Contribution to IO-Link Wireless Safety – Architecture and System Extensions

Von der Fakultät für Elektrotechnik
der Helmut-Schmidt-Universität / Universität der Bundeswehr Hamburg
zur Erlangung des akademischen Grades eines Doktor-Ingenieurs
genehmigte

DISSERTATION
vorgelegt von

Thomas Robert Doebbert

aus Neubrandenburg, Deutschland

Hamburg 2023

Gutachter:	Univ.-Prof. Dr.-Ing. Gerd Scholl Helmut-Schmidt-Universität, Hamburg, Germany
	Univ.-Prof. Dr.-Ing. Frank Schiller Beckhoff Automation, East China University of Science and Technology, Shanghai, China
Vorsitzender:	Univ.Prof. Dr.-Ing. habil. Udo Zölzer Helmut-Schmidt-Universität, Hamburg, Germany
Tag der Disputation:	11.12.2023

Acknowledgments

The accomplishments that resulted in this dissertation could not have been achieved without several persons' assistance, support, and encouragement.

First of all, I would like to thank my doctoral adviser, Professor `Gerd Scholl`, for the opportunity to research and work at his institute. I am deeply grateful for his encouragement and his trust he placed in me and my work. The intellectual freedom he has offered throughout the years in combination with guidance and his invaluable advice were of great importance to complete this dissertation.

My sincere thanks go to the members of the evaluation board: Professor `Udo Zölzer`, Helmut Schmidt University, and Professor `Frank Schiller`, Beckhoff Automation GmbH & Co. KG and East China University of Science and Technology. Professor Schiller had a great influence with his knowledge and achievements in the field of functional safety resulting in profound discussions.

During my work as a research assistant for the Department of Electrical Measurement Engineering at the Helmut-Schmidt-University, I had the privilege to be part of a great team. I am very thankful for the rich and important discussions about research and other important topics with all my colleagues. My thanks go in particular to `Christoph Cammin` and `Henry Beuster` especially for proofreading and finding bugs in my manuscripts and code.

Within the dtec.bw project Digital Sensor-2-Cloud Campus Platform (DS2CCP), I have been in exchange with several companies Kunbus GmbH, Pilz GmbH, TÜV SÜD Rail GmbH, and Rohde & Schwarz GmbH & Co. KG. I would like to thank all partners for supporting the project and influencing the positive outcome. Especially, I am grateful for the rich exchange and numerous discussions with `Dymtro Krush, Dirk Krüger,` and **Housam Wattar** from Kunbus GmbH, **Reinhard Sperrer** from Pilz GmbH, and **Peerasan Supavatanakul** from TÜV SÜD Rail GmbH.

My sincere thanks also go to my close friends and family for their support and encouragement.

Finally, and not the least, I like to give the warmest gratitude to my wife Kristina and my daughter Feliza for their unconditional encouragement, patience, and support during these years.

Hamburg, December 2023 Thomas Doebbert

Abstract

Functional safety systems protect humans and equipment from hazards while machines or humans perform automation processes. Therefore, the systematic and safe design of functional safety protocols and systems together with appropriate safety management and maintenance concepts is critical and must follow quality standards.

In the field of production automation, IO-Link Wireless (IOLW) offers energy-efficient and cost-effective solutions for wireless sensors/actuator communication close to the machines on the industrial shop-floor. In case of safety applications within IO-Link (IOL), currently only a wired extension of a functional safety protocol, called IO-Link Safety (IOLS), exists. Thus, the applied safety features in IOLS are not sufficient for a safety extension of IOLW. Therefore, a safety concept proposal to enhance IOLW with safety features is suggested. This proposal is realized for safety critical communication in industrial environments with performance characteristics of demanding safety integrity level (SIL) 3 requirements.

As also data security is of paramount importance, security-for-safety mechanisms are adopted for IOLW Safety, especially to meet the necessary criteria within the safety requirement specification (SRS) to ensure a one-to-one connection between an IOLW Master and an IOLW Device. Potential cryptographic algorithms are evaluated with respect to energy consumption and timing. Reliable and energy-efficient characteristics are crucial for a fast and secure wireless communication solution, especially for mobile safety applications. Therefore, the current consumption should not significantly increase due to implemented cryptographic algorithms. A current measurement method is designed to evaluate the current consumption for different crypto-algorithms together with an uncertainty estimation.

Furthermore, a SRS is elaborated together with an authorized certification organization with a profound focus on standards (mainly IEC 61508 and IEC 61784-3) regulating the probability of dangerous failure on demand (PFD) addressed within SRSs. Also, relevant security standards (e.g., IEC 62443) involving security-for-safety for IO-Link Wireless Safety (IOLWS) are considered. The PFD is determined using probabilistic models to verify the regulations stated in the standards. Taking performance parameters into account, which are crucial for industrial manufacturing processes, a safety process data unit (SPDU) is designed and certified by the authorized safety organization for different payload lengths and cycle times. This is necessary, because for various applications safety devices require different payload lengths. Therefore, measurements for different payload lengths to enable various safety devices are performed to analyze cycle and processing times of the communication channels and devices.

The protocol architecture, including a safety and security communication layer, is introduced including services to provide features to the application layer. A prototype implementation assures that the concept is applicable in real world with existing hardware to meet the stated requirements within the SRS. The measurements demonstrate feasibility of the concept and its assumptions.

Kurzfassung

Funktionale Sicherheitsprotokolle schützen Menschen und Geräte vor Gefahren, während diese in automatisierten Produktionsprozessen tätig sind. Daher ist das systematische und sichere Design von Kommunikationsprotokollen und Systemen der funktionalen Sicherheit in Kombination mit geeigneten Management- und Wartungskonzepten von entscheidender Bedeutung und muss Qualitätsstandards folgen.

Im Bereich der Fertigungsautomatisierung und industriellen Automatisierung ermöglicht IO-Link Wireless (IOLW) energieeffiziente und kostengünstige Lösungen zur maschinennahen Vernetzung drahtloser Sensoren und Aktoren. Für Sicherheitsanwendungen innerhalb von IO-Link (IOL) existiert momentan ausschließlich eine drahtgebundene Erweiterung eines funktionalen Sicherheitsprotokolls, genannt IO-Link Safety (IOLS). Da die in IOLS verwendeten Sicherheitsmaßnahmen für eine Safety-Erweiterung von IOLW zu einem funktionalen Sicherheitsprotokoll nach SIL 3 nicht genügen, werden weitere Sicherheitsmaßnahmen vorgeschlagen.

Da auch die Cyber-Sicherheit von großer Bedeutung ist, werden Sicherheitsmechanismen, die bereits in anderen drahtlosen Protokollen implementiert sind, untersucht und Security-for-Safety-Mechanismen für IOLW ausgearbeitet und empfohlen, insbesondere um die erforderlichen Kriterien relevanter Normen (IEC 61508, IEC 61784-3, IEC 62443) zu erfüllen. Potenzielle kryptografische Algorithmen werden für IOLW im Hinblick auf Energieverbrauch und Timing evaluiert, um zuverlässige und energieeffiziente Eigenschaften für eine schnelle, sichere und batteriebetriebene drahtlose Kommunikationslösung zu gewährleisten. Eine Voraussetzung hierfür ist, dass der Stromverbrauch durch zusätzliche kryptografische Operationen nicht signifikant ansteigt. Zur Bewertung des Stromverbrauchs wird ein prinzipielles Strommessverfahren entwickelt und eine Unsicherheitsab-

schätzung (guide to the expression of uncertainty in measurement (GUM)) anhand statistischer Messdaten unter Berücksichtigung der kombinierten Standardunsicherheit durchgeführt.

Zum Schutz vor inakzeptablen Risiken, die z.B. bei Automatisierungssystemen durch Ausfälle entstehen können, wurde gemeinsam mit einer autorisierten Zertifizierungsorganisation eine Sicherheitsanforderungsspezifikation (safety requirement specification (SRS)) für IOLW Safety erarbeitet. Bei diesem Ansatz wurde ein starker Fokus auf internationale Standards gelegt, die die durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls bei Bedarf (probability of dangerous failure on demand (PFD)) regeln, die in SRSs und relevanten Sicherheitsnormen unter Berücksichtigung der funktionalen Sicherheit und Security-for-Safety-Betrachtungen für IOLWS behandelt werden. Die Ausfallwahrscheinlichkeit (PFD) wird mithilfe probabilistischer Modelle ermittelt, um die in den Normen festgelegten Vorschriften zu überprüfen. Unter Berücksichtigung von Leistungs- und Sicherheitsparametern, die für industrielle Automatisierungsprozesse von entscheidender Bedeutung sind, wird eine Sicherheitsprotokolldateneinheit (safety process data unit (SPDU)) für unterschiedliche Datenlängen und Zykluszeiten entwickelt und von einer autorisierten Sicherheitsorganisation zertifiziert. Messungen für verschiedene Datenlängen von Protokollapplikationsdaten zur Nutzung unterschiedlicher Sicherheitsgeräte werden durchgeführt und analysiert, um Zyklus- und Verarbeitungszeiten der Kommunikationskanäle und -geräte darzustellen.

Eine Protokollarchitektur mit einer Kommunikationsschicht für funktionale und cyber-Sicherheit wird eingeführt, die Dienste zur Bereitstellung von Funktionen für die Anwendungsschicht enthält. Dabei stellt eine Prototyp-Implementierung sicher, dass das Konzept in der realen Welt mit vorhandener Hardware anwendbar ist, um die Anforderungen an funktionaler und cyber-Sicherheit zu erfüllen. Die durchgeführten Messungen zeigen auch die Umsetzbarkeit des Konzepts und ggfs. entsprechende Akzeptanz.

Contents

Glossary

In this glossary, the abbreviations used in this work are introduced. The elements are arranged in alphabetical order. Mathematical operators, functions, and symbols are described directly when used.

Abbreviations

A-code authentication-code

AI artificial intelligence

AGV automated guided vehicle

API application programming interface

BSC binary symmetric channel

BEP bit error probability

BLE Bluetooth Low Energy

CIA confidentiality, integrity, authenticity/availability

CPKE certificate-based pairwise key establishment

CPF communication profile families

CPS cyber-physical system

CRC cyclic redundancy check

CPU central processing unit

CT ciphertext

DH Diffie-Hellman

DL downlink

DOS denial-of-service

DSLOT double slot

DUT device under test

ECC elliptic curve cryptography

ECDH elliptic-curve Diffie-Hellman

ECMQV elliptic-curve Menezes-Qu-Vanstone

eMBB enhanced mobile broadband

EMT Electrical Measurement Engineering

EUC equipment under control

FAT factory acceptance test

FDS functional design specification

FFT fast Fourier transformation

FMEA failure mode and effects analysis

FSM functional safety management

FSSM functional safety state machines

FSoE Safety over EtherCAT

FSCP Functional Safety Communication Profile

FS-Device functional safety device

FS-Master functional safety master

FS-Bridge functional safety bridge

FSP functional safety protocol (parameter)

FS functional safety

FS-W functional safety wireless

FST functional safety technology (parameter)

FS-PDin functional safety process data input

FS-PDout functional safety process data output

FS-W-Device IOLW safety device

FS-W-Bridge IOLW safety bridge

FS-W-Master IOLW safety master

FS-W-PDin functional safety wireless process data input

FS-W-PDout functional safety wireless process data output

FS-Gateway fail-safe gateway

F/TDMA frequency- and time-division multiple access

GFSK Gaussian frequency-shift keying

GUM guide to the expression of uncertainty in measurement

HSM hardware security module

HSU Helmut-Schmidt-University

IEC International Electrotechnical Commission

ICS industrial control system

ICT information and communications technology

IIoT Industrial Internet of Things

IO input/output

IODD input/output device description

IOL IO-Link

IOLS IO-Link Safety

IOLW IO-Link Wireless

IOLWD IO-Link Wireless Device

IOLWM IO-Link Wireless Master

IOLWS IO-Link Wireless Safety

IP internet protocol

IPsec internet protocol security

ISM industry, scientific, and medical

IT information technology

LTE long-term evolution

mMTC massive machine type communication

mS2CAT modular sensor-2-cloud automation topology

MAC message authentication code

MIC message integrity check

MITM man-in-the-middle

NFC near-field communication

nonce number used once

OD on-request data

OI organization interval

OOB out-of-band

OPC UA open platform communications unified architecture

OT operational technology

PDE process data exchange

PD process data

PDCT port and device configuration tool

PDU process data unit

PFD probability of dangerous failure on demand

PFH probability of a dangerous failure per hour

PL performance level

PhyL physical layer

PLC programmable logic controller

PSA platform security architecture

PT plaintext

REP residual error probability

RFID radio frequency identification

RER residual error rate

RSA Rivest-–Shamir-–Adleman

RSSI received signal strength indicator

SCADA supervisory control and data acquisition

SCL safety communication layer

SDCI single-drop digital communication interface

SDCI-FS single-drop digital communication interface for functional safety

SeCL security communication layer

SFRT safety function response time

SIL safety integrity level

SMI standardized master interface

SPDE safe process data exchange

SPDU safety process data unit

SPI service provider interface

SRS safety requirement specification

SSH secure shell protocol

SSLOT single slot

T-code timeliness-code

TI Texas Instruments

TLS transport layer security

TrackSlotNr track and slot number

TSC time sensitive communication

TSN time sensitive networking

uRLLC ultra-reliable low-latency communication

UDS uniformly distributed segments

UL uplink

UML unified modeling language

VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.

V&V validation and verification

W-Device Wireless Device

W-Master Wireless Master

W-PDin non-safety wireless process data input

W-PDout non-safety wireless process data output

CHAPTER 1

Introduction

1.1. Personal Motivation

The scientific interest of designing and developing a functional safety protocol applied for a wireless technology incorporating also security-for-safety mechanisms within the calculations of the residual error probability considerations is complex and from a scientific point of view highly interesting.
The development of complex laser system was essential part of my first steps within industry, which sometimes required on-site support of systems being disposed all over the world. Because this implied long traveling times associated with non-negligible costs, remote access of these systems was considered or even favored. Unfortunately, the lasers had an output power of up to 8 kW, which could cause serious injuries or even kill operators. For the pure remote access, secure connections were necessary and for the safe operation, a failure mode and effects analysis (FMEA) consisting of a safety requirements specification were absolute indispensable. Therefore, already after university, functional safety and (cyber-)security were part of my first practical experience and directly caught my intention and interest.
Research in the field of a wireless communication protocol being developed from scratch at the university and eventually becoming a product in industry is fascinating. Moreover, being involved in the scientific exchange e.g., within research articles and scientific conferences, in combination with the scientific freedom of research itself, creates new ideas and impulses. The focus to eagerly research within this great field of study is almost self-created with new knowledge being beforehand blurred or even unknown.

1.2. Theoretical Background

Within this Section, a short introduction to the involved technologies and necessary theory including related standards is given.

1.2.1. IO-Link

IOL is an open interface standard, which is internationally standardized in IEC 61131-9 [1] describing how actuators and sensors are universally connected to a fieldbus system. Fig. 1.1 illustrates an example of a combined system architecture based on IOL and IO-Link Wireless (IOLW) with its fieldbus-neutral communication.

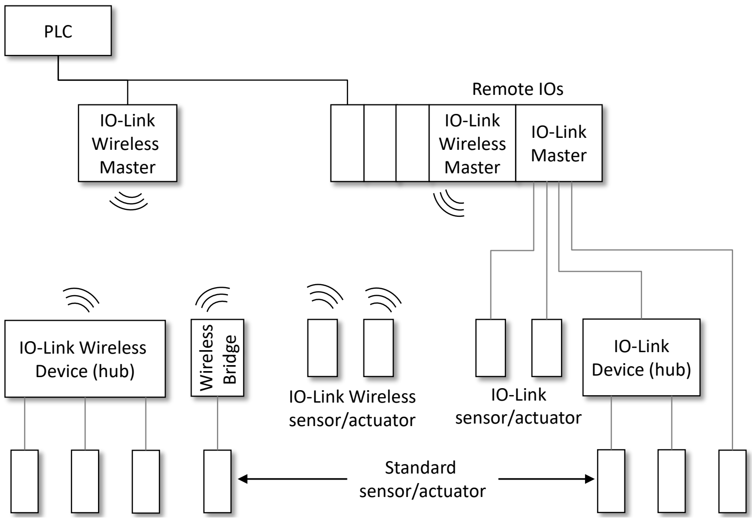


Figure 1.1.: Combined system architecture based on IO-Link and IO-Link Wireless based on [1].

The IOL system typically consists of an IOL master providing one or more master ports, each being connected to one or more IOL devices e.g., sensors, RFID readers, valves, motor starters, I/O modules, unshielded three or five conductor cables, and an engineering tool to configure and assign IOL parameters [2]. For the communication, four basic data types are defined, such as:

- Process data (cyclic) with up to 32 bytes being exchanged within every communication cycle.

- Value status data (cyclic) describing the validity of the process data.
- Device data (acyclic) such as parameters, identification data, and diagnostic information.
- Events (acyclic) such as error messages and warnings or maintenance data.

In [1], three transmission rates (baud rates) are defined:

- COM 1 = 4.8 kbaud,
- COM 2 = 38.4 kbaud, and
- COM 3 = 230.4 kbaud,

whereas only one of the defined data transmission rates is supported per IOL device. The cycle time depends on the frame length and the delay times in the IOL master and device. For instance at a baud rate of COM 2 and a frame length of 2 octets, the cycle time is typically 2 ms [2].

An electronic device description file, called input/output device description (IODD), is used for each device to store information, such as the supported baud rate, device ID, manufacturer ID, device specific data and parameters as well as a description of the process data provided by the sensor or actuator. An IOL configuration tool is required to parameterize the entire IOL system. Its task is the assignment of the devices to the ports of the IOL master, address assignment, and parameter assignment [2].

1.2.2. IO-Link Wireless[1]

Key aspects of IOLW with focus on wireless capabilities, its uniqueness in comparison to other wireless communications protocols are presented in [4, Table 1] and [5, Table 3].

General surveys of IOLW are given in [4–8] with a focus on roaming in [9], antenna planning in [10], coexistence in [11–13], security enhancement in [14–16] or on IOLW testing in [17–21]. However, a short introduction to IOLW is given here for completeness.

IOLW [22] is an open-vendor communication solution for factory automation on the shop floor. This wireless communication standard has been developed as an extension of the proven IO-Link standard [1], also known as single-drop digital communication interface (SDCI) or IEC 61131-9 [23]. Therefore, IOLW is mainly intended for sensor/actuator communication below the fieldbus level of abstraction within the factory automation structure [1, 4, 23]. IOLW specification was released in v1.1 in early 2018. A revised version was published in June 2023 [22].

[1] based on [3]

IOLW offers bidirectional wireless communication for (cyclic) process data and (acyclic) on-request data between a Wireless Master (W-Master) and Wireless Device (W-Device) in a star-shaped topology [4, 22]. The physical layer (PL) is based on Bluetooth Low Energy (BLE) 4.2 and utilizes the 2.4 GHz industry, scientific, and medical (ISM) band with Gaussian frequency-shift keying (GFSK) modulation [4, 22]. A combined frequency- and time-division multiple access (F/TDMA) scheme is used with frequency hopping. Furthermore, a blocklisting allows single frequency channels to be omitted in order to improve the wireless coexistence behavior [4, 13]. Wireless bridges ("W-Brides") are also standardized to operate in a similar way to W-Devices but to offer a wired IO-Link port in order to retrofit legacy systems.

