.

[114] Matrix - prometheus. tex.key: Matrix.

[115] M. Magno and D. Boyle. Wearable Energy Harvesting: From body to battery. In *2017 12th International Conference on Design & Technology of Integrated Systems In Nanoscale Era (DTIS)*, pages 1–6, Palma de Mallorca, Spain, Apr. 2017. IEEE.

[116] M. Magno, X. Wang, M. Eggimann, L. Cavigelli, and L. Benini. InfiniWolf: Energy Efficient Smart Bracelet for Edge Computing with Dual Source Energy Harvesting. In *2020 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 342–345, Grenoble, France, Mar. 2020. IEEE.

[117] Q. Wan, Y.-K. Teh, Y. Gao, and P. K. T. Mok. Analysis and Design of a Thermoelectric Energy Harvesting System With Reconfigurable Array of Thermoelectric Generators for IoT Applications. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 64(9):2346–2358, Sept. 2017.

[118] T. T. Kim Tuoi, N. Van Toan, and T. Ono. Heat Storage Thermoelectric Generator for Wireless IOT Sensing Systems. In *2021 21st International Conference on Solid-State Sensors, Actuators and Microsystems (Transducers)*, pages 924–927, Orlando, FL, USA, June 2021. IEEE.

[119] W. Wang, X. Chen, Y. Liu, X. Wang, and Z. Liu. Thermo-electric Energy Harvesting Powered IoT System Design and Energy Model Analysis. In *2019 IEEE 13th International Conference on Anti-counterfeiting, Security, and Identification (ASID)*, pages 303–308, Xiamen, China, Oct. 2019. IEEE.

[120] H. Elahi, K. Munir, M. Eugeni, S. Atek, and P. Gaudenzi. Energy Harvesting towards Self-Powered IoT Devices. *Energies*, 13(21):5528, Oct. 2020.

[121] F. Yuan, Q. T. Zhang, S. Jin, and H. Zhu. Optimal Harvest-Use-Store Strategy for Energy Harvesting Wireless Systems. *IEEE Transactions on Wireless Communications*, 14(2):698–710, Feb. 2015.

[122] RIOT operating system. tex.key: RIOT.

[123] Avanzi, Roberto and Bos, Joppe and Ducas, et al. CRYSTALS-KYBER: Algorithm specifications and supporting documentation.

[124] Bai, S. and Ducas, L. and Kiltz, E. and Leopoint, T., and Lyubashevsky, V. and Schwabe, P. and Seiler, G. and Stehlé, D. CRYSTALS-Dilithium – algorithm specifications and supporting documentation (version 3.1).

[125] M. Pedaste, M. Mäeots, L. A. Siiman, T. De Jong, S. A. Van Riesen, E. T. Kamp, C. C. Manoli, Z. C. Zacharia, and E. Tsourlidaki. Phases of inquiry-based learning: Definitions and the inquiry cycle. *Educational Research Review*, 14:47–61, Feb. 2015.

[126] A. Hofstein and V. N. Lunetta. The laboratory in science education: Foundations for the twenty-first century. *Science Education*, 88(1):28–54, Jan. 2004.

[127] N. G. Holmes, J. Ives, and D. A. Bonn. The Impact of Targeting Scientific Reasoning on Student Attitudes about Experimental Physics. In *2014 Physics Education Research Conference Proceedings*, pages 119–122, Minneapolis, MS, Apr. 2015. American Association of Physics Teachers.

[128] S. J. Husnaini and S. Chen. Effects of guided inquiry virtual and physical laboratories on conceptual understanding, inquiry performance, scientific inquiry self-efficacy, and enjoyment. *Physical Review Physics Education Research*, 15(1):010119, Mar. 2019.

[129] H. O. Kapici, H. Akcay, and T. De Jong. Using Hands-On and Virtual Laboratories Alone or Together—Which Works Better for Acquiring Knowledge and Skills? *Journal of Science Education and Technology*, 28(3):231–250, June 2019.

[130] B. R. Wilcox and H. Lewandowski. Developing skills versus reinforcing concepts in physics labs: Insight from a survey of students' beliefs about experimental physics. *Physical Review Physics Education Research*, 13(1):010108, Feb. 2017.

[131] T. De Jong. Moving towards engaged learning in STEM domains; there is no simple answer, but clearly a road ahead. *Journal of Computer Assisted Learning*, 35(2):153–167, Apr. 2019.

[132] A. W. Lazonder and R. Harmsen. Meta-Analysis of Inquiry-Based Learning: Effects of Guidance. *Review of Educational Research*, 86(3):681–718, Sept. 2016.

[133] S. Kapp. *Experimentorientierte augmented-reality-lernumgebungen in der physikdidaktik*. phd, Technische Universität Kaiserslautern, 2022.

[134] J. Sweller. Cognitive Load During Problem Solving: Effects on Learning. *Cognitive Science*, 12(2):257–285, Apr. 1988.

[135] J. Sweller, P. Ayres, and S. Kalyuga. *Cognitive Load Theory*. Springer New York, New York, NY, 2011.

[136] P. Ayres. Impact of reducing intrinsic cognitive load on learning in a mathematical domain. *Applied Cognitive Psychology*, 20(3):287–298, Apr. 2006.

[137] J. Sweller and P. Chandler. Why Some Material Is Difficult to Learn. *Cognition and Instruction*, 12(3):185–233, Sept. 1994.