In a fully-equipped IOLW system, up to three W-Masters can operate in the same manufacturing cell. Each W-Master can provide one to five tracks, whereby each track supports up to eight slots. Single slot (SSLOT) and double slot (DSLOT) W-Devices are specified. SSLOT W-Devices offer two (one) octet(s) for payload and are intended for simple sensors or actuators like switches, whereas DSLOT W-Devices offer 15 (14) octets for payload and are thus suitable for smart sensor applications (the values in parenthesis exclude the obligatory control octet). SSLOT and DSLOT W-Devices can be combined within one track [22]. Overall, up to 120 (SSLOT) W-Devices are supported within e.g., a single manufacturing cell [4,22]. Additionally, roaming capabilities between different W-Masters are implemented [9, 22].

One key feature of IOLW compared to other wireless protocols is its deterministic media access, which is shown in Fig. 1.2. The communication is divided into cycles and sub-cycles. A cycle lasts typically 5 ms and contains three sub-cycles, each with a duration of 1.664 ms. Frequency hopping takes place between the sub-cycles, whereby the hopping distance is greater than the typical coherence bandwidth of radio channels in industrial environments in order to increase transmission robustness. In the organization interval (OI), a switch-over between transmit and receive mode exists, or vice versa. Communication is organized in five tracks, each consisting of a downlink (DL) followed by an OI and four uplink (UL) slots each (numbered evenly starting from zero) are shown, which corresponds to the maximum configuration level of a W-Master for pure DSLOTs.

In case of a communication error, the protocol stack repeats the message a configurable number of times (retries). IOLW promises a latency time of 5 ms with a remaining probability of below 10^{-9} that this latency cannot be realized [7,22]. However, IOLW is not suitable for safety and/or security applications, yet.

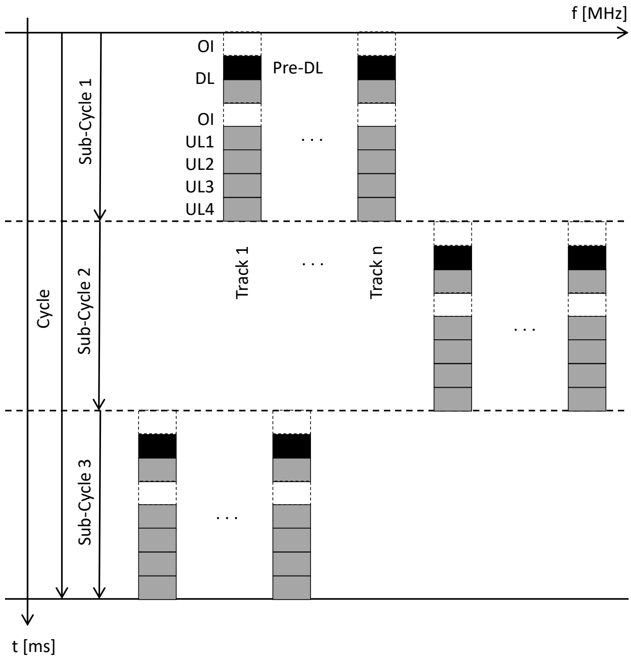


Figure 1.2.: Media access scheme of the IOLW protocol based on [4].

1.2.3. Functional Safety[2]

In general, “safety is defined as the freedom from unacceptable risk of physical injury [...]” [24]. Furthermore, safety is also defined as “absence of unacceptable risk of physical injury or damage to the health of people [...]” and risk in combination of the probability of harm occurring and the resulting consequence [25].

Functional safety (FS) has the task to “automatically reduce the level of risk in a device or system” [24]. And FS is therefore a type of product characteristic involving extensive analysis activities and their documentation during the development process to reduce risk to people.

More specific, according to the generic basic safety standard IEC 61508:2010 [25], FS is defined as follows:
FS designates the essential part of the overall safety of a system, which depends on the correct function of the safety-related electrical, electronic,

[2] based on [3]

programmable electronic safety-related system (E/E/PE, or E/E/PES) and other risk-reducing measures. Based on the international standard ISO 26262 [26] as an adaption of IEC 61508 in the automotive field for electrical, electronic, programmable electronic systems, FS is defined as the ability of these systems to turn to a well-defined safe state or to remain in a safe state in the event of systematic failures (e.g. faulty system design) and random hardware failures (e.g. communication breakdown, hardware failure, or effect of environment) with a dangerous effect. Note that IEC 61508 only describes electrical or electronic systems, whereas EN ISO 13849-1 [27] and IEC 62061 [28] additionally cover mechanic, pneumatic and hydraulic components.

Since FS is all about reducing the risk to people and equipment, it is important to distinguish between systematic and stochastic failures, which result to a hazardous failure. Systematic faults may occur during the development of safety equipment or software, which shall be avoided using adequate design principles and verification methods. Stochastic faults are only detectable during operation and are not avoidable. Fig. 1.3 represents a possible functional safety risk reduction framework.

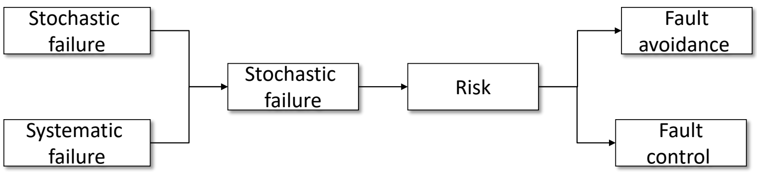


Figure 1.3.: Functional safety risk reduction framework based on [25].

Typically, safety protocols support a safety integrity level (SIL) from at least SIL 3 [25] or Category 4 and performance level (PL) e [27], but this is no requirement. Also, a safety function response time (SFRT) of about 10 ms or less shall be feasible. Additionally, a combination of a SPDU addressing different SIL levels and a non-safety process data unit (PDU) combined in one communication protocol shall be possible, whereas the safety transmission protocol shall be realized by only one additional safety layer and support the requirements of IEC 61784-3 [29]. In IEC 61784-3 all (mentioned) safety protocols rely on the black channel principle, which is also adopted in the considerations of this dissertation. A black channel is defined as a specified communication system consisting of one or more elements without proof of design or validation according to IEC 61784-3 [29]. In Chapter 5, adequate safety and security- for- safety measures to cope with typical communication failures [30] are listed. Communication reliability can be significantly increased by employing, e.g., a (sequence) counter and/or inverted counter, a watchdog timer and receipt messages indicating timeliness, connection validation at commissioning, startup and repair, and a cyclic redundancy check (CRC) for data integrity. For safety communication applications, CRCs are widely used as countermeasure against data consistency check failures, which is based on adding n redundancy bits to the m bit message to create a N bit codeword with $N = m + n$.

Current trends in the field of functional safety are e.g., interoperability of diversified encoding [31] and safe program execution with diversified encoding, which allows to build safety-critical systems from non-safety-critical hardware components due to its hardware-independence [32]. Furthermore, software coded processing is used to solve the problem of low integrity controllers for advanced reliability in detection of execution errors with high diagnostic coverage of processing units' failures [31]. Note that coded processing is a principle and hardware and software under which the concept is implemented still need test and validation.

1.2.4. Cyber-Security[3]

A number of definitions for the term security exist, but in general security may be defined as "the ability of an entity to protect resources for which it bears protection responsibility" [33]. Since the main focus of this thesis is on wireless communication using IOLW, only certain standards such as IEC 62443-3-3:2013 [34] series on industrial communication networks, networks and system security apply.

Security engineering requires cross-disciplinary expertise, ranging from cryptography and computer security through hardware tamper-resistance and formal methods to a knowledge of economics, applied psychology, organizations and law [35, pp. 3-16].

The three fundamental principles in information security are specified as confidentiality, integrity, and availability being commonly referred to as CIA triad, describing a model to form the main objectives of classical security properties [36, pp. 12-14]. Additionally to the three fundamental principles, authenticity must also be considered. With a strong focus on safety applications, this section is not intended to review all aspects concerning wireless security, instead a starting point for further research and implementation issues shall be given.

Principally, security threats can also be classified from a system access perspective, in which an attacker can pose three main types of threats [37]: remote network access by, e.g., an unsecured gateway, access in close prox-

[3] based on [3]

imity, or physical access to a critical electronic module. The features, indicated in Fig. 1.4, are vital to implement appropriate security functionalities: physical security, software and key provisioning security, run-time security, and foundation for security.

The details of each layer are described in [37]. A prerequisite for the security of wireless communication, especially for IOLW, is the use of up-to-date cryptographic algorithms for encryption, authentication, integrity and for key exchange. System security shall be tailored to the specific needs on the factory floor with a focus on implementing algorithms in a very resource efficient way. Therefore, cryptographic performance and timing for IOLW shall also be taken into consideration within this thesis.

Additional security measures such as device-unique joining authentication, device-unique re-entry authentication, pairwise privacy and integrity, network-wide privacy and integrity, secure over-the-air (OTA) updates, impersonation or replay attack prevention, and e.g., frequency agility (i.e., adaptive frequency hopping) have also been implemented as security options in wireless systems [37]. This is often considered using different security levels depending on the specific application.

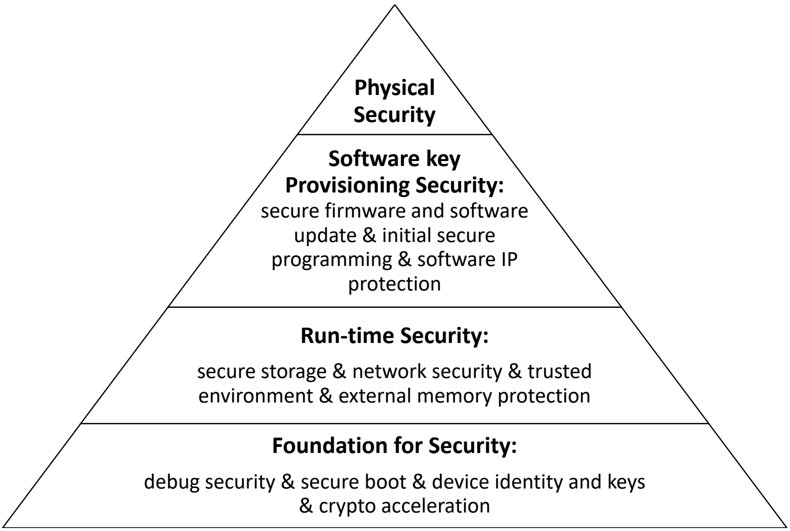


Figure 1.4.: Security enablers of an embedded processor with or without wireless interface based on [37].

1.2.5. Binary Symmetric Channel (BSC)

A common channel model used in communication is described as binary symmetric channel (BSC) being characterized as follows [38–40]:

- Each bit is erroneous independently of the other bits.
- Each bit is erroneous with the same bit error probability of BSC (p^{BSC}).
- The probability of the falsification from value 0 to value 1 and vice versa is identical.
- The probability p^{BSC} holds for $0 \leq p^{BSC} \leq 0.5$.

For the case of $p^{BSC} > 0.5$, a bitwise inverter may reduce the bit error probability (BEP) to $1 - p^{BSC}$ with the inverted value of a bit being more probable than the correct one. The communication would cause numerous errors making a reasonable communication unfeasible. Therefore, for safety application the maximum BEP is specified with 10^{-2} in [29].

With the assumptions made above, the probability for i erroneous bits of a bit string consisting of n bits can be calculated using the binomial distribution according to

$$P(n, i, p^{BSC}) = \binom{n}{i} \cdot (p^{BSC})^i \cdot (1 - p^{BSC})^{n-i}. \tag{1.1}$$

Thus, the sum of all undetectable error patterns is described in [40] as residual error probability (REP) with:

$$P_{rep}^{BSC}(p^{BSC}) = \sum_{i=d}^{n} \binom{n}{i} \cdot (p^{BSC})^i \cdot (1 - p^{BSC})^{n-i}, \tag{1.2}$$

where: p^{BSC} : bit error probability,
P_{rep}^{BSC} : sum of all undetectable error patterns.

Depending on the generator polynomial (CRC polynomial) [41] and message length, all error patterns with maximum $d - 1$ (Hamming distance) shall be detectable. The Hamming distance is the maximum possible number of bit errors on the received message to guarantee error detection using CRC decoding. An example for a proper generator polynomial for the given message length with its maximum REP being smaller than 2^{-r} [40,42] is presented in Fig. 1.5. With the same polynomial 0xF1922815, but a message length of n=1048 the REP with BSC model illustrates improperness in Fig. 1.6. The determination of the residual error probability is explain in more detail in Appendix B.

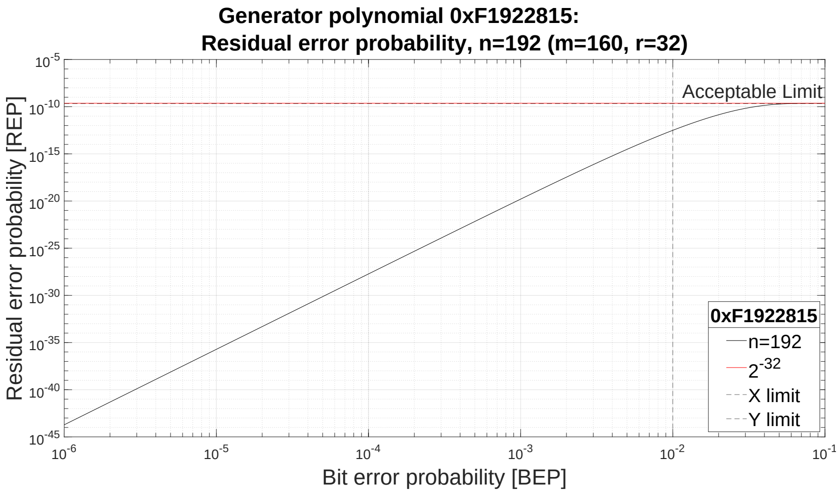


Figure 1.5.: Residual error probability of generator polynomial 0xF1922815 with BSC model (properness) for $P_{BSC}^{max} = 10^{-2}$

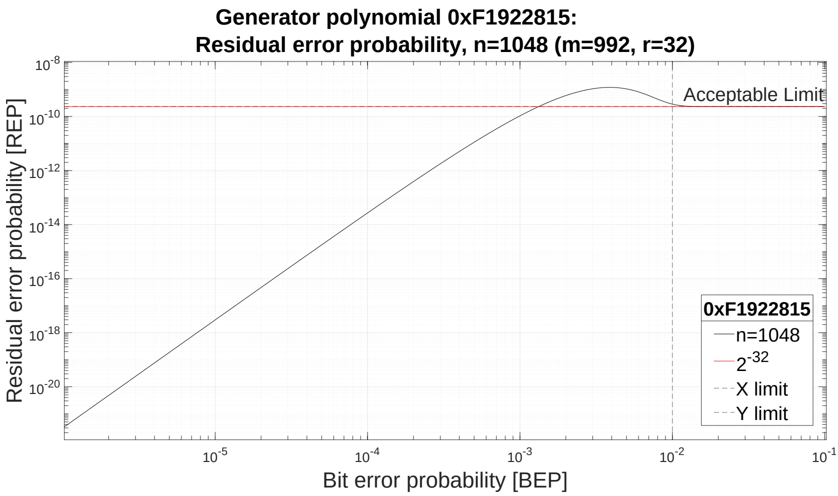


Figure 1.6.: Residual error probability of generator polynomial 0xF1922815 with BSC model (improperness) for $P_{BSC}^{max} = 10^{-2}$.

1.2.6. Error Types in Communication

Communication involves the transmission of information e.g., messages from one device to another or to a group of devices. However, during the process of communication, errors may occur, which possibly lead to misinterpretation of the message. Communication errors are classified in different categories [29] and are described in the following:

Corruption errors (BSC errors) occur when the message is damaged or altered during the transmission process due to several reasons, such as errors on the transmission medium, or message interference.

Unintended repetition errors occur when the same message is delivered to the receiver multiple times. This error can be caused due to an error, fault, or interference.

Incorrect sequence errors occur when the message is delivered to the receiver in the wrong order. This type of error may emerge due to an error, fault, or interference when multiple messages are sent simultaneously, and the receiver receives them in a random order.

Loss errors occur when the message is not delivered to the intended recipient due an error, fault, or interference. Therefore, the message or acknowledgement is not received.

Unacceptable delay errors occur when messages are delayed within its permitted arrival time window. This type of error may result from errors in the transmission medium, congested transmission lines, interference or from bus participants sending messages such as services are delayed or denied.

Insertion errors occur when additional information is added to the message during the transmission process belonging to an unexpected or unknown source entity.

Masquerade errors occur when a message from a non-safety related source is interpreted as originate from a valid safety related source due to a fault or interference. The receiving safety related participant treats the non-safety message as safety related.

Addressing errors occur when the safety related message is sent to the wrong safety related recipient, which then triggers a reception. Here, also the so-called loopback error is often included as addressing error.

A loop-back error is a special addressing error, where the sender receives back its own sent message due to a fault or interference.

Unfortunately, further error types, such as burst errors, shift errors, masquerade errors, or e.g., data errors before decryption or error correction [40], cannot be described by the BSC model and are not separately addressed in [29].

1.2.7. Residual Error Probability Considerations in Safety-Related Systems

A safety-related system is defined in [25] as a system that implements "the required safety functions necessary to achieve or maintain a safe state". Therefore, a certain residual error probability (REP), which is defined as "probability of an error undetected by the safety communication layer (SCL) safety measures" [29], must be determined and corresponds to a specific SIL. According to [29], a SIL is defined as "discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest." The total residual error rate (RER) and SIL relationship is illustrated in the Table 1.1.

Table 1.1.: Typical relationship of RER to SIL based on [29].

Applicable for safety functions (SF) up to SIL	Average frequency of a dangerous failure for SF (PFH)	Maximum permissible residual error rate (RER) for one logical connection of the SF ($\lambda_{SC}(P_e)$)
4	$< 10^{-8}/h$	$< 10^{-10}/h$
3	$< 10^{-7}/h$	$< 10^{-9}/h$
2	$< 10^{-6}/h$	$< 10^{-8}/h$
1	$< 10^{-5}/h$	$< 10^{-7}/h$

IEC 61784-3 [29] states that "the residual error rate (RER) is calculated from the REP of the residual error probability of the superimposed (safety) data integrity assurance mechanism and the sample rate of SPDUs" and also defines equations for its calculation:

$$\lambda_{SC}(Pe) = REP_{SC}(Pe) \cdot v \tag{1.3}$$

$$\lambda_{SCL}(Pe) = \lambda_{SC}(Pe) \cdot m \tag{1.4}$$

where:
- $\lambda_{SC}(Pe)$: Residual error rate per hour of the safety communication channel with respect to the bit error probability,
- $\lambda_{SCL}(Pe)$: Residual error rate per hour of the safety communication layer with respect to the bit error probability,
- Pe : Bit error probability,
- $REP_{SC}(Pe)$: Residual error probability of the safety communication channel with respect to the bit error probability,
- v : Maximum sample rate of SPDUs per hour,
- m : Maximum number of logical connections that is permitted in a single safety function.

Note that the maximum number of logical connections depend on the individual safety function application (see [29] for details).

1.3. Research Aims and Objectives

The overall research aim of this thesis is in the field of the IOLW protocol and its enhancement to communicate safety process data via IOLW.
The research objective is to clarify the feasibility of a safety extension for the IOLW communication protocol and which steps are necessary to obtain a safety extension for IOLW. Therefore, a research field is the domain of functional safety communication with its related standards, necessary functional safety measures applicable and its effectiveness. Also, existing safety protocols on the market with its application-dependent reaction times or necessary reaction times, architecture requirements for a safety protocol designed for IOLW, and e.g., requirements needed for a safety certification are considered. With context to the entire architecture of IOL and IOLW, a new safety extension proposal shall fit to the entire architecture and be implemented with ease. Generally thinking of functional safety applications, a major research objective rises the question how the influence of (cyber-)security is and how the co-adjutant relationship between safety and security is. Is it possible to apply security measures for

safety implementations and how does it effect e.g., the safety requirement specification (SRS)? When implementing security measures or algorithms, power consumption and timing is critical, especially for battery-powered IOLW devices, therefore, these aspects shall also find consideration.

1.4. Structure of the Thesis

This thesis contains within the introduction theoretical background information to introduce the main topics regarding applied protocols, functional safety and (cyber-)security.
In Chapter 2, different state-of-the-art safety protocols are shortly introduced and referenced as well as typical reaction times of safety communication protocols. In the following Chapter 3, a safety architecture proposal for IO-Link Wireless Safety (IOLWS) is discussed. Therefore, the automation environment of IOLW and IOLS is assessed, the relationship of functional safety and (cyber-)security is addressed and general requirements for real-time wireless safety and security applications are stated.
Within Chapter 4, security-for-safety considerations for IOLW are described. Therefore, analysis regarding security of IOLW in the safety domain and device cryptographic performance and energy efficiency are developed and realized. Furthermore, a precision measurement of the application dependent current consumption of a wireless transceiver chip in the time and frequency domain is obtained based on guide to the expression of uncertainty in measurement (GUM). At the end of Chapter 4, a proposal to establish a one-to-one connection from device and master and cryptographic algorithms for IOLW message exchange are suggested.
Chapter 5 is based on the achievements with the certification authority regarding safety requirements for IOLWS. Within the requirement specification, general requirements are stated and a strategy to fulfill the safety requirements is developed. A proposal for an IOLWS SPDU is described and the safety measures and their effectiveness are outlined. Also, the REP is considered and tools for its implementation are presented.
The prototype implementation of the proposed IOLWS protocol is described in Chapter 6. The chapter starts with a system overview followed by the description of the IOLW safety master (FS-W-Master) and IOLW safety bridge (FS-W-Bridge)/IOLW safety device (FS-W-Device). Also, the process data exchange, the security-for-safety communication layer and tests with verification of the prototype implementation are addressed.
Finally, the thesis includes a conclusion and evaluation of the developments, an outlook of further research topics in the field of IOLWS and an extended summary and outlook in German language.

CHAPTER 2

State-of-the-Art Safety Protocols

In this chapter, functional safety protocols such as PROFIsafe, IO-Link Safety, and Safety over EtherCAT (FSoE) are analyzed, representing only an extraction of safety protocols. These functional safety protocols are defined within the IEC 61784-3 [29] with its communication profile families (CPF) and are designed following the black channel principle. Therefore, often a regular communication such as PROFINET, IO-Link or e.g. EtherCAT is utilized and the safety layer must guarantee a high probability of error detection. The error detection of the safety layer must detect the worst conceivable case to offer a high degree of flexibility [40]:

- Various underlying communication protocols are possible.
- Wired or wireless physical layers are feasible.
- The safety communication layer is independent from modifications of the underlying communication layers, e.g., usage of security algorithms.

The safety measures of the respective protocols are outlined with the types of errors and hazard potentials on the basis of a quantitative analysis to demonstrate the suitability for detecting specific error types.

2.1. PROFIsafe

PROFIsafe [43] is a standardized communication protocol for industrial automation applications that combines the real-time capabilities of the PROFINET fieldbus communication system [43] with the functional safety of industrial control systems. The protocol provides a reliable communication network for safety-related data, ensuring that critical information is transmitted accurately and within a specified time frame. PROFIsafe is developed for SIL 3 according to IEC 61508 [25], whereas the black channel principle is utilized using the patented probability of a dangerous failure per hour (PFH) monitor [44] to guarantee the quality of the communication channel. The PROFIsafe protocol is specified in the standard IEC 61784-3-3 [45]. Within the specification the naming F-Host is used for safety controller and F-Device for input or output device. A F-GSD file (General Station Description) is used to transport all information to allow an F-Controller to set up and communicate with the device [43]. Table 2.1 depicts the communication errors being detectable using the specific safety measure referenced.

Table 2.1.: PROFIsafe deployed measures to detect errors based on [43, 45].

Communication error	(virtual) Monitoring Number[a] (MNR)	Timeout with receipt[b]	Codename and optional BaseID for sender and receiver[c]	Data integrity check[d]
Corruption	-	-	-	X
Unintended repetition	-	X	-	-
Incorrect sequence	X	-	-	-
Loss	X	X	-	-
Unacceptable delay	-	X	-	-
Insertion	X	-	-	-
Masquerade	-	-	-	X
Addressing	X	-	X	-
Out-of-sequence	X	-	-	-
Loop-back of messages	X[e]	-	-	-

[a] Instance of “sequence number” of IEC 61784-3.
[b] Instance of “time expectation”(Timeout) and “feedback message”(Receipt) of IEC 61784-3.
[c] Instance of “connection authentication” of IEC 61784-3.
[d] Instance of “data integrity assurance” of IEC 61784-3, based on CRC signature.
[e] In mode $F\_CRC\_Seed = 0$ via status bit 7, in mode $F\_CRC\_Seed = 1$ via one’s complement of MNR.

Furthermore, a watchdog time monitoring with acknowledgment is used to detect timeouts of faulty safety response times. The PROFIsafe SPDU structure is illustrated in Fig. 2.1.

F-Input/Output data	Status / Control Byte	CRC2
Safe process data	Status information, incl. LSB of MNR (toogle bit)	CRC24 or CRC32
0..12/13 octets, max. 123 octets	1 octet	3 or 4 octets

Figure 2.1.: PROFIsafe SPDU structure based on [43, p. 27].

The CRC2 is calculated including F-Input/Output data, status/control byte, MNR(LSB) and the F-Parameter (see [43, p. 74]. If using up to 12 octets process data length, the CRC 24 is used and for up to 123 octets, the CRC 32 is utilized. Therefore, a maximum message length of 128 bits [(13 octets F-Input + 3 octets CRC 24)·8] and 104 bits [(123 octets F-Input + 4 octets CRC 32)·8] is feasible, respectively.
The 32-bit CRC generator polynomial used for PROFIsafe ensures a probability of dangerous failures per hour of less than 10^{-9}/h for the maximum process data length.

2.2. IO-Link Safety

IO-Link Safety (IOLS) is an extended version of IOL that provides safety-critical communication and control between field devices, called functional safety device (FS-Device) and control systems e.g., an functional safety master (FS-Master). The traditional switching of input and output interfaces [46] is extended using coded switching with the specification of a SDCI. Therefore, cyclic exchange of digital input and output process data between a FS-Master and corresponding FS-Devices, such as sensors or actuators, is enabled, whereas the FS-Master may possibly be part of a fieldbus communication. Acyclic communication of parameter or diagnosis information of the FS-Master to its FS-Device is also supported.

All FS-Devices are physically connected in a point-to-point manner to the FS-Master using three wires over distances up to 20 m. Three transmission rates of 4.8 kbit/s, 38.4 kbit/s and 230.4 kbit/s are supported and 24 V I/O signaling is employed. The IODD carries the parameter information and their permitted ranges for the FS-Devices being negotiated during commissioning and testing using a FS-Master tool [30].

Main advantages regarding the SDCI technology are stated in [30]:

- dual use of switching signals (DI/DO) or coded switching communication,
- traditional switching sensors/actuators support single drop digital

communication within the same FS-Device,

- only one cable without shielding for power supply and signaling,
- cost-efficient digital communication.

The IO-Link Safety system is designed to be fully compliant with international safety standards, such as IEC 61508 [25], IEC 62061 [28], and EN ISO 13849-1 [27], providing a high level of safety and reliability. Additionally, the IO-Link Safety system is designed to be easy to integrate into existing control systems, reducing the time and cost associated with its simplicity. The communication errors being detectable using the specific safety measure of IOLS are presented in the following Table 2.2.

Table 2.2.: IO-Link Safety communication errors and safety measures based on [30].

Communication error	Counter/ inverted counter	Timeout with receipt	PortNum + Connection validation[a]	Cyclic redundancy check (CRC)
Corruption	-	-	-	X
Unintended repetition	X	X	-	-
Incorrect sequence	X	-	-	-
Loss	X	X	-	-
Unacceptable delay	-	X	-	-
Insertion	X	-	-	-
Masquerade	-	-	X	X
Addressing	-	-	X	-
Loop-back of messages	X	-	X	-

[a] Connection validation comprises an FSCP authenticity (see A.2.1 in [30]) and the FS-Master Port number.

IOLS uses the following safety measures [30, p. 70]:

- (Sequence) counter / inverted counter
- Watchdog timer and receipt messages
- Connection validation at commissioning, start-up, and repair
- Cyclic redundancy check for data integrity

The structure of the IOLS SPDU of the FS-Master and FS-Device with standard input and output data is presented in Fig. 2.2. The safety measures are explicitly transferred within the protocol regarding measures for timeliness and authenticity (see [29]). A 3-bit counter is used for the timeliness measure and FS-Master port number is included to fulfill the requirements needed for authenticity.

Output PD	CRC signature	Control&MCnt	PortNum	FS-PDout
	Across FS-PDout, PortNum, Control&Cnt	Including 3 bit counter	FS-Master port number	0 to 3 octets, or 0 to 25 octets
32 to 0 octets	2/4 octets	1 octet	1 octet	3/25 octets

From FS-W-Master

From FS-W-Device (one DSlot):

FS-PDin	PortNum	Control&MCnt*	CRC signature	Input PD
0 to 3 octets, or 0 to 25 octets	FS-Master port number inverted	Including 3 bit counter inverted	Across FS-PDin, PortNum, Control&Cnt	
3/25 octets	1 octet	1 octet	2/4 octets	32 to 0 octets

Figure 2.2.: IO-Link Safety SPDU structure based on [30, p. 70].

The specification of IOLS [30] states that "it is suitable for functional safety applications up to SIL 3 or PL_e resulting in a PFH for one connection being less than 10^{-9}/h."

2.3. Safety over EtherCAT

Safety over EtherCAT (FSoE) is a safety communication protocol that provides real-time control and communication between field devices and control systems in industrial environments. It is a specialized version of the EtherCAT protocol that implements safety features to ensure reliable and functional safety operation. FSoE is designed to be fully compliant with international safety standards, such as IEC 61508 [25] and EN ISO 13849-1 [27], providing a high level of safety and reliability. FSoE is developed for SIL 3 according to IEC 61508 [25] utilizing the black channel principle, whereas FSoE uses an partially implicit implementation of safety measures. FSoE is also specified in the standard IEC 61784-3-3 [45]. Table 2.3 depicts the communication errors being detectable using the specific safety measure of [47] referenced.

FSoE uses a combination of hardware and software components to implement safety-related communication and control. The hardware components include specialized safety input/output (I/O) modules and safety-related field devices, while the software components include safety-related communication protocols, such as Safe-RTOS, and safety-related control algorithms [47].

Additionally, FSoE implements diagnostic and error reporting functions to enable the detection and reporting of communication errors. This allows system administrators to quickly identify and resolve issues before escalating into more significant issues. The protocol also includes fail-safe mechanisms, such as redundant communication channels and dual-channel

Table 2.3.: FailSafe over EtherCAT (FSoE) deployed measures to detect errors [45, 47].

Communication error	Sequence Number	Watchdog	Connection optional ID	CRC Calculation
Unintended repetition	X	-	-	-
Loss	X	X	-	X
Insertion	X	-	-	X
Incorrect sequence	X	-	-	X
Corruption	-	-	-	X
Unacceptable delay	-	X	-	-
Masquerade	-	X	-	X
Repeating memory errors in swiches	X	-	-	X
Incorrect forwarding between segments	-	-	X	-

safety systems, to ensure that safety-critical functions continue to operate even in the event of a communication failure.

In contrast to other safety protocols, FSoE includes inheritance of the last received SPDU in the CRC calculation to ensure its difference, even if the previous data was similar [47].

2.4. Reaction Times of Safety Communication Protocols

The response time, i.e. the time duration that an actuator reacts on a message of a sensor device, is a key performance indicator of safety-related communication protocols. In case of safety-related communication routes in the chain between input and output, reaction times are added to receive the total reaction time. As model of such a safety-related chain, typically five components are considered:

- $\Delta\, t_{in}$: processing time of the input signal.
- $\Delta\, t_{com-in}$: the time it takes to transmit a new signal value detected by the input component in a message to the safety controller.
- $\Delta\, t_{logic}$: the time needed by the safety controller with its logic until a result based on the signal value received with the message was calculated.
- $\Delta\, t_{com-out}$: the time it takes to transmit a new calculated safety control result in a message to the output component.
- $\Delta\, t_{out}$: the time that the output component needs until it sets the result that has arrived with the message at its output.

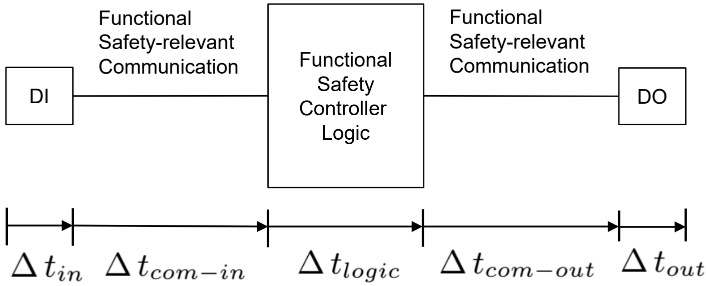


Figure 2.3.: Processing chain of reaction times in communication protocols based on [48, p. 31].

The maximum response time $\Delta\, t_{max}$ is defined as the maximum time that the components with its function, without the presence of an error, need to respond to an event at the input with a reaction at the output. With consideration of safety-related communication systems, the case in which the communication is not violating safety-related monitoring and disturbances in the transmission system must be taken into account. The maximum reaction time of the chain is:

$$\begin{aligned}\Delta\, t_{max} =& \Delta\, t_{max-in} + \Delta\, t_{max-com-in} + \Delta\, t_{max-logic} \\ &+ \Delta\, t_{max-com-out} + \Delta\, t_{max-out}.\end{aligned} \tag{2.1}$$

The maximum times of the individual components are selected for the individual time shares. The maximum time for logic processing $\Delta\, t_{max-logic}$ is typically twice the cycle time of the safety controller.

Furthermore, IEC 61784-3 [29] defines the worst case elapsed response time as “safety function response time” (SFRT), which describes the maximum time needed for a safety function to react.
All relevant components including the programmable electronic system (PES) shall be considered for the safety function response time, even if several functional safety communication profiles consist of different components [29].

CHAPTER 3

Safety Architecture Proposal for Low-Latency Sensor/Actuator Networks using IO-Link Wireless[1]

To enhance the IOLW protocol towards a robust and secure safety protocol in a cyber-physical system (CPS), it is mandatory to provide highly deterministic data exchange functionalities. Therefore, low latency times, low jitter, and low packet loss rates are vital [49]. In the last decades, wireless communication systems have become a fundamental pillar of modern industrial communication realizations (e.g., [11, 50–55]). Even though cellular mobile communication like 2G, 3G, 4G and in particular 5G or beyond are proposed, e.g., in [56–60], several other wireless standards were developed, typically operating in the ISM (industrial, scientific, medical) frequency bands. Classically, wireless automation standards are dedicated or application-related for a specific domain [61], e.g., building automation (ZigBee [62], EnOcean [63]), process automation (wirelessHART [64, 65], ISA 100a [65, 66], WIA-PA [67, 68]) or factory automation (IOLW [4, 22], WIA-FA [68, 69]). Compared with cellular mobile communication technologies, these standards offer lower costs due to highly available energy-efficient, simple, and application-oriented transceiver components operating registration-free, almost worldwide in the ISM bands [8]. The use of a wireless standard for applications in the field of functional safety with ensured latency times in the order of 10 ms as safety critical communication still remains a major technical challenge that none of the aforementioned technologies has yet fully met. As main aspect, the IOLW Safety concept shall be fully compatible with IO-Link Safety and the safety communica-

[1] based on [3]

tion model IEC 61784-3 [29] representing the wireless extension. The engineering tool, the relevant parameters and e.g., the parameter files (IODD) shall be compatible with the IO-Link and IO-Link Safety specifications.

3.1. Wireless Safety-Applications

Wireless communication technologies are key enablers in the context of Industry 4.0, cyber-physical system (CPS) or the Industrial Internet of Things (IIoT).

In the application field of factory automation, strict requirements, such as low latency times in the range of a few milliseconds and high sensor densities in the order of hundred sensors/actuators per production cell [51, 61, 70] have to be fulfilled. As outlined e.g., in [5, Sec. VIII.], the advantages of wireless manufacturing automation are clearly reflected in the area of flexible moving, rotating systems like robots, roaming personnel or automated guided vehicles (AGVs), harsh environments such as aggressive chemical or extreme physical environmental conditions, and especially in the flexible retrofitting of existing systems.

Automation applications are safety-relevant, especially when people and machines interact. Examples include AGVs (e.g., in [71]) or an exoskeleton that helps workers process heavy components (e.g., [72, 73]) and can be controlled wirelessly.

As indicated in [5], existing wireless solutions often cannot offer sufficient performance with respect to real-time and reliability requirements. Furthermore, energy concerns of wireless safety proposals [74–76] as well as the shared transmission of safety and non-safety messages are significant. These challenges shall be overcome with the proposal of IOLW Safety.

3.2. Assessment of the Automation Environment

To develop a suitable solution approach, the automation environment for typical use cases of IOLW and IOLS is analyzed in this section. Therefore, IOLW and IOLS specifications are briefly reviewed.

3.2.1. IO-Link Wireless Architecture

The architecture of an automation topology with an IOLW system is presented in [22, p. 29] describing a programmable logic controller (PLC) or an embedded system exchanging process data (PD) and/or on-request data (OD) wired or wirelessly via the IO-Link Master or W-Master, respectively. The IOLW port and device configuration tool (PDCT) has been already extended compared to the wired IOL Interface and System Specification [1] with features such as device discovery and pairing support, connection quality optimization features, wireless coexistence management features, and support to configure wireless parameters. Faulty W-Devices replacement is achieved using the data storage mechanism of the (wired) IOL specification [1].

3.2.2. IO-Link Safety Architecture

The IO-Link Safety System Extensions, i.e. single-drop digital communication interface for functional safety (SDCI-FS) [30], is the relevant document describing the system architecture and how IO-Link Safety is embedded into a complete factory automation concept. IO-Link Safety aims for two main application areas: safety functions across IO-Link Safety communications and across fieldbusses as well as for safety functions “locally” between a safety controller and safety sensors or actuators. A Functional Safety Communication Profile (FSCP) on top of the fieldbuses support variable parameterization and detailed diagnosis. SDCI (i.e. IO-Link) provides communication as well as power supply on the same unshielded cable to the sensors and actuators. Otherwise, the traditional switching mode or the coded switching mode communication can be used [30, p. 30]. Furthermore, IOLS also supports self-testing safety sensors and actuators in order to avoid battery shortage and yearly testing. An open communication concept as precondition for Industry 4.0 or the Industrial Internet of Things (IIoT) is also established.

3.2.3. IO-Link Wireless Safety Architecture Proposal

Fig. 3.1 shows the proposed IOLW Safety architecture mainly based on IOL (IEC 61131-9) [1,23]. Additional or modified components and features for fail-safe communication are highlighted in bold to address a fail-safe FS-W-Master, fail-safe FS-W-Device as sensor/actuator nodes as well as a fail-safe FS-W-Bridge connected to a wired fail-safe device (FS-Device). Fail-safe IO device descriptions (IODDs) are included within the regular IODD as a digital data sheet as for IOLS. Currently, the IODD is not structured as a certificate using e.g., the X.509 certificate structure [77], which is necessary to identify and to prove the integrity of individual FS-W-Device or FS-W-Bridges. Therefore, public key management including key distribution between the FS-W-Master and the FS-W-Devices / FS-W-Bridges might be a possibility to solve this issue.

The FS-W-Master includes the original standardized master interface (SMI) and the FSCP gateway application (black channel) [30, p. 49]. The master application configuration manager (CM) shall be modified to cope with more track configurations and to send a verification record during each start-up.