[138] M. Florax and R. Ploetzner. What contributes to the split-attention effect? The role of text segmentation, picture labelling, and spatial proximity. *Learning and Instruction*, 20(3):216–224, June 2010.

[139] N. L. Schroeder and A. T. Cenkci. Spatial Contiguity and Spatial Split-Attention Effects in Multimedia Learning Environments: a Meta-Analysis. *Educational Psychology Review*, 30(3):679–701, Sept. 2018.

[140] M. Thees, S. Kapp, K. Altmeyer, S. Malone, R. Brünken, and J. Kuhn. Comparing Two Subjective Rating Scales Assessing Cognitive Load During Technology-Enhanced STEM Laboratory Courses. *Frontiers in Education*, 6:705551, July 2021.

[141] K. R. Butcher. The Multimedia Principle. In R. E. Mayer, editor, *The Cambridge Handbook of Multimedia Learning*, pages 174–205. Cambridge University Press, 2 edition, July 2014.

[142] R. E. Mayer. *Multimedia Learning*. Cambridge University Press, 2 edition, Jan. 2009.

[143] R. E. Mayer and L. Fiorella. Principles for Reducing Extraneous Processing in Multimedia Learning: Coherence, Signaling, Redundancy, Spatial Contiguity, and Temporal Contiguity Principles. In R. E. Mayer, editor, *The Cambridge Handbook of Multimedia Learning*, pages 279–315. Cambridge University Press, 2 edition, July 2014.

[144] F. Yeboah, H. Guo, and A. Bill. A High-throughput Calcium-flux Assay to Study NMDA-receptors with Sensitivity to Glycine/D-serine and Glutamate. *Journal of Visualized Experiments: JoVE*, (137):58160, July 2018.

[145] C.-Y. Tsui and D. F. Treagust. Introduction to Multiple Representations: Their Importance in Biology and Biological Education. In D. F. Treagust and C.-Y. Tsui, editors, *Multiple Representations in Biological Education*, volume 7, pages 3–18. Springer Netherlands, Dordrecht, 2013. Series Title: Models and Modeling in Science Education.

[146] D. F. Treagust, R. Duit, and H. E. Fischer, editors. *Multiple Representations in Physics Education*, volume 10 of *Models and Modeling in Science Education*. Springer International Publishing, Cham, 2017.

[147] S. Ainsworth. The functions of multiple representations. *Computers & Education*, 33(2-3):131–152, Sept. 1999.

[148] S. Ainsworth. DeFT: A conceptual framework for considering learning with multiple representations. *Learning and Instruction*, 16(3):183–198, June 2006.

[149] M. Thees, S. Kapp, M. P. Strzys, F. Beil, P. Lukowicz, and J. Kuhn. Effects of augmented reality on learning and cognitive load in university physics laboratory courses. *Computers in Human Behavior*, 108:106316, July 2020.

[150] D. Sonntag, G. Albuquerque, M. Magnor, and O. Bodensiek. Hybrid learning environments by data-driven augmented reality. *Procedia Manufacturing*, 31:32–37, 2019.

[151] G. Albuquerque, D. Sonntag, O. Bodensiek, M. Behlen, N. Wendorff, and M. Magnor. A Framework for Data-Driven Augmented Reality. In L. T. De Paolis and P. Bourdot, editors, *Augmented Reality, Virtual Reality, and Computer Graphics*, volume 11614, pages 71–83. Springer International Publishing, Cham, 2019. Series Title: Lecture Notes in Computer Science.

[152] O. Amiraslanov, H. Javaheri, S. Bian, and P. Lukowicz. Preparation for Future Learning: Augmented-Reality Enhanced Interactive Science Labs. In *Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers*, pages 331–334, Singapore Singapore, Oct. 2018. ACM.

[153] S. Kapp. *Experimentorientierte augmented-reality-lernumgebungen in der physikdidaktik*. Technische Universität Kaiserslautern, 2022.

[154] S. Staacks, S. Hütz, H. Heinke, and C. Stampfer. Advanced tools for smartphone-based experiments: phyphox. *Physics Education*, 53(4):045009, July 2018.

[155] E. Kutlu, H. Bakirci, and Y. Kara. STEM Education Effect on Inquiry Perception and Engineering Knowledge. *Participatory Educational Research*, 9(3):248–262, May 2022.

[156] S. Kapp, M. Thees, M. P. Strzys, F. Beil, J. Kuhn, O. Amiraslanov, H. Javaheri, P. Lukowicz, F. Lauer, C. Rheinländer, and N. Wehn. Augmenting Kirchhoff's laws: Using augmented reality and smartglasses to enhance conceptual electrical experiments for high school students. *The Physics Teacher*, 57(1):52–53, Jan. 2019.

List of Figures

List of Tables

Lebenslauf

Persönliche Daten

Name: Frederik Lauer

Ausbildung

Technisches Gymnasium Kaiserslautern 2008–2011

Hochschulstudium: Bachelor Studium: Elektro- und Informationstechnik
Vertiefungsrichtung: Eingebettete Systeme
Technische Universität Kaiserslautern
10/2011–09/2016

Master Studium: Elektro- und Informationstechnik
Vertiefungsrichtung: Eingebettete Systeme
Technische Universität Kaiserslautern
04/2016–06/2018

Beruflicher Werdegang

07/2018–01/2023 Wissenschaftlicher Mitarbeiter
Arbeitsgruppe Entwurf Mikroelektronischer Systeme
Fachbereich Elektrotechnik und Informationstechnik
Rheinland-Pfälzische Technische Universität Kaiserslautern-Landau