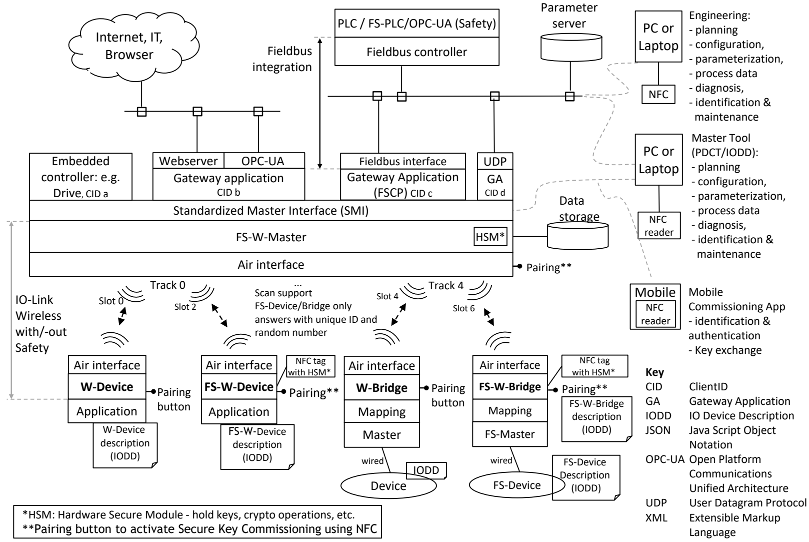


Figure 3.1.: Proposed IOLW Safety configuration (with added features in bold) within the automation hierarchy based on [22], fullpage view in Appendix Fig. D.1.

A functional safety device shall always create a point-to-point or one-to-one connection. Therefore, specific configuration steps are necessary when establishing a connection between functional safety devices. This requirement can be fulfilled using cryptographic algorithms for integrity and authentication in combination with near-field communication (NFC) to establish a secure point-to-point connection between a FS-W-Device and the safety dedicated tool of the FS-W-Master. The FS-W-Device has to be in close proximity equipped with an acknowledgment button for additional identification functionality. It should be noted that the NFC readers and tags shall be protected for unauthorized access, such as controlled access to the environment. Furthermore, the button has to be operated by a qualified safety person initializing the FS-W-Device to the dedicated tool of the FS-W-Master. This process shall be limited in time.
To store cryptographic keys for executing cryptographic algorithms, the NFC tag has been advantageously combined with a hardware security module (HSM). NFC is a short range radio frequency identification (RFID) wireless technology operating around 13.56 MHz, which typically uses an active reader and a passive memory tag. NFC is based on the high frequency RFID standards [78–83]. An advantage using NFC tags technology

is that the tags embedded in the FS-W-Devices do not need an additional power source as the necessary energy is harvested from the electromagnetic near-field. In the application of IOLW, NFC shall be used in the mode of reader-to-passive tag. Commissioning via NFC is explained in Section 4.4. Key management and organization is also a central part of secure operations, therefore, principles should be followed, such as [84–86].

3.2.4. Protocol Stack Architecture

The safety and security enhanced IOLW layered architecture of a FS-W-Master and a FS-W-Device is presented in Fig. 3.2. The physical layer as well as the data link layer of IOLW remain unchanged. System management (SM) services coordinate the system startup phase and allow configuration of possible operational modes, which needed modification compared to the standard W-Devices. This has an effect on communication properties, identification data, and for instance communication states [22].

On top of the data link layer, a security communication layer (SeCL) is provided with the following general and configurable features:

- Handling of pairing and bonding
- Security parameter negotiation
- Encryption key generation and distribution
- Communication to HSM

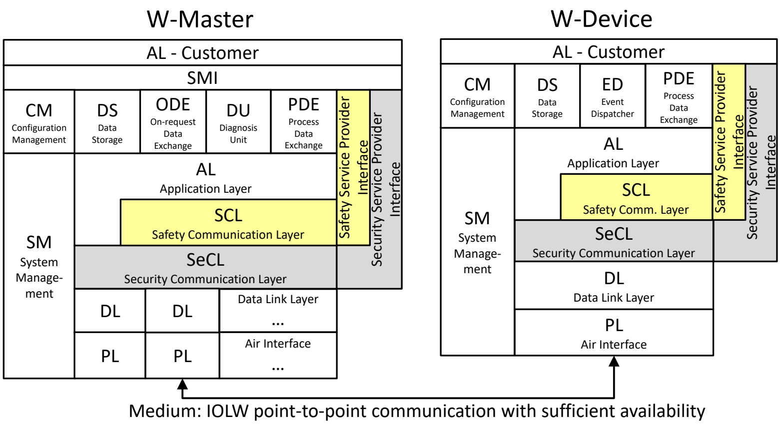


Figure 3.2.: Proposed IOLW safe and secure data transfer architecture.

Depending on the negotiated security parameters ensuring e.g., confidentiality, integrity and authentication of the SPDU, the SeCL exchanges data with the application layer (AL) or the SCL interface. In addition, a service provider interface (SPI) is used to provide security services to the SMI offering services to the customer application layer. In the case of the FS-W-Device, the customer application layer is able to directly access the security service interface. Therefore, a direct interaction of safety and security parameter can be safeguarded. The SCL offers a service provider interface for safety relevant parameters through SMI (FS-W-Master) or directly to the customer AL (FS-W-Device). Also an integration to other safety protocols shall be possible, such as to open platform communications unified architecture (OPC UA) Safety [87].

3.2.5. Key Management

A key management system for FS-W-Masters and FS-W-Devices is vital to securely hold a root/master key or key pair to derive keys for different usage. The secrets are unique for each connection between a FS-W-Master and FS-W-Device or FS-W-Bridge. Depending on the configuration, the following key options should be provided:

- Root FS-W-Master keys, FS-W-Device keys or FS-W-Bridge keys: pre-installed/shared in each device to provide confidentiality for exchanging link keys between a FS-W-Master and a FS-W-Device or FS-W-Bridge during the key exchange procedure.

- Link keys are unique between a single FS-W-Device/FS-W-Bridge and a FS-W-Master and are managed by the application layer. Link keys are used to encrypt all the information exchanged between the FS-W-Master and the FS-W-Devices or FS-W-Bridges as well as to exchange session keys, which shall be changed periodically to secure the data channel.

- Session keys:
  - Safety keys shall be unique between one FS-W-Device or FS-W-Bridge and one FS-W-Master slot and shall be managed by the safety application layer. The keys are used to encrypt SPDU data and to append a message authentication code (MAC).
  - Further application-depend keys should be specified.

3.3. Relationship between Functional Safety and (Cyber-)Security Layer

As already mentioned, functional safety aims to reduce risk of unintended hazards caused by malfunction of system components, whereas security aims to reduce the risk of intentional threats. Nevertheless, safety and security layers and/or functionalities are often separated, because of the following reasons [88]:

- Security is a more dynamic field.
  - New attacks are created constantly with unknown pace.
  - Constant update and verification are needed.
  - Complexity increases through number of connected devices.
  - Several systems of different vendors must be connected securely.
  - Security often handles systems containing or processing secrets or sensitive data (e.g., personal devices and information and communications technology (ICT) systems.
- Functional safety risk analysis is more quantitative compared with security threats relying more on estimates.

Even though functional safety and security are still separated; some interaction might be favorable e.g., because:

- Functional safety is traditionally realized on embedded systems with dedicated control functions, but in future systems interaction with other cyber-physical systems is necessary, which exposes these traditionally enclosed systems to cyber-threats.
- Autonomous driving challenges will change the safety perspective, because of the impact of artificial intelligence. Therefore, applications within the vehicle and with cloud connectivity will create the necessity to update even functional safety functions.

In the field of artificial intelligence and autonomous moving objects, an evolution from fail-safe to fail-operational systems is necessary [88]. Even after an incident or fault, the system must kept functioning and replicate to be safe itself.

CHAPTER 4

Security-for-Safety Considerations for Low-Latency Sensor/Actuator Networks using IO-Link Wireless[1]

4.1. Security Analysis of IO-Link Wireless Communication in the Safety Domain[2]

Security is an essential requirement of industrial control system (ICS)s and its underlying communication infrastructure. Especially the lowest communication level within supervisory control and data acquisition (SCADA) systems or the automation pyramid - the field level - commonly lacks security measures. Since emerging wireless technologies within field level expose the lowest communication infrastructure towards potential attackers, additional security measures above the prevalent concept of air-gapped communication must be considered.

The overall attack surface of IOLW within its typical environment is analyzed and attack preconditions are investigated to assess the effectiveness of different security measures. Additionally, enhanced security measures are evaluated for the communication systems and the results are summarized. Also, interference of security measures and functional safety principles within the communication are investigated, which do not necessarily complement one another but may also have contradictory requirements.

This chapter is intended to discuss and propose enhancements of the IOLW standard with additional security features in future implementations. Due to the constant increase of interconnections within ICSs and CPSs in Industry 4.0, also wireless technologies are increasingly employed

[1] based on [3]
[2] based on [16]

across all communication domains. This improved connectivity pervades all communication layers within typical SCADA systems from the management and planning level to the lower control and field level. Therefore, the attack surface increases not only within internet protocol (IP) based networks but also within the field level. Especially wireless technology can enlarge the attack surface drastically within this low level of communication. Therefore, networks are often physically isolated or separated from one another, such as e.g., information technology (IT) and operational technology (OT) networks. This is called air-gapping and is also employed in field level systems being considered as a sufficient protection measure in combination with physical access control.

But even if field level wireless communication is not the most targeted part for attacks on ICS systems, the lack of attention for security threats within this communication layer can also result in cyber attacks with very high impact for the whole system. Therefore, reasonable security measures should be implemented also for this communication layer to not become the weakest link within a holistic security concept. Besides the number of attacks on ICS rises from year to year. Future areas of applications for field level communication may be found in domains (e.g. mobile roaming device) where physical segregation are unfeasible, therefore security aspects become even more urgent.

IOLW is an example for a wireless field level communication protocol, commonly used below the field bus level. As a safety specification already exists for the wired IO-Link standard [30], a safety extension for the wireless equivalent is proposed for future safey applications [3]. In the first phase of the IOLW standardization process, security risks considerations were not the focus of the protocol design and therefore, at the moment, no security measures are part of the protocol specification [22].

As devices that use IOLW communication protocol are constrained in its resources, common state of the art asymmetric cryptographic methods, e.g. transport layer security (TLS), are not feasible here. But next generation transceiver chips offer hardware acceleration for elliptic curve cryptography (ECC) and may be implemented into the IOLW device stack.

Nevertheless, trade offs must be accepted, when increasing the security level of IOLW communication. A recent proposal already outlined practical security measures for IOLW, while aligning common state of the art wireless protocols and its security measures [3].

The contribution of this section is to determine the overall risk for IOLW communication systems. Therefore relevant attack scenarios are outlined and the impact from safety and security perspective is investigated. Moreover, already proposed security measures, which are intended to protect the communication were analyzed and compared with other existing wireless technologies [3]. Further security enhancements are derived and its applicability is investigated.

4.1.1. Methodology

The methodology depicted in Fig. 4.1 starts with identifying potential security issues of IOLW with reference to the IOLW Systems Extensions - Specification [22]. In the next step, security measures proposed in [3] for safety related IOLW applications are identified and in a further step security enhancements are evaluated regarding prerequisites, consequences, safety and security impact and additional mitigation of the specific attack. Finally, security measures affecting functional safety applications are briefly discussed because this impact is critical and shall be kept in mind.

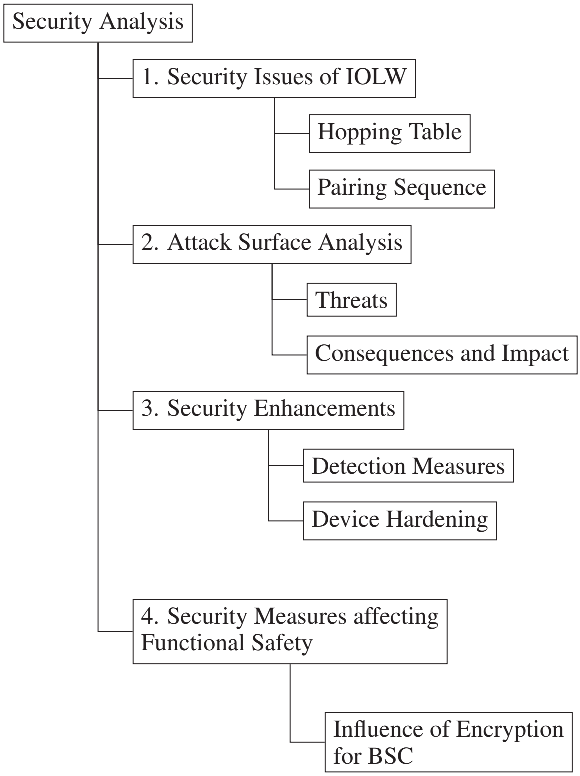


Figure 4.1.: Methodology of Security Analysis

4.1.2. Security Analysis

In this section, an analysis of potential attack surfaces of IOLW communication is presented including a threat and risk analysis.

Therefore, known security issues of IOLW are outlined including the frequency hopping table and the pairing sequence.

4.1.2.1. Frequency Hopping Table

IOLW defines dedicated channel hopping sequence algorithms to compute the frequency hopping tables for a W-Master and its W-Devices. These channel hopping sequence algorithms depend on the individual W-Master ID to achieve wireless coexistence within neighboring IOLW systems. Additionally, a blocklisting can be utilized to avoid certain frequency channels in the computed hopping table favoring wireless coexistence with other wireless systems nearby.
Blocklisting is a mechanism to avoid over-the-air collisions with other wireless systems, such as WLAN. Conventional Bluetooth cannot be blocklisted, since it is an uncoordinated frequency hopper. The blocklist itself uses eighty 1 MHz wide frequency channels and the master configuration setting can be used to suspend frequency ranges [22, p. 35].

The default channel hopping table of IOLW is $HT01$ omitting frequencies f_{1-2} and f_{79-80}. For configuration, the frequency channels f_1 and f_{80} are used and f_2 and f_{78} are Guard-Channels. Blocklisting of each 1 MHz frequency channel is possible. The carrier frequencies f_n in IOLW are defined according to [22] as $f_n = f_0 + n \cdot 1\,\mathrm{MHz}$; (1) with $f_0 = 2400\,\mathrm{MHz}$ and $n = 3$ to 78 (i.e. up to 76 frequency channels) for cyclic data communication. The Adaptive Hopping Table mechanism enables a change of the hopping table of a track while the communication is already running, which may be an improvement of the connection [22, p. 300–302].

4.1.2.2. Pairing Sequence

IOLW offers different possibilities to pair a W-Device with a W-Master [22]:

- Pairing by UniqueID, which enables the pairing of an unpaired W-Device to a W-Master Port using a pairing request.
- Pairing by Button / Re-Pairing can be used to change a damaged W-Device without using a port and device configuration tool (PDCT) or to pair a W-Device to an unused, pre-configured W-Port during commissioning phase. Therefore, a pairing button or a similar trigger is mandatory for a W-Device.

- Roaming describes a feature to pair a W-Device temporary to a W-Master, which allows predefined W-Devices between multiple W-Masters.

If one W-Master track is in ServiceMode, the configuration channels are available and only in this mode scan, pairing, and roaming activities are possible [22]. But in all cases, messages are sent without encryption and authentication. Also, no shared secret between two devices initially exists or is created, which can be used for initial authentication or as temporary authentication or encryption key. The transfer of a W-Device identification in plain-text is fairly insecure.

For a security-enhanced pairing sequence, a key establishment technique ideally approved by [89] and recommendations for cryptographic key generations [90] are essential. Key exchange possibilities such as Rivest-–Shamir-–Adleman (RSA), Diffie-Hellman (DH), elliptic-curve Diffie-Hellman (ECDH) based key exchange protocol, elliptic-curve Menezes-Qu-Vanstone (ECMQV), or certificate-based pairwise key establishment (CPKE) are described and evaluated for security-enhanced IOLW pairing in [3]. Here, an out-of-band (OOB) commissioning technology using NFC is suggested to exchange a shared secret. Note that additional hardware is necessary in this case.

4.1.2.3. Attacks on Cryptographic Measures

In [3], AES-CCM with 32-bit or 64-bit authentication tag is suggested and investigated. Crafting a valid authentication tag would enable an attacker to bypass the cryptographic authentication measure. Therefore, the probability of a birthday attack on the authentication tag shall be evaluated.

$$Adv < \frac{q_{dec}}{2^{\tau}} + \frac{\sigma^2}{2^n} \tag{4.1}$$

with
τ: length of the tag in bits
σ: number of encrypted / decrypted blocks
n: block size of the cipher, in bits (128 for AES)
q_{dec}: allowed number of decryption queries
Adv (adversary): the probability that an attacker breaks the associated security definition, which shall be less than one in 1,000,000 for each random attempt to succeed or a false acceptance to occur [89].

Additionally, in [89] is also stated that “for multiple attempts to use authentication mechanism during a one-minute period, the probability shall be less than one in 100,000 that a random attempt will succeed or a false acceptance will occur”. For each attempt, the value of q_{dec} shall be ideally 1, respectively as low as possible.

For one IOLW DSLOT payload (14 bytes) with a MAC of $\tau = 32$ using all three uplink messages (message from a W-Device to a W-Master), the following parameter can be assumed:

$$\begin{aligned} Adv[\tau = 32] &\leq \frac{3}{2^{32}} + \frac{1^2}{2^{128}} \\ Adv[\tau = 32] &\leq 7 \cdot 10^{-10} \end{aligned} \tag{4.2}$$

For $\tau = 64$, the probability of crafting a valid MAC is:

$$\begin{aligned} Adv[\tau = 64] &\leq \frac{3}{2^{64}} + \frac{1^2}{2^{128}} \\ Adv[\tau = 64] &\leq \ 1.6 \cdot 10^{-19} \end{aligned} \tag{4.3}$$

The lowest transmission time for one message in IOLW is about 1.664 ms and with two retries about 5 ms. If within two retries no correct message in combination with a valid MAC was sent, the W-Master rejects further messages of this W-Device and W-Port. A reconfiguration is needed, therefore the probability values are already based on 1 min as referred to in [89].

In both cases, the probability is much smaller than one in 1,000,000 that a random attempt will succeed and, hence the attack to craft a valid MAC is very unlikely. Possibly a shorter MAC would also be secure, since a three byte MAC results in a probability of about 10^{-7} (considering that within one minute, the probability shall be less than one in 100,000). Even if a high computational power is available, the prove for a three byte MAC is unfeasible, therefore this topic is investigated with a theoretical approach. With a two byte MAC, the probability

$$Adv[\tau = 16] \leq 4.6 \cdot 10^{-5} \tag{4.4}$$

does not fulfill the requirements of [89].

If accepting more faulty packets and the allowed number of decryption queries increases by three tries (including each two retries), the availability of the application increases and the probability that an attacker breaks the associated security definition is still low:

$$\begin{aligned} Adv[\tau = 32, q_{dec} = 9] &\leq \frac{9}{2^{32}} + \frac{1^2}{2^{128}} \\ Adv[\tau = 32, q_{dec} = 9] &\leq 2.1 \cdot 10^{-9} \end{aligned} \tag{4.5}$$

Increasing the payload (multiple DSLOTs), while only using a four byte MAC for e.g. ten DSLOTs, does not significantly increase the probability that an attacker breaks the associated security definition and is therefore regarded to be sufficient. Here, the approximation that one DSLOT is equal to one encrypted/decrypted block is used.

$$\begin{aligned} Adv[\tau = 32, q_{dec} = 9, \sigma = 10] &\leq \frac{9}{2^{32}} + \frac{10^2}{2^{128}} \\ Adv[\tau = 32, q_{dec} = 9, \sigma = 10] &\leq 2.1 \cdot 10^{-9} \end{aligned} \tag{4.6}$$

This evaluation depicts that the proposed authentication length is sufficient secure for the probability of an attacker breaking the associated security definition [89].

4.1.3. Attack Surface Analysis

This section examines the attack surface for IOLW communication using relevant attack scenarios. Previous mentioned security issues are considered during the discussion of attack scenarios.

Timeliness of communication bursts and knowledge of the frequency hopping table are two additional hurdles to take for executing a successful attack on the wireless communication.

The consequences of different attack scenarios vary, and therefore the overall impact must be investigated in detail. Within this analysis section, the impact for each attack scenario is rated from a security and a safety perspective. This analysis is used to select and derive suitable protection mechanisms and to assess the effectiveness of already proposed measures.

Security goals within a threat analysis are a common approach to describe the impact of cyber attacks. A very common security goal model is the CIA-triad, which contains the security goals *Confidentiality*, *Integrity* and *Availability*. This concept has its origin in the IT domain, but is also usable in the OT domain. The most important distinction for the OT environment is the fact, that availability is one of the most important goals.

While the use of CIA-triad is common practice within the security domain, approaches exist including security aspects being mapped onto safety functionalities [91].

A safety function relying on IOLW may have two states according to intended disturbance attempts from an attacker - affected or unaffected. No advantage of a finer distinction of impact from safety perspective is recognized, therefore only a differentiation of impact or no impact is done.

The result of this attack surface analysis is depicted in Table 4.1.

Table 4.1.: Possible IOLW attacks influencing the safety and security of its application

Attacks	Prerequisites	Consequences	Safety Impact	Security Impact (CIA-triade)	Additional Mitigation
Denial-of-Service (Flooding)	- Known Hopping Table, - Knowledge of IOLW configuration - IOLW W-Master in pairing mode	- W-Master is blocked by processing flooding packets - Valid packets cannot be processed in time - W-Master goes back to initial safe mode	No	Availability	- Early Attack detection using a IOWL Sniffer - Secure transmission of Hopping Table
Jamming	- Jamming 2.45 GHz communication	- W-Master is blocked by processing flooding packets - Valid packets cannot be processed in time - W-Master goes back to initial safe mode	No	Availability	Jammer detection
Replay Attack	- Hopping Table - Sniff valid traffic - Replay sniffed packets	- W-Master is blocked by processing flooding packets - Valid packets cannot be processed in time - W-Master goes back to initial safe mode	No	Availability	Replay attack discovery on IOLW W-Master
Packet Forgery	- Current counter value - Known Hopping Table	- Rare chances to craft valid MAC/payload	Yes	Availability, Integrity	Detection of malicious packets on IOLW W-Master
Packet Forgery (Leaked Key)	- Current counter value - Known Hopping Table - Leaked key	- Attacker can create valid MAC for any payload.	Yes	Availability, Integrity	IOLW W-Device hardening measures e.g. tamper detection
Attacker controls IOLW W-Device (backdoor)	- Physical or remote access to IOLW W-Device e.g. via backdoor	Full control to create valid IOLW messages	Yes	Availability, Integrity, Confidentiality	Device hardening, IDS Systems, Anomaly detection in IOLW W-Master

Each attack scenario is described with the prerequisites necessary for successful execution of each threat. Next, the consequences of an successful attack are described. These consequences are rated for its safety and security impact on a generic use case based on IOLW communication. At the end of each attack scenario description, additional mitigation are listed, which are intended to protect against the mentioned threat. These mitigation are outlined in more detail within the following section.

The overall outcome of the attack surface analysis, presented in Table 4.1 shows that attacks, which only disturb the communication or the timely arrival of messages, have no safety impact. This is supported by the fact, that common safety peers enter a safe state in such events, where no harm originates from the system. These events only lead to impact the availability of the system and are relevant for security observations.

Critical and often not considered within safety analysis is the crafting of valid messages and injecting these into the communication system. Therefore, safety functions relying on IOLW communication can be manipulated, e.g. safety sensor values become falsified. These attacks are considered having a severe safety impact.

From a security perspective all considered attack scenarios impact the protection goal availability of the communication system, which is assumed to be the most targeted goal for attackers. Disturbances of availability lead directly to financial consequences for the asset owner. Attacks like flooding, jamming or replay attack are considered to be more innocuous in its execution, in comparison to the attack scenarios, which also impact functional safety. An attacker with the goal to disturb the availability is assumed to use these attacks instead of attacks with more pre-work necessary.

When security enhancements are enabled within the protocol stack, all safety impacting attacks have to bypass the cryptographic measures, e.g., key knowledge or weak cryptographic measures. These measures are considered to address the threat of safety impact by state of the art cryptography. Further mitigation are necessary to detect and react early on attack attempts. These are presented in the following section.

4.1.4. Further Security Enhancements

All attack scenarios on IOLW communication require physical proximity to the devices. Therefore, the feasibility of such attacks is generally rated potentially low. Nonetheless, further measures beyond physical access restrictions are considered necessary, since wireless networks may not be physical protectable for all use cases. Therefore, the following enhanced security implementations are recommended:

1. Assessment of the automation environment
2. Establishing a one-to-one connection
3. Cryptographic algorithms for IOLW message exchange

The counter measures include the handling of pairing and bonding, security parameter negotiation, encryption, key generation and distribution, and e.g. communication to a HSM.
Establishing a one-to-one connection involves security during commissioning of secrets and security after commissioning of the network key.
Also, possible cryptographic algorithms for IOLW message exchange, such as AES-CCM and others e.g. in [14], are evaluated.

Next to these measures, additional mitigation are derived from the listed attack scenarios. Attacks on IOLW communication itself have multiple preliminaries. Execution of attacks with real impacts to the communication system are considered difficult, especially due to the need of physical proximity, knowledge of cryptographic key, frequency hoping table and correct time of message exchange.

Further mitigation can be categorized in the following two types, which are depicted now.

4.1.4.1. Detection Measures

A potential security loophole was identified within the beginning of communication via IOLW. As the hopping table is transmitted in clear text without using any cryptographic measures between the W-Master and W-Device, sniffing of this table is a potential threat. Possession of the frequency hopping table enables certain previous presented attack scenarios.

A cryptographic protected transmission of the table is seen as a possible solution to address this threat. If an security-enhanced pairing exchanges a session or link key to encrypt further communication packets, the frequency hopping table could be adjusted post initial pairing. Another possible solution to protect the transmission of the hopping table is e.g. via OOB.

Integrity and authenticity is addressable by the use of a MAC [92]. Unfortunately, the limited message length restricts the use of only four bytes or even three bytes for the MAC. The use of truncated MAC authenticator length weakens the state of the art cryptography and does not match recommendations. To inhibit brute force attacks, the W-Master should react on receiving wrong MAC authenticators with the transition of the communication system towards a fail-state. Receiving multiple wrong MACs indicate malicious actions on the involved W-Device. A shut down of the communication path after detection of irregular behavior reduces the probability of a successful guess for a valid MAC. This behavior results in availability impact of the system, but reduces the potential successful guessing and safety impact. To sum up these observations, the truncated MAC is seen as sufficient measure.

To detect and react early on attack attempts further measures should be implemented within the communication environment. For instance, an independent sniffer node, which is described for IOLW in [93], could be installed, to detect malicious traffic at an early state of attack. Especially flooding and jamming attempts are addressed by this measure. Since no measures within the protocol design can mitigate flooding or jamming attacks, an early detection of such attacks is an essential building block within an overall IOLW security concept.

4.1.4.2. Device Hardening

Attacks on the IOLW communication are overall rated rather unlikely, since attacks on remotely accessible devices, e.g. the IOLW master are more likely and the impact is assumed higher. Therefore, further device hardening measures on the W-Master are considered necessary and should be implemented by the vendor. Here, the main focus is the communication itself.

But also W-Device should be hardened by implementing a defense-in-depth protection strategy. This addresses the attack scenario of fully controlled W-Device for instance by applying secure boot, tamper detection and cryptographic protection for key information stored on the W-Device. Therefore, the development cycle should be aligned to the IEC 62443-4-1 security standard and security measures from IEC 62443-4-2 should be defined as targeted security levels [34].

4.1.5. Security Measures Affecting Functional Safety

A functional safety protocol is not initially secure and also vice versa a security protocol is not in general functional safe, because functional safety mechanisms detect residual errors whereas security mechanisms try to detect errors/manipulations injected purposely or created unintentionally.

The assumption of a certain residual error probability, such as the probability of undetected errors, with a distribution for the black channel principle is typically based on the BSC model [29]. Several error types might not be described sufficiently using the BSC model, particularly when using security algorithms in the underlying communication layers [40]. Security algorithms being BSC-preservative and even being viewed as part of the black channel are offering greater efficiency and flexibility [94, 95]. Both papers also describe that fail-safe communication mainly focuses on random errors, but lacks cryptographic techniques protecting against attacks.

A particular problem evolves because some well-established assumptions for functional safety mechanisms may become incorrect using cryptographic algorithms. Therefore, an authenticated and encrypted message may become secure, but the necessary risk reduction for a certain SIL classification cannot be guaranteed any longer. In this case, functional safety and (cyber-)security are not independently from each other. This case and complexity is described in detail in [95] with a short safety telegram being transferred encrypted and received with a complete different plaintext as initially intended. The logical consequence is that a sustainable safety protocol must meet modern communication requirements including encryption and the worst possible BEP of 0.5 being stated in EN 50159 [96]. Starting in 2019, a IEC working group (project IEC TR 63069 Ed1) created a framework for functional safety and security, which involves guidance on the common application of IEC 61508 [25] and IEC 62443 [34] in the area of industrial-process measurement, control and automation. The aim of the working group and its technical report is to provide guidance that both fields have no negative influence on each other.

4.1.6. Summary of IOLW Threat Analysis

Need for security within IOLW has been outlined using a methodology to identify potential security issues of IOLW, evaluating the security measures proposed in a former publication for safety related IOLW applications, and depicting security enhancements regarding prerequisites, consequences, safety and security impact and additional mitigation of specific attacks.

The probability of a birthday attack on the authentication tag has been evaluated for different tag and message length showing that the proposed tag length is sufficient secure. Also impact on safety and security goals have been rated within the listed evaluation. The derived security enhancements for the listed attack scenarios have been outlined and can be used for real world applicability evaluation.

The attack scenarios analyzed have all impact on the availability of the communication system. On the other hand, safety impact requires bypassing of implemented cryptographic measures. Attackers with the intention to disturb the availability will more likely execute attacks without safety impact, since attacks like flooding are easier to carry out.

Furthermore, security measures affecting functional safety have been discussed with the influence of creating new models for the residual error probability when applying cryptographic algorithms within the black channel. To maintain existing and previous model calculations, a separation of functional safety and security is still eligible.

4.2. Device Cryptographic Performance and Energy Efficiency[3]

In this section, cryptographic performance and energy efficiency of an W-Device are analyzed. The power consumption and the influence of the cryptographic operations on the transmission timing of the IOLW protocol are exemplary measured employing a module based on a TI CC2650 system-on-chip (SoC) radio transceiver [97]. Confidentiality is considered in combination with the cryptographic performance as well as the energy efficiency. Different cryptographic algorithms are evaluated using the on chip hardware accelerator compared to a cryptographic software implementation.

4.2.1. Accurate Measurement of Cryptographic Performance and Energy Efficiency on CC265x

The cryptographic performance and energy efficiency of IOLW Devices is essential for its acceptance and usage. Application report [98] describes the duration and the power consumption of different cryptographic algorithms in software and hardware using the CC2652. The benefits of using the hardware accelerated drivers in comparison to a software based implementation is discussed for crypto operation duration, relative runtime performance and energy efficiency versus a software implementation. The tests are measured on a SimpleLink multi-standard CC26x2R wireless MCU LaunchPad development kit [99], which offers AES, hash, public key accelerator and true random number generator (TRNG).

The execution time of the hardware implemented algorithm is measured using the hardware accelerators with the crypto drivers. For the crypto software duration, the open source software mbedTLS (build with version 2.7.9 and compiled with the TI ARM C/C++ 18.12.1.LTS compiler using -O3 optimization settings) is used as a reference implementation. The average current of the hardware accelerator consumed during the operation

[3] based on [14]

is measured through turning on and off accelerators. In the application report [98], measurements were made with an Agilent N6705B Power Analyzer [100]. The accuracy of the voltage and current measurements is based on the type of power modules that are installed. Currently, a good fit for this measurement seems to be the Keysight Precision DC Power Modules N6761A or N6762A with the following DC power module key performance specifications shown in Table 4.2.

Table 4.2.: DC Power Module Key Performance Specifications according to [100, p. 24].

	DC output ratings (volts/amps/watts)	Current programming accuracy	Current measurement accuracy
N6781A	20 V/±3 A/20 W	0.04% + 0.3 mA	0.03% + 0.25 mA
N6782A	20 V/±3 A/20 W	0.04% + 0.3 mA	0.03% + 0.25 mA

For measurement evaluation e.g. of AES-CBC for 64 bytes with 3.84 mA the current measurement accuracy of the measurement device is decisive. For an average current of 3.84 mA the current measurement accuracy ($I_{acc/N6700}$) with the N6700 is:

$$\begin{aligned} I_{acc/N6700} &= 3.84\,\text{mA} \pm \left[\frac{0.03\%}{100\%} \cdot 3.84\,\text{mA} + 0.25\,\text{mA} \right] \\ &= 3.84\,\text{mA} \pm 0.2512\,\text{mA}. \end{aligned} \tag{4.7}$$

The lower limit is at around 3.59 mA and the upper limit at 4.09 mA, when measuring a current of 3.84 mA.

Therefore, different commercially-available measurement equipment to measure the current more accurate was evaluated. The R&S RT-ZVCxx with an 18 bit ADC was chosen to measure the current due to its suitable measurement range and accuracy, whereby the measurement range and DC accuracy is given in Table 4.15.

Table 4.3.: DC Characteristics of the R&S RT-ZVCxx [101, p. 5].

Measurement range	DC accuracy
system all ranges except 4.5A and 10A	±(0.2%of reading +0.02% of range)
system, 4.5A range	±(0.3%of reading +0.02% of range)
system, 10A range	±(0.2%of reading +0.09% of range)

The measurement range is 45 mA and results in a measurement accuracy for the RT-ZVC ($I_{acc/ZVC}$), which can be calculated for a measured current value of 3.84 mA:

$$\begin{aligned} I_{acc/ZVC} &= 3.84\,\mathrm{mA} \pm \left[\frac{0.2\%}{100\%} \cdot 3.84\,\mathrm{mA} + \frac{0.02\%}{100\%} \cdot 45\,\mathrm{mA} \right] \\ &= 3.84\,\mathrm{mA} \pm 0.0167\,\mathrm{mA}. \end{aligned} \tag{4.8}$$

In this case, the measurement accuracy is about factor 15 improved compared to the measurement accuracy of the calculated one in Eq. 4.7. The measurement range is adjusted with an external resistor to achieve a smaller measurement range, which is shown in the following subsection.

4.2.1.1. Different Measurement Setup Approach

In the application report [98, p. 8], the power management driver approach is described for Elliptic-curve Diffie–Hellman (ECDH) in general. The peripheral driver and power driver put the device into the lowest possible power state to measure only the influence on the cryptographic algorithms. In comparison to the measurement setup of the application report [98], the measurement setup described in 4.2.1.2 does not only measure the cryptographic algorithm and powers down all peripherals, this measurement rather measures the influence of cryptographic algorithms while operating in IOLW mode.

4.2.1.2. Measurement Setup for IOLW Transmission

For all measurements, the radio transceiver was programmed to use the maximal output power during wireless data transfer. Additionally, the radio transceiver is using a bare metal application rather than an real-time operating system (RTOS). Therefore, all power saving modes were disabled in order to achieve reproducible results.
To achieve a more appropriate measurement range, a measurement setup, shown in Fig. 4.2 with an external shunt is used.

The tolerance of the resistor is considered in the overall measurement accuracy. Therefore, the external shunt resistor represented by $\mathrm{R_{ext}}$ with a resistance of 2.21 Ω and a tolerance level of 0.1% is evaluated. As Device-Under-Test (DUT) a Phytec module based on a CC2650 SoC radio transceiver chip is used. A measurement range of ±20.362 mA is achieved. The values from Subsection 4.2.2.1 fit in this range and higher current values when starting the measurement can be compensated.

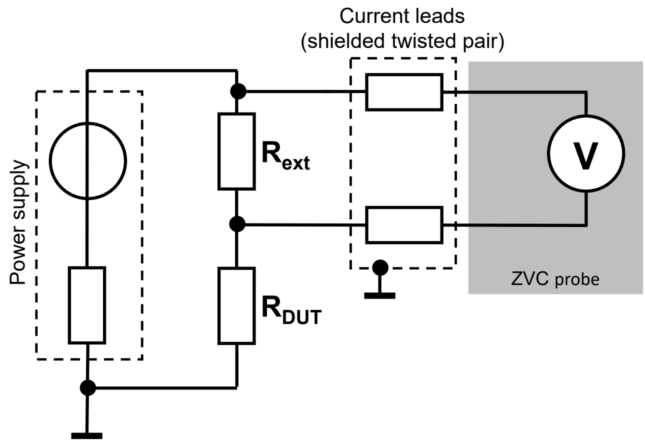


Figure 4.2.: Simplified setup of measurement with external shunt, recommended in [102].

The abbreviated symbols characterize the measured current (I_{meas}), tolerance of the external resistor with additional connectors (R_{tol}), and the internal ADC tolerance of the ZVC probe (ADC_{tol}). With this configuration, the following accuracy is achieved:

$$\begin{aligned} I_{acc/ZVC} &= I_{meas} \pm \left[\frac{\%R_{tol}}{100\%} \cdot I_{meas} + \frac{\%ADC_{tol}}{100\%} \cdot I_{range} \right] \\ &= 8.6\,\mathrm{mA} \pm \left[\frac{0.2\%}{100\%} \cdot 8.6\,\mathrm{mA} \right. \\ &\left. + \frac{0.02\%}{100\%} \cdot 20.362\,\mathrm{mA} \right] \\ &= 8.6\,\mathrm{mA} \pm 0.0213\,\mathrm{mA}. \end{aligned} \tag{4.9}$$

With the 18 bit ADC, 262143 vertical steps can be realized over a scale of $\pm 20.362\,\mathrm{mA}$, which results in $155.35\,\mathrm{nA}$ steps. If it can be assumed that the last two bits are negligible, the accuracy of $621\,\mathrm{nA}$ steps over $\pm 20.362\,\mathrm{mA}$ should be feasible.

4.2.2. Measuring Performance and Energy Efficiency of AES algorithms with different message lengths

Different return behaviors for calling the cryptographic operations are possible. The return behavior can be characterized as following:

- Callback: The function call will return immediately while the cryptographic operation goes on in the background. After the operation completes, the registered callback function is called. It depends on the implementation if the callback function is called as task, hardware interrupt (HWI), or software interrupt (SWI).
- Blocking: The function call will block while the cryptographic operation goes on in the background. After the function returns, the cryptographic operation results are available.
- Polling: The function call will continuously poll a flag while the cryptographic operation goes on in the background. After the function returns, the cryptographic operation results are available.

For the equation of performance values and for energy efficiency characterization (4.11), the return behavior blocking is used due to its simplicity and the fact that no other operation needs to be performed simultaneously. For many applications callback and polling return behavior might be more relevant or applicable. There are multiple ways to store cryptographic keying material on an embedded system. The different options are: RAM or flash, key store, key blob, or plaintext (PT). For performance tests, only PT cryptographic keying material are used. For real applications, a different option for higher security concerns shall be considered.
The tests and measurements concerning energy consumption and time duration of the different cryptographic algorithms are performed with official test vectors from the following sources:

- AES-ECB test vectors from: [103]
- AES-CBC test vectors from: [103] and [104]
- AES-CTR test vectors from: [103] and [105]

Each measurement consists of 50 k samples, acquired at 5 MSa/s time. In each measurement series, 445 data sets consisting of each 50 k samples (at 5 MSa/s) are recorded (2.225 G samples). In Matlab, these records are averaged and then used for further calculations. To measure the influence of the cryptographic algorithms compared to the PT mode or unencrypted operation, only every other downlink, cryptographic operation is activated. This way, in a measured time of 10 ms three measurements with cryptographic operation and three without (in regular) operation are recorded and evaluated. At the same time, thermal effects are neglected, because the effects are subtracted with the operation without cryptographic algorithm. The debugging equipment was connected to the transceiver chip during the operation for automated testing and adds a current consumption of 0.13 mA to the overall consumption. An example measurement of 16 bytes AES-CBC is shown in Fig. 4.3. The data was smoothed by a moving average filter over 101 samples.

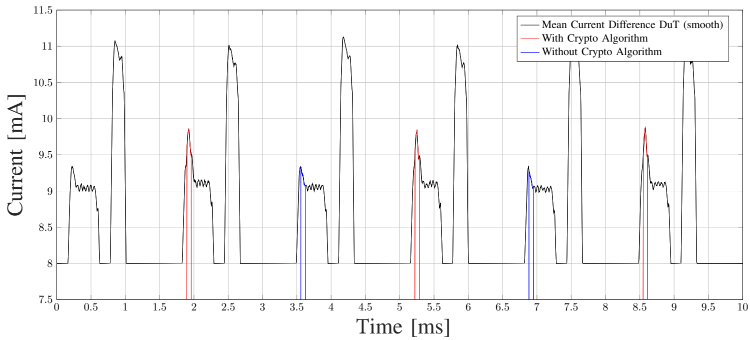


Figure 4.3.: AES-CBC Encryption of 16 bytes using the on chip hardware accelerator.

The difference of the mean current ($I_{DuT\_Diff\_Mean}$) with and without cryptographic operation is shown in Fig. 4.3 and the different cryptographic algorithms are presented in each individual table. From the measured values, the duration improvement (K_{DI}) and the energy efficiency improvement (K_{EEI}) can be calculated as following:

$$K_{DI} = \frac{\Delta t_{mbedTLS}}{\Delta t_{HW}} \tag{4.10}$$

$$\text{and} \qquad K_{EEI} = \frac{\Delta t_{mbedTLS} \cdot \overline{I_{mbedTLS}}}{\Delta t_{HW} \cdot \overline{I_{HW}}}. \tag{4.11}$$

The duration and energy efficiency improvement describe the relative performance increase or decrease, depending of the value being greater or smaller than 1, of a hardware accelerated module or a pure software implementation. The larger the number, the more efficient it is to use a hardware accelerated module.

4.2.2.1. Plaintext Mode

In plaintext (PT) mode (non-encrypted), an indentation is needed of how long a general-purpose input and output (GPIO) takes to switch when transmitting PT data. Therefore, the switching duration is measured. As shown in Table 4.4, the duration increases from 0.53 μs to 1.8 μs.

Table 4.4.: Plaintext GPIO Swiching Duration.

Payload Length [bytes]	Duration [μs]
8	0.53
16	1.53
32	1.80

The average current consumption is measured on each uplink of the W-Device and shown in Table 4.5 with a value of around 8.6 mA.

Table 4.5.: Plaintext Average Current Consumption.

Payload Length [bytes]	Average Current Consumption [mA]
8	8.607
16	8.608
32	8.609

4.2.2.2. AES-ECB

The Electronic Code Book (ECB) mode of operation is a generic encryption block cipher mode, which can be used with any block cipher. AES-ECB encrypts or decrypts one or multiple blocks of PT or ciphertext using the Advanced Encryption Standard (AES) block cipher. Each input block is individually encrypted or decrypted. Therefore, blocks of ciphertext can be decrypted individually and do not have to be in order [106]. When encrypting the same PT with the same key an identical ciphertext results, which raises security issues. Hence, it is not recommended that ECB shall be used. For scientific purposes, AES-ECB on the CC2650 is analyzed as software library and hardware accelerator using the IOLW protocol stack. A default key length of 128 bits and PT input length of 8, 16, 32 bytes are used, therefore, the duration is only affected by the PT input length. The duration improvement using an hardware acceleration depends on the

length of the payload and is shown for AES-ECB in Fig. 4.4.
For 8 to 16 bytes, the improvement factor is 1.5 to 1.6 and for 32 bytes around 2.9. Time duration of up to 172.9 μs do not result in transmission errors and are in general feasible for IOLW transmissions.

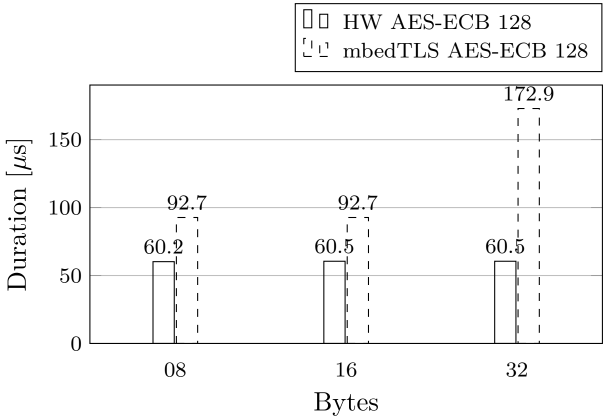


Figure 4.4.: AES-ECB Duration Improvement.

The energy efficiency depends on the duration of the operation and the average current consumption. If the value is higher than 1, the hardware accelerator consumes less energy than the software algorithm. For 8 and 16 bytes the energy efficiency improvement is about a factor of around 1.6 and for the payload length of 32 bytes, the energy efficiency improvement is around 2.9, which is shown in Table 4.6.

Table 4.6.: Comparison of AES-ECB Hardware and Software Cryptographic Algorithm's Energy Efficiency.

Payload Length [bytes]	Average Crypto Current HW [mA]	Average Crypto Current SW mbedTLS [mA]	Energy Efficiency Improvement
8	9.635	9.686	1.55
16	9.549	9.700	1.60
32	9.598	9.663	2.86

If different length of payloads are used to measure the difference of current consumption for AES-ECB with hardware acceleration or software implementation to current consumption for PT transmission, the PT-based energy efficient improvement(K_{PT-EEI}) can be calculated as follows:

$$K_{PT-EEI} = \frac{\Delta t_{mbedTLS} \cdot \overline{Idiff_{mbedTLS}}}{\Delta t_{HW} \cdot \overline{Idiff_{HW}}}, \tag{4.12}$$

whereby $Idiff$ is the current difference with cryptographic operation and without in PT mode operation. Table 4.7 is showing current difference and PT-based energy efficiency improvement for AES-ECB.

Table 4.7.: Comparison of AES-ECB Hardware and Software Cryptographic Algorithm's Current Difference to Plaintext and its Energy Efficiency Improvement.

Payload Length [bytes]	HW Idiff AES-ECB to pt [μA]	mbedTLS Idiff AES-ECB to pt [μA]	PT-based Energy Efficiency Improvement
8	356.7	547.3	2.4
16	368.5	547.7	2.3
32	403.1	414.0	2.9

If the PT-based energy efficiency improvement is larger than 1, the hardware accelerator shows a higher efficiency than the software implementation.

The relative battery lifetime reduction can be calculated using the average current measured over 10 ms (i.e. six wireless cycles) with AES-ECB compared to the PT average current consumption from Table 4.5. Table 4.8 shows the relative battery reduction of 0.4 to 1.2% depending on the payload length and hardware accelerator (HW) or software-based (SW) cryptographic algorithm.

4.2.2.3. AES-CBC

The Cipher Block Chaining (CBC) mode of operation is a generic block cipher mode of operation. It can be used with any block cipher including AES. CBC mode encrypts messages of any practical length that have a length evenly divisibly by the block size.

Table 4.8.: Comparison of AES-ECB Hardware and Software Cryptographic Algorithm's Average Current Consumption and its Relative Battery Lifetime Reduction.

Payload Length [bytes]	Average Current HW [mA]	Relative HW Battery Lifetime Reduction [%]	Average Current SW [mA]	Relative SW Battery Lifetime Reduction [%]
8	8.683	0.9	8.682	0.9
16	8.646	0.4	8.646	0.4
32	8.648	0.4	8.718	1.2

In comparison to ECB, CBC guarantees confidentiality of the entire message whenever the message is larger than one block [104]. This is the reason for the duration time for 8 or 16 bytes to be almost similar, which is shown in Fig. 4.5. For the hardware accelerator, the values stay almost constant. The software implementation shows an increase of about 1.5 from 16 to 32 bytes. The duration improvement from the hardware accelerator to the software implementation increases with higher payload than 16 bytes from the factor of 1.66 to 2.65 for 32 bytes.

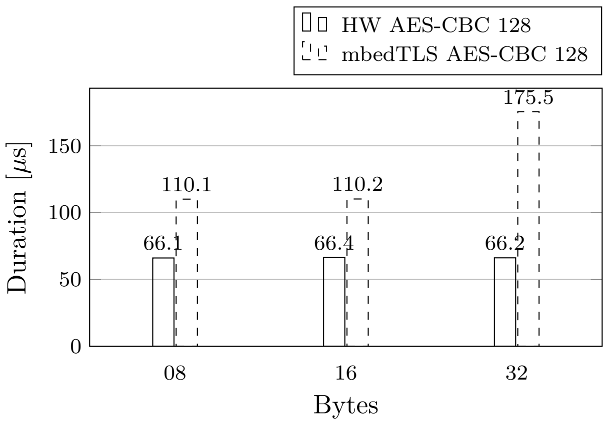


Figure 4.5.: AES-CBC Duration Improvement.

The energy efficiency improvement for AES-CBC increases by the similar factor than the duration improvement and has an significant advantage for the hardware accelerator, which is shown in Table 4.9.

Table 4.9.: Comparison of AES-CBC Hardware and Software Cryptographic Algorithm's Energy Efficiency.

Payload Length [bytes]	Average Crypto Current HW [mA]	Average Crypto Current SW mbedTLS [mA]	Energy Efficiency Improvement
8	9.662	9.602	1.66
16	9.673	9.663	1.66
32	9.632	(9.457)	(2.60)

The measurements for mbedTLS with a payload of 32 bytes had to be repeated with a similar setup due to an error in the data set. Therefore, the measurements are in parenthesizes.
The PT-based energy efficiency improvement of AES-CBC shows values below 2 for payload length of 8 and 16 bytes. For 32 bytes payload length, the hardware accelerator has a factor of 2.5 higher efficiency than the software implementation, which is shown in Table 4.10.

Table 4.10.: Comparison of AES-CBC Hardware and Software Cryptographic Algorithm's Current Difference to Plaintext and its Energy Efficiency Improvement.

Payload Length [bytes]	HW Idiff AES-CBC to pt [μA]	mbedTLS Idiff AES-CBC to pt [μA]	PT-based Energy Efficiency Improvement
8	476.2	486.4	1.7
16	505.0	458.8	1.5
32	423.8	(396.1)	(2.5)

The relative HW battery reduction compared to PT is 0.3% to 0.8% and the relative SW battery reduction compared to PT is slightly higher between 0.7% and 1.1%. The values are presendetd in Table 4.11.

4.2.2.4. AES-CTR

The Counter (CTR) mode of operation is a generic block cipher mode, which can be used with any block cipher including AES. The CTR mode of operation encrypts and decrypts messages. An advantage of this algorithm is that it is not required for the message length to be evenly divisible by the cipher block size. Therefore, padding the message is not required [105].

Table 4.11.: Comparison of AES-CBC Hardware and Software Cryptographic Algorithm's Average Current Consumption and its Relative Battery Lifetime Reduction.

Payload Length [bytes]	Average Current HW [mA]	Relative HW Battery Lifetime Reduction [%]	Average Current SW [mA]	Relative SW Battery Lifetime Reduction [%]
8	8.679	0.8	8.670	0.7
16	8.633	0.3	8.668	0.7
32	8.640	0.4	(8.709)	(1.1)

The duration improvement of the hardware accelerator compared to the software implementation is for 8 bytes and 16 bytes almost similar with a factor of 1.7 and 1.75. For 32 bytes, the duration improvement equals 2.84. The values are presented in Fig. 4.6.

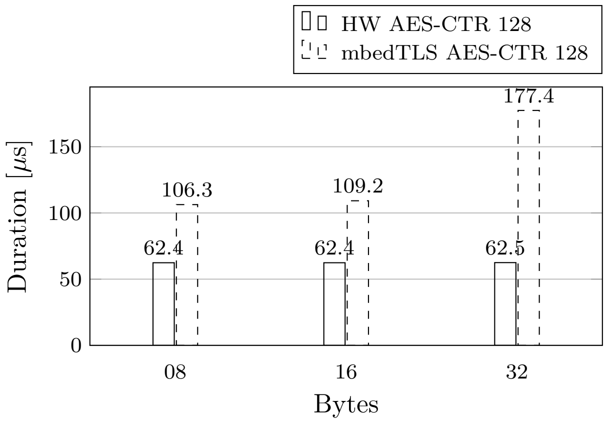


Figure 4.6.: AES-CTR Duration Improvement.

Table 4.12 shows that the energy efficiency improvement increases by a similar factor for 8 and 16 bytes than the duration improvement in favor of the hardware accelerator. The value of 32 bytes for the energy efficiency improvement is slightly smaller than the one for the duration improvement.

Table 4.12.: Comparison of AES-CTR Hardware and Software Cryptographic Algorithm's Energy Efficiency.

Payload Length [bytes]	Average Crypto Current HW [mA]	Average Crypto Current SW mbedTLS [mA]	Energy Efficiency Improvement
8	9.537	9.579	1.71
16	9.560	9.557	1.75
32	9.637	9.442	2.78

In Table 4.13, the PT-based energy efficiency improvement shows for the evaluation of AES-CTR for 8 and 16 bytes a factor of above 2 in favor of the hardware accelerator. It seems with an increase in payload, also the PT-based energy efficiency improvement decreases. This is not highly relevant for IOLW because the focus is rather on short message lengths.

Table 4.13.: Comparison of AES-CTR Hard- and Software Cryptographic Algorithm's Current Difference to PT and its Energy Efficiency Improvement.

Payload Length [bytes]	HW Idiff AES-CBC to pt [μA]	mbedTLS Idiff AES-CBC to pt [μA]	PT-based Energy Efficiency Improvement
8	298.8	390.8	2.2
16	315.6	387.6	2.2
32	424.7	272.1	1.8

The relative battery reduction compared to PT is 0.2% to 0.9%, depending on the payload length and hardware accelerator (HW) or software-based (SW) cryptographic algorithm. The detailed results are presendetd in Table 4.14.

Table 4.14.: Comparison of AES-CTR HW and SW Crypto Algorithm's Average Current Consumption and its Relative Battery Lifetime Reduction.

Payload Length [bytes]	Average Current HW [mA]	Relative HW Battery Lifetime Reduction [%]	Average Current SW [mA]	Relative SW Battery Lifetime Reduction [%]
8	8.683	0.9	8.689	0.9
16	8.645	0.4	8.673	0.7
32	8.630	0.2	8.665	0.6

4.2.3. Summary of W-Device Cryptographic Performance and Energy Efficiency

The possibility to implement different cryptographic algorithms to accomplish confidentiality for the IOLW protocol has been demonstrated. The hardware accelerator driver of a CC2650 based transceiver chip as well as an open source software implementation from mbedTLS have been used to encrypt PT during the uplink transmission of the IOLW Device. The execution time and energy improvement of the transceiver chip have been measured using an external shunt resistor circuit to achieve an appropriate measurement range as well as an adequate accuracy. Therefore, standardized block cipher modes of operations have been tested and evaluated for the hardware accelerator driver and the software implementation. The measurements have shown that by using the chosen cryptographic algorithms for confidentiality the hardware accelerator driver has advantages in duration and energy efficiency. The factor of improvement ranges from around 1.5 to almost 3 in favor of using the hardware accelerator of a Phytec module based on a CC2650 SoC radio transceiver chip for payload length of 8, 16 and 32 bytes.

In addition, the relative influence of the different cryptographic algorithms and implementations on the battery life were investigated. As a result, the battery lifetime is only reduced by up to 0.9% for the hardware accelerator and up to 1.2% for the software implementation (mbedTLS) used in a worst case. For most algorithms and payload lengths, the relative battery lifetime reduction is even less. Thus, the implementation of such cryptographic algorithms have no significant drawback on the battery lifetime.

The question of how to enhance the presented measurement is analyzed and answered within the next Section 4.3.

Furthermore, some wireless technologies such as BLE or Zigbee, use AES-CCM, which is a generic authenticate-and-encrypt block cipher mode [107]. CCM can be described as counter with CBC-MAC, defined as cipher block chaining mode with message authentication code. Therefore, in Section 4.5 AES-CCM is tested for different payload length to add authentication to messages. Possibilities to achieve integrity for each message is also investigated.

4.3. Precision Measurement of the Application dependent Current Consumption of a Wireless Transceiver Chip[4]

Modern production concepts generate a demand for reliable, energy-efficient, fast and secure wireless communication solutions. Therefore, the current consumption should not increase highly due to additional cryptographic operations. Here, a principle current measurement method exemplary of a transceiver for the IO-Link Wireless protocol is presented. Low-pass filtering and single side amplitude spectrum analysis are used to evaluate the main information of the current measurement. An uncertainty estimation is realized using statistical measurement data with considerations of the measurement setup to approximate the combined standard uncertainty. The results show that the current consumption only increases slightly, when using additional cryptographic operations. This can be measured with acceptable uncertainty.

In Sect. 4.3.1, the principle measurement method is presented and in the following Sect. 4.3.2, the measurement setup is depicted. In the corresponding Subsect. 4.3.2.1, the utilized equipment with its characteristics, the low-pass filtering and single side amplitude spectrum evaluating the information of the signal are described.

4.3.1. Principle Measuring Method

Figure 4.7 shows the principle measurement approach for the application- and time-depending current. Preliminaries for the principle measurement approach are among other things, the option to add an external shunt circuit to the power probe to approximate the measurement range. Also a constant voltage source is needed as well as a precision ohmmeter (or multimeter) to measure the final external shunt with its connectors.

Power probes are benchmarked depending on the measurement task, therefore, a market research is performed and data sheets are evaluated. Then, the first measurement is realized with the internal shunt resistor of the selected power probe to find an indentation of the measurement range using the transceiver in plaintext mode of operation. In the next step, an external shunt resistor circuit is selected to achieve a fitting measurement range for the plaintext mode of operation, because an external exchangeable shunt resistor achieves a better fitting measurement range for using the full internal analog to digital converter (ADC) resolution of the measurement device. When enabling the W-Device to send alternating plaintext and encrypted messages, the external shunt resistor circuit is adjusted. This alternating mode is used for the measurement of the application dependent current. In the following step, a variable low-pass

[4] based on [15, 108]

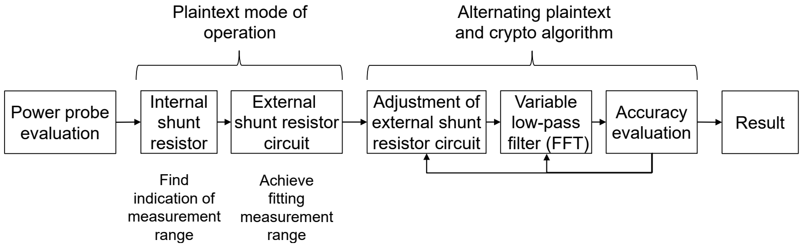


Figure 4.7.: Principle Measurement Approach presenting the chronological Sequence of the individual Steps.

filter using fast Fourier transformation (FFT) is used iteratively to eliminate noise and observe, in which frequency ranges the information of the current measurement signal is located. An accuracy evaluation consisting of a statistical evaluation is performed. If the result is considered as accurate enough, the measurement is completed by an overall uncertainty estimation. If not, the external shunt resistor circuit and/or the variable low-pass filter shall be adjusted again. This contribution mainly focuses on the last steps, consisting of the low-pass filtering, accuracy evaluation and uncertainty estimation.

4.3.2. Measurements

Current measurements via a shunt resistor are very common [109, 110]. This approach is also utilized here, as described in the following. A measurement setup with an external shunt is used [14] as shown in the previous Section 4.2 in Fig. 4.2 in order to achieve a more appropriate (and accurate) measurement range compared to the setup with an internal shunt. A RT-ZVC power probe [102] is used to measure the current consumption. As device under test (DUT), a Phytec module based on a CC2650 SoC radio transceiver is used [97]. The external debugger being connected to the DUT is not depicted here. A constant voltage source [111] provides a stable voltage supply for the DUT.

4.3.2.1. Measurement Assessment

For each measurement series, 445 data sets consisting of each 50 k samples (at 5 MSa/s) are recorded within a period of 10 ms, which makes in total 2.225 GSa. The period of 10 ms corresponds to two IOLW cycles or in total six IOLW sub-cycles (i.e., six DL and UL messages). The appropriate measurement range of 13.81 mA was chosen by selecting a shunt resistor measured with a precision multimeter [112] having a value of 3.259 Ω. Note that the current measurement range corresponds to the internal measurement range of 45 mV in the power probe RT-ZVC. The accuracy of the current measurement can be approximated by selecting the appropriate type of current (DC or AC) according to the data sheet of the power probe. Table 4.15 depicts the measurement range of DC and AC signals of the power probe. Theoretically, the 18 bit ADC resolves 105.3 nA steps over an input range of 13.81 mA (45 mA / 3.259 Ω). Practically, the accuracy is usually not limited by the internal ADC resolution, but rather other effects, as described in the following.

Table 4.15.: DC and AC Characteristics of the R&S RT-ZVCxx [102, p. 5].

Measurement range	DC and AC accuracy
all ranges except 4.5 A and 10 A	± (0.2 % of reading + 0.02 % of range)
AC1: 10 Hz to 40 kHz	± (0.4 % of reading + 0.02 % of range)
AC2: 40 kHz to 100 kHz	± (2 % of reading + 0.02 % of range)
AC3: 100 kHz to 270 kHz	± (10.9 % of reading + 0.02 % of range)

4.3.2.1.1. Low-pass Filtering

In this section, a comparison with different low-pass filtering is performed in order to determine a suitable frequency-related accuracy range of the measurement device. The current measurement without additional low-pass filtering, in the following referred to as "unfiltered current measurement", is compared to low-pass filtered signals with cutoff frequencies of 100 kHz, 40 kHz, and 5 kHz. These cutoff frequencies corresponds to the characteristic measurement ranges referred to in Table 4.15 with the addition of a cutoff frequency of 5 kHz resulting from the iterated process described in Fig. 4.2.

Figure 4.8 shows one example measurement series of an AES-ECB encryption of 16 bytes using the on-chip hardware accelerator without any filtering. In black the current of the DUT is presented over a time of 10 ms with 6 sub-cycles. The mean current value of the example measurement is 8.62 mA. The lower current ripple is always the DL message and the higher current ripple the UL to the W-Master. The red mark shows, when a crypto algorithm is performed, and the blue mark shows, when the signal is transferred using plaintext. Using Matlab, the same time interval in the next UL is evaluated and marked in blue without crypto algorithm. $I_{DuT\_Diff\_Mean\_ifft}$ represents the mean current difference of the measurement signal of the red (with cryptographic operation) and blue (without cryptographic operation) current consumption. In the following, it is referred to as "mean current crypto difference".

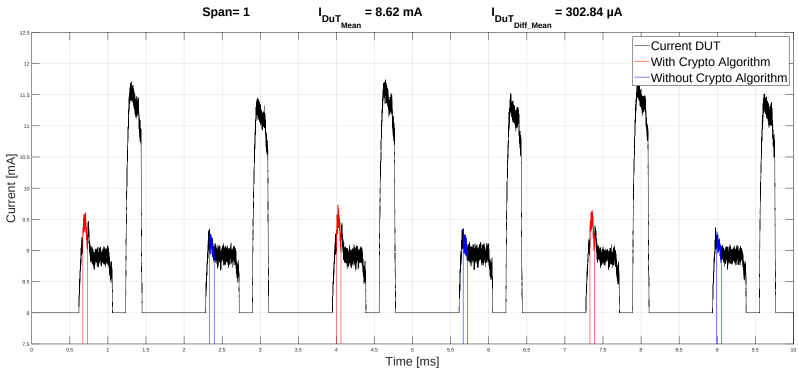


Figure 4.8.: Current measurement without additional low-pass filtering.

The measurement is performed for cutoff frequencies of 100 kHz in Fig. 4.9, 40 kHz in Fig. 4.10, and 5 kHz in Fig. 4.11. Here, a variable low-pass filter using FFT was used to eliminate noise and to observe, in which frequency ranges the information of the signal is located.

If the unfiltered current measurement is compared to the signal with a cutoff frequency of 100 kHz, the mean current of the DUT is similar to the value of the unfiltered current measurement. Comparing the value of the mean current crypto difference (100 kHz) to the value of the unfiltered current measurement results in a difference of about 1 μA.

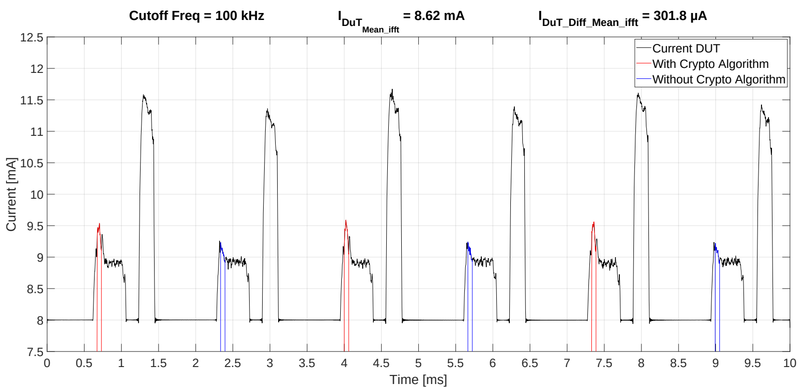


Figure 4.9.: Signal of the Current Measurements with Low-pass Filtering (Cutoff 100 kHz).

When low-pass filtering using a cutoff frequency of 40 kHz is applied, the mean current of the DUT is still similar to the mean current value of the unfiltered current measurement. The mean current crypto difference is about 301 μA, which corresponds to a difference of about 2 μA compared to the unfiltered current measurement.

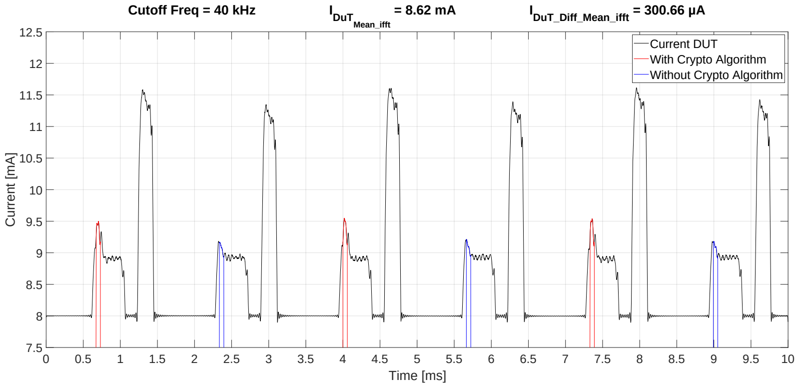


Figure 4.10.: Signal of the Current Measurements with Low-pass Filtering (Cutoff 40 kHz).

When low-pass filtering at a cutoff frequency of 5 kHz is performed, the mean current of the DUT still remains at 8.62 mA, but the value of the mean current crypto difference is about 90 μA compared to the value of the unfiltered current measurement.

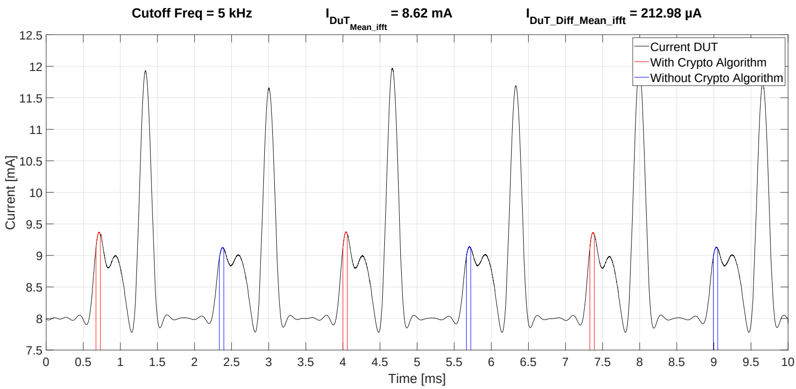


Figure 4.11.: Signal of the Current Measurements with Low-pass Filtering (Cutoff 5 kHz).

Table 4.16 shows the mean current crypto difference and its difference to the unfiltered current measurement. The difference at a cutoff frequency of 5 kHz is around 30% to the unfiltered current measurement. This deviation is orders of magnitude above the accuracy specified for the AC1 range in Table 4.15. In addition, it is already optically recognizable that the current signal in Fig. 4.11 clearly deviates from the unfiltered current measurement by a significant amount of information loss. Further research on the single side amplitude spectrum and a statistical evaluation shall define the suitable frequency-related accuracy range.

Table 4.16.: Mean Current Crypto Difference compared to Value of the unfiltered Current Measurement.

Low-pass filtering (cutoff frequency)	Mean current crypto difference [μA]	Difference to unfiltered current measurement [μA]
Unfiltered measurement current	303	-
5 kHz	213	90
40 kHz	301	2
100 kHz	302	1

4.3.2.1.2. Single Side Amplitude Spectrum

The single side amplitude spectrum obtained from FFT is evaluated in the following. In Fig. 4.12, the full spectrum of the measured current without low-pass filtering is displayed. Respectively, Fig. 4.13 depicts the single side amplitude spectrum with a cutoff frequency of 100 kHz, which shows similar information as the original spectrum. Fig. 4.14 represents the spectrum with a cutoff frequency of 40 kHz showing most of the information content. The main information seems to be presented in the area up to about 30 kHz, therefore Fig. 4.15 shows that parts of the main information are cutoff, which might be necessary to represent the signal.

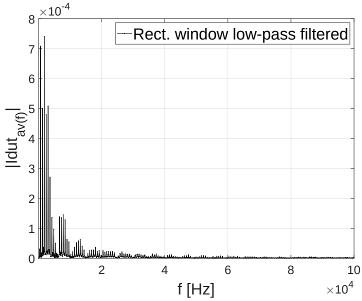


Figure 4.12.: Single Side Amplitude Spectrum of the Current Measurement Signal, without additional Low-pass Filtering.

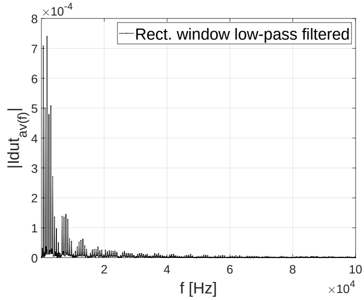


Figure 4.13.: Single Side Amplitude Spectrum of the Current Measurement Signal with Low-pass Filtering (Cutoff 100 kHz).

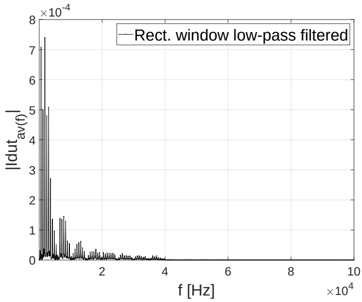


Figure 4.14.: Single Side Amplitude Spectrum of the Current Measurement Signal with Low-pass Filtering (Cutoff 40 kHz).

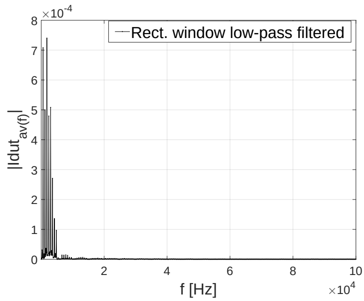


Figure 4.15.: Single Side Amplitude Spectrum of the Current Measurement Signal with Low-pass Filtering (Cutoff 5 kHz).

4.3.2.1.3. Comparison of Signals with different Cutoff Frequencies

Overall, the frequency components above 40 kHz can be neglected in very good approximation, because the main information is in the area up to about 30 kHz. The accuracy in terms of the current can be calculated for example with AC 1, range of 13.81 mA, a reading of 8.63 mA and measurement accuracy of the power probe given in Table 4.15.

For example if using the AC 1 range (10 Hz to 40 kHz) for a measurement of 8.63 mA an accuracy of plus minus $37.3\,\mu A$ can be achieved according to the data sheet, as shown in Eq. (4.13).

$$\begin{aligned} I_{\text{acc/ZVC}} &= 8.63\,mA \pm \left[\frac{0.4\%}{100\%} \cdot I_{\text{reading}} + \frac{0.02\%}{100\%} \cdot I_{\text{range}} \right] \\ &= 8.63\,mA \pm \left[\frac{0.4\%}{100\%} \cdot 8.63\,mA + \frac{0.02\%}{100\%} \cdot 13.81\,mA \right] \\ &= 8.63\,mA \pm 0.0373\,mA. \end{aligned} \tag{4.13}$$

Table 4.17 shows the DC and AC characteristics of power probe applied to the measurement. As it is assumed that the main information is in the range of AC1, the corresponding accuracy will be considered in Sect. 4.3.3.2.2.

Table 4.17.: Applied DC and AC Characteristics of the R&S RT-ZVCxx from the Measurement.

Measurement range	Mean current [mA]	Accuracy [mA]
DC	8.63	± 0.02
AC 1: 10 Hz to 40 kHz	8.63	± 0.037
AC 2: 40 kHz to 100 kHz	8.63	± 0.175
AC 3: 100 kHz to 270 kHz	8.63	± 0.943

4.3.2.2. Intermediate Results

The mean values and experimental standard deviation were calculated for the mean current of the DUT and the current difference of crypto to plaintext mode, respectively. Table 4.18 shows the intermediate measurement results.

Table 4.18.: Statistical Measurement Results.

	Current mean DUT	Current difference of crypto to plaintext
Mean value	$8.63\,mA$	$316.2\,\mu A$
Experimental standard deviation	$15.2\,\mu A$	$25.0\,\mu A$

The experimental standard deviations of the mean currents are factor 2.5 smaller than the accuracy according to the data sheet of the measurement equipment, and therefore, about two orders of magnitude larger than the theoretical step size of the ADC. The mean value of the current difference has a value of $316\,\mu A$, resulting in a minor influence on potential battery lifetime. The experimental standard deviation of the current difference of crypto to plaintext is $25\,\mu A$, which is significantly smaller than the mean current difference of crypto to plaintext and also smaller than the calculated accuracy of the AC1 measurement range of the power probe.

4.3.3. Uncertainty Estimation

Based on the "Guide to the expression of uncertainty in measurement" (GUM) [113] an abbreviated uncertainty estimation is presented in this section. An integrated measurement equipment is used, which is specified with respect to the measurement uncertainty (see Table 4.15). Therefore, the focus is on the parameters, which have an additional influence on the measurement results. In [114–118], the current consumption of different chips in various operation conditions or configurations are presented. This section will adopt some of the approaches for the uncertainty estimation presented in [118] and [116].
For this current measurement via a shunt resistor, it can be assumed for the modeling of the measurement, that the uncertainty of the measurand, i.e., the current, is (at least) related to the shunt resistance, frequencies of the signal, sampling, etc., temperatures of the individual components and its environments, the supply voltage, the device characteristics of the power supply as well as the measuring device. However, the focus lies on the influencing factors for which the expected impact is greatest, as outlined in Sect. 4.3.3.1.

4.3.3.1. Uncertainty Sources

The components indicated before are discussed here in detail. In particular, Table 4.15 lists an accuracy according to the datasheet, which is at least 0.2% of the reading value. This best-case value is taken as reference to consider, whether single uncertainty components might be negligible.

4.3.3.1.1. Frequency Dependence

As indicated in Paragraph 4.3.2.1.1, the frequency of the signal or its components determines, which measurement range has to be adjusted for the RT-ZVC power probe. In the frequency ranges considered here, however, other frequency-dependent effects are comparatively negligible: First, the overall circuit is small compared to the relevant wavelength. Second, a typical SMD (surface-mounted device) shunt resistor often the skin effect becomes secondary, according to [109]. Furthermore, for frequencies far below 1 MHz, the SMD shunt resistor can even be assumed as purely resistive with almost constant characteristics over frequency.

4.3.3.1.2. Supply Voltage Dependence

A precision power supply was used, whereby its characteristics are given in the data sheet [111] as voltage ripple noise $< 500\,\mu V$(RMS). Furthermore, the Phytec CC2650 module has a typical operating voltage of 1.8–3.8 V, as the module has internal power regulation [97]. The nominal operating voltage is 3.3 V, thus the relative voltage ripple and noise from the power supply is about $1.5 \cdot 10^{-4}$ and thus small in comparison with the tightest accuracy of the power probe.

4.3.3.1.3. Shunt Resistor

As indicated in Fig. 4.2, the current measurement is essentially based on a voltage measurement across the shunt resistor R_{shunt}. Thus, the measurement device outputs a value for the current to be measured, which is calculated from the internally measured voltage and the entered value of the external shunt resistor.

4.3.3.1.4. Measurement Instrument

The main uncertainty contribution is estimated to be related with the RT-ZVC power probe (see Table 4.15). The values given in Table 4.15 are treated as Type B uncertainties according to GUM. Basically, the shunt resistance, the measuring device and the current consumption of the chip itself have an influence on the measurement result. However, temperature effects will not be considered here in detail for the following reasons:

- The DUT and the measurement device were switched on for a while before the measurements. Therefore, a stationary state is assumed for their temperature.
- The ambient temperature was kept constant during the measurements.
- The temperature coefficient of the shunt resistor is $\alpha = \pm 2\,\text{ppm}/^\circ\text{C}$, according to [119]. Even an unrealistically large assumed temperature difference of 20 K would consequently only cause a relative change of 40 ppm, which can be neglected with respect to the other uncertainty sources.
- The temperature coefficient of the power probe is stated as $0.15\,\times$ specified accuracy/°C outside the nominal specified temperature range, according to [102]. As the nominal specified temperature range covers an ambient temperature interval of 6°C, it was to ensure that this was not exited during the measurements. As a result, no additional temperature related effect has to be considered here.

Furthermore, due to the applied measurement principle based on the difference with and without crypto algorithms, effects caused by a changing temperature are neglected for the following reason. The mass as well as the heat capacity of the used transceiver chip is such that its temperature can be assumed to be unchanged during the period of time considered for evaluation .

4.3.3.2. Combined Uncertainty Assessment

According to GUM [113] and assuming linear approximation, the combined uncertainty u_c can be derived from

$$u_c = \sqrt{u_A^2 + u_B^2}, \tag{4.14}$$

whereby u_A denotes the Type A uncertainty obtained by statistical methods (measured) and u_B denotes the Type B uncertainty, obtained e.g., from data sheets (equipment including shunt resistor).

For further details on the derived combined uncertainty see Appendix A.

4.3.3.2.1. Type A Uncertainty Analysis

To determine the current I_{DUT_Mean}, the mean value was calculated of ten measurements consisting each of 445 datasets with each 50 k samples, according to Sect. 4.3.1. Furthermore, its experimental standard deviation was calculated according to [113] and presented in Table 4.18. Thereby, it was assumed that the values obtained from the ten measurements and each 445 data sets are uncorrelated as they represent resultant quantities of different evaluations that have been made independently. This assumption is motivated by the fact that both the temporal behavior of the DUT and the power probe are sufficiently fast having no (temporal) correlation of the samples. Furthermore, the common setup is accounted for by an independent standard uncertainty, which is considered in the following section. This approach is based on [113, Sect. 5.2.4]. Using the same approach, the mean value as well as the experimental standard deviation of the current difference of the crypto to plaintext mode were determined. The results are listed in Table 4.18.

4.3.3.2.2. Type B Uncertainty Analysis

As reasoned before in Paragraph 4.3.2.1.3, the AC 1 measurement range according to Table 4.15 are considered here. Due to [113, Sec. 4.3.7, Ex. 2], a uniform distribution is assumed for this data sheet statement, resulting in a half-width a_{ZVC} of the assumed symmetric uniform distribution with $a_{\mathrm{ZVC}} \approx 37.3\,\mu A$, as calculated in Eq. 4.13 and stated in Table 4.17. Using [113, Eq. 7], i.e., $u^2(x_i) = a^2/3$, this results in

$$u_{\mathrm{ZVC}}\left(I_{\mathrm{DUT\_Mean}}\right) = \sqrt{a_{\mathrm{ZVC}}^2/3} \approx 21.5\,\mu\mathrm{A}. \tag{4.15}$$

As a second aspect, the uncertainty of the shunt resistor is also considered as Type B uncertainty here, because it is not purely based on statistical evaluation but rather also on the data sheet of the utilized multimeter. A symmetric uniform distribution is assumed. With the given values in its data sheet [112] resulting in a half-width of $a_{\mathrm{R}} \approx 2 \cdot 10^{-3}\,\Omega$. Using [113, Eq. 7], this yields to

$$u_{\mathrm{R}}\left(R_{\mathrm{shunt}}\right) = \sqrt{a_{\mathrm{R}}^2/3} \approx 1.2 \cdot 10^{-3}\,\Omega. \tag{4.16}$$

As approximation, a linear influence of the relative uncertainty of R_{shunt} is assumed for the current $I_{\mathrm{DUT\_Mean}}$ [113]. Thus, $u_{\mathrm{R}}\left(R_{\mathrm{shunt}}\right)/R_{\mathrm{shunt}} \approx 3.5 \cdot 10^{-4}$ will be considered as another Type B uncertainty for the current by $u_{\mathrm{R}}\left(I_{DUT\_Mean}\right) \approx \frac{u_{\mathrm{R}}(R_{\mathrm{shunt}})}{R_{\mathrm{shunt}}} \times I_{\mathrm{DUT\_Mean}}$, resulting in

$$u_{\mathrm{R}}\left(I_{\mathrm{DUT\_Mean}}\right) \approx 0.0031\,\mathrm{mA} \approx 3.1\,\mu\mathrm{A}. \tag{4.17}$$

For the (overall) Type B uncertainty, $u_B^2 = u_{\mathrm{ZVC}}^2 + u_{\mathrm{R}}^2$ is considered in the following.

4.3.3.3. Resulting Uncertainties

The combined uncertainty of the mean current $I_{\mathrm{DUT\_Mean}}$ is obtained from Eq. 4.14 using the experimental standard deviation and the uncertainties associated with the ZVC probe as well as the shunt resistor. This results in $u_c\left(I_{\mathrm{DUT\_Mean}}\right) \approx 27\,\mu A$.

For the current $I_{\mathrm{DUT\_Diff\_Mean}}$, the uncertainty is estimated using the same approach as for the uncertainty of $I_{\mathrm{DUT\_Mean}}$, with another empirical standard uncertainty as Type A component. The individual samples of the current differences were also considered as uncorrelated, as they represent resultant quantities of different evaluations that have been made independently.

The Type B uncertainty components are assumed to apply both the minuend (i.e., the current in crypto mode) and the subtrahend (i.e., the current in plaintext mode) equally prior to subtraction. Thus, the combined uncertainty u_c of $I_{\mathrm{DUT\_Diff\_Mean}}$ results in $u_c\left(I_{\mathrm{DUT\_Diff\_Mean}}\right) \approx 33\,\mu\mathrm{A}$.

The results of the uncertainty estimation are presented in Table 4.19.

Table 4.19.: Measurement Results including Uncertainties.

	Current mean DUT	Current difference of crypto to plaintext
Mean value	8.63 mA	316.2 μA
Combined standard uncertainty $u_c(Y)$	27 μA	33 μA
Relative combined standard uncertainty $u_c(Y)/\lvert Y\rvert$	$3 \cdot 10^{-3}$	$1 \cdot 10^{-1}$

In addition to the mean values of the currents, this table also contains the relative combined measurement uncertainties related to the mean value. The mean current $I_{\text{DUT\_Mean}}$ was determined with a relative uncertainty of about $3 \cdot 10^{-3}$, which is a precise measurement considering the bandwidth of the pulsed current. The current $I_{\text{DUT\_Diff\_Mean}}$ is comparatively lower and could be determined with a relative uncertainty of about $1 \cdot 10^{-1}$, which is still sufficient to determine a reliable statement about the additional power consumption for e.g. a specific crypto algorithm.

4.3.4. Summary of the Application dependent Current Consumption

The measurement of application dependent currents of e.g., a wireless transceiver chip, is challenging due to the small currents and bandwidth. Here, a method has been shown to measure the current accurately. Thereby, an external shunt resistor was selected to exploit the measuring range of the power probe and to achieve a high accuracy.
This approach was used to measure the current consumption of an IOLW transceiver in normal operation (plaintext mode) and encrypted operation (ciphertext mode). Furthermore, the current difference between normal operation and encrypted operation was determined within one experimental measurement. The relevant signal frequencies were determined using variable, FFT-based low-pass filtering. These findings were incorporated into the analysis of the combined measurement uncertainty. Finally, the application dependent current consumption could precisely be measured with a feasible uncertainty.

4.4. Establishing a One-to-one Connection[5]

To establish a one-to-one connection, three distinct security features are recommended:

- Pairing: the process of creating shared secrets.
- Bonding: secure storage of created secrets during pairing for the use in specific connections to establish a trusted device pair.
- Authentication: device authentication to verify identical keys.

Different protocols for authentication and key establishment can be used [120], hence some are selected in the following subsection.

4.4.1. Security during Commissioning of Secrets

The following key establishment techniques are approved by FIPS [89] and the recommendations for cryptographic key generation shall be obeyed [90]. Different options for key exchange are possible such as:

- RSA (Rivest-Shamir-Adleman) is a public-key cryptosystem based on the difficulty of factoring the product of two large prime numbers. RSA is mainly used to securely exchange symmetric keys [121].
- Diffie-Hellman (DH) is a key exchange protocol based on the discrete logarithm problem. DH generates key pairs very fast, but does not directly support encryption, decryption or digital signatures such as RSA [122].
- ECDH key exchange protocol allows both communication partners to establish a shared secret. ECDH is based on DH key exchange protocol using elliptic curve cryptography. The security of ECC is based on the elliptic curve discrete logarithm problem (ECDLP) [123]. The overall performance, which is important in embedded controller design, is higher when compared with e.g. RSA, because of shorter key length for similar security levels [124]. Public keys can be used as static or ephemeral, which are not authenticated and temporary [125].
  - Curve25519 is an elliptic curve using 128-bit security level, offering high performance gains over traditional elliptic curves, and addresses issues such as side channel attacks and poor-quality random-number generators [126].
  - FourQ is a high-performance elliptic curve, which also targets a 128-bit security level, claiming to be between four to five times faster than NIST P-256 curve and two to three times faster than Curve25519 [126, 127].

[5] based on [3]

- Elliptic curve Menezes-Qu-Vanstone (ECMQV) key agreement is an authenticated protocol for key agreement based on the DH [128].
- Certificate-based pairwise key establishment (CPKE) [129].

Before starting general process data exchange or even safe process data exchange (SPDE), the configuration needs to be specified. Therefore, possible configuration levels could be introduced: no security, pre-shared key or out-of-band (OOB) using e.g. NFC, bar codes, QR codes, magnetic codes, SIM-cards, memory-cards, optical codes or others.

The preferred OOB commissioning technology is NFC providing the following advantages:

- Operating only in close proximity to the communication modules generating a higher level of confidentiality.
- Start of commissioning by tapping tag to reader.
- Usage of any commissioning protocol.
- No additional power supply needed.

In the case of key exchange, low visibility makes man-in-the-middle (MITM) attacks unlikely, because of a very low range of about 10 cm [130]. This combination of limited distance, access control in the production area and the ability to switch the NFC signal on a FS-W-Device results in a more secure combination for fast short bursts of sensitive data exchange [131].

4.4.2. Security after Commissioning of the Network Key

Generally, the configuration channel is available if one track is configured in “IOLW-ServiceMode” (pairing state), while the W-Master sends a pairing request to a specific unpaired W-Device as described in [22]. On the basis of the existing pairing mechanism, the secure pairing sequence, presented in Fig. 4.16, is proposed including security features from [132].

In addition to the regular IOLW pairing request, a “CryptoHeader” is introduced as well as a random number to reduce vulnerabilities against replay attacks. The CryptoHeader configuration should consist of the following parameters:

- Security control: consisting of security level and key identifier mode.
- Frame counter.
- Key identifier: consisting of key source and key index.

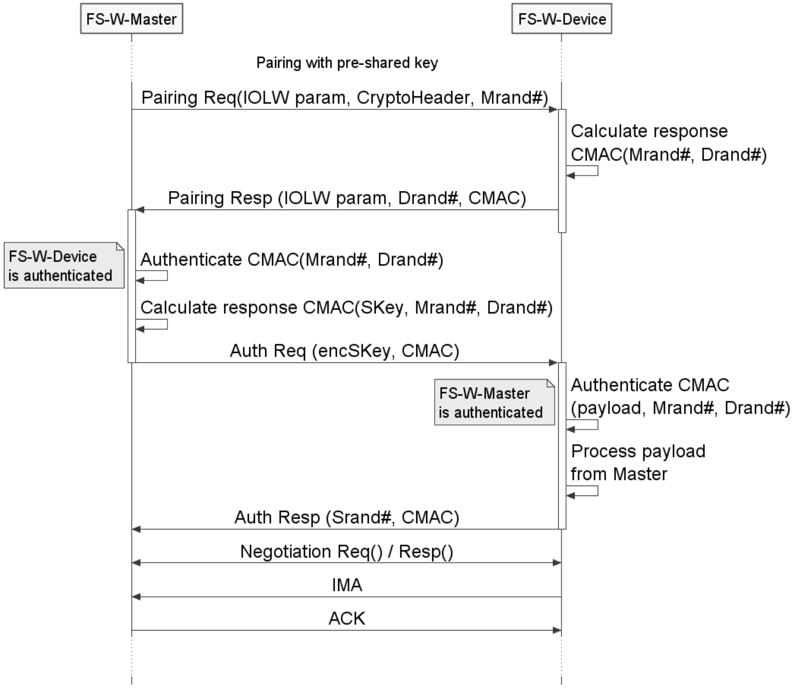


Figure 4.16.: Proposed secure IOLW pairing sequence, which is based on the original IOLW pairing sequence [22] and features taken from [132].

Fig. 4.17 depicts the "CryptoHeader" with the available octets in the pairing sequence of IOLW. Further investigations shall show whether the available length and configuration are sufficient.

4 octets available		
Security Control	Frame Counter	Key Identifier
Security level, key identifier, reserved bits	Each message with unique sequence ID	Key source, key index
1 octets	2 octet	1 octet

Figure 4.17.: Structure of the proposed CryptoHeader.

A key identifier mode is introduced, setting the kind of key (e.g., session or application-dependent) used by a FS-W-Master, FS-W-Device or FS-W-Bridge. The frame counter provides replaying protection and is appended to each message with a unique sequence ID. The key identifier states the key source (e.g. HSM or non-volatile memory (NVM)) and the key index in case there are keys for different usage.
Both communication ends, FS-W-Master and FS-W-Device, shall be authenticated. Therefore, two “numbers only used once” (nonces) as random numbers (Mrand#, Drand#) are exchanged and are included with the IOLW parameters and CryptoHeader in the calculation of the CMAC algorithm [133]. The nonce can be used during CMAC counting as well as initialization vector for the AES algorithm.

If a FS-W-Device has to rejoin or reconnect after connection loss or some other incidence to a FS-W-Master, new nonces need to be created by both communication ends. As nonce, a random number of at least 32-bits shall be used, which must be a non-repeating sequence. A combination of the nonces and the pre-shared key may be used as key derivation function (KDF) for a session key for further application dependent communication, which is described in Section 4.5. This shall especially be used if only one pre-shared root key is held by the FS-W-Master, FS-W-Device, or FS-W-Bridge.

4.5. Cryptographic Algorithms for IOLW Message Exchange[6]

In this section, a suitable cryptographic algorithms including authentication for IOLW message exchange is exemplary implemented as well as measurements of power consumption and timing are presented. Beforehand, the order of authentication and encryption is discussed.

4.5.1. Order of Authentication and Encryption

For data exchange, there are three approaches regarding the order of authentication and encryption [92]:

- Encrypt-then-authenticate: encrypt first the plaintext and then authenticate the ciphertext (see Fig. 4.18).
- Authenticate-then-encrypt: authenticate the plaintext and then encrypt both the plaintext and the MAC (see Fig. 4.19).
- Encrypt-and-authenticate: encrypt and authenticate the plaintext and then combine both results (such as concatenate) (see Fig. 4.20).

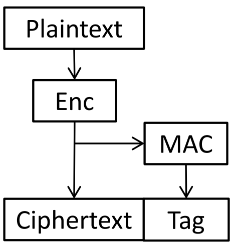


Figure 4.18.: Encrypt-then-authenticate.

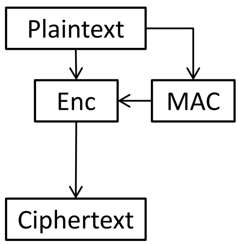


Figure 4.19.: Auth-then-encrypt.

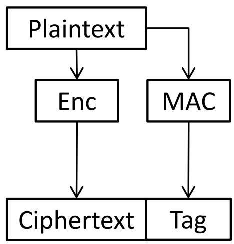


Figure 4.20.: Encrypt-and-authenticate.

Today, there is no simple answer, which approach is most secure. An argument for using less computation power is that bogus messages can be identified if encrypt is used first, because the receiver will first check the MAC and might not need to decrypt (encrypt-then-authenticate). This would for instance make a denial-of-service (DOS) attack a little bit more challenging, but often the communication channel would be saturated instead of the central processing unit (CPU) [92]. For instance, Internet protocol security (IPsec) [134] employs encrypt-then-authenticate.

[6] based on [3]

When using encrypt-and-authenticate, the encryption and authentication process can be processed in parallel, which may increase the performance, but the encryption does not secure the MAC (authenticate-then-encrypt) and vice versa (encrypt-then-authenticate). An example for encrypt-and-authenticate is the secure shell protocol (SSH) being defined in [135].

In the authenticate-first configuration (authenticate-then-encrypt), the ciphertext is only visible for the attacker and the MAC is hidden within. Therefore, it is much harder to attack the MAC value in comparison to the encrypt-first configuration. This configuration is e.g., applied in transport layer security (TLS) version 1.3 [136].

But the configuration applied last, encryption or authenticate, will be exposed to the attacker without further hindrance [92]. The order of authentication and encryption might be a question of philosophy. Furthermore, it might be a question of meaning like the Horton Principle: "You should authenticate what you mean, not what you say" [92, 137].
In general, both configurations shall be applied with enough entropy and security bits.

4.5.2. Exemplary Authenticated and/or Encrypted IOLW Message Exchange

After commissioning, regular communication is established transmitting messages in SSLOT or DSLOT. As only one octet payload is possibly transmitted in SSLOTs and compatibility with IOLW and IO-Link Safety is mandatory, authentication and confidentiality cannot be established for SSLOT data exchange. Thus, only DSLOT transmission is considered.

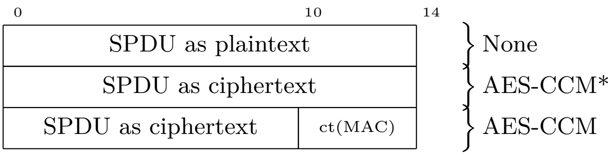
As already mentioned in Section 1.2.2, a single DSLOT transmits up to 14 bytes payload and can be configured with 2 retries having a cycle time of 5 ms. The transmission of one and two DSLOTs equipped with random data are measured in respect of its time duration and power consumption throughout the cryptographic algorithm used.

Since AES-ECB/CBC are not considered "state-of-the-art" block cipher modes, AES-CCM or GCM is recommendable. Here, AES-CCM is considered and implemented for further investigations. The counter with CBC-MAC (CCM) is a generic authenticated encryption block cipher mode, which can be used with any block cipher [107]. Therefore, 128-bit block ciphers, such as AES, are used. AES-CCM combines CBC-MAC with an AES block cipher in CTR mode of operation, whereas any length of message can be encrypted and not only multiples of the block cipher size [138]. AES-CCM is applied in an "authenticate-then-encrypt" manner with CBC-MAC being computed first on the plaintext. Then, the plaintext and the MAC are encrypted. Further details on the implementation are given in [138] and [139].

Exemplary realizations and measurements of security features on CC2650 transceiver chips are shown in [140]. This transceiver was chosen, because it is widely used for IOLW implementations, as demonstrated in [13–15]. In contrast to those measurements, AES-CCM is used for the following measurement series.

The CC2650 AES-CCM driver supports both, classic AES-CCM as defined by NIST SP 800-38C [139] and the AES-CCM* variant used in IEEE 802.15.4 [141]. AES-CCM* allows for unauthenticated encryption using CCM by permitting a message authentication code (MAC) length of zero. It also imposes the requirement that the MAC length be embedded in the nonce used for each message if the MAC length varies within the protocol using AES-CCM* [138]. Different return behaviors for calling the cryptographic operations are possible such as callback, blocking, and polling, which are described in [14]. The return behavior blocking is used due to its simplicity and the fact that no other operation needs to be performed simultaneously. Test vectors from RFC 3610 [107] were used for verification of the parameter for the algorithm used.

Fig. 4.21 depicts the configurations of the SPDU using plaintext, AES-CCM* (14 bytes decrypted), and AES-CCM (ten bytes decrypted and four bytes MAC).



Note: For AES-CCM, the MAC is encrypted within the ciphertext (ct).

Figure 4.21.: One DSLOT message with confidential and/or authenticated data.

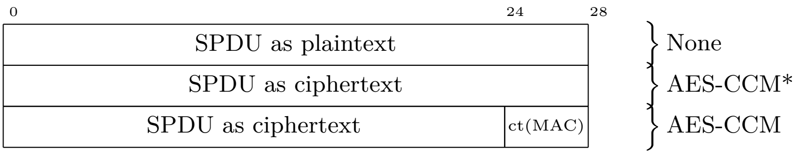
Table 4.20 shows the time duration, average current consumption, and relative battery lifetime reduction of the plaintext and cryptographic algorithms. The measurement setup and calculations are discussed in Section 4.3. The time difference for AES-CCM* is around 69 μs higher or for AES-CCM operation 72 μs compared to plaintext, which has no influence on the timing of IOLW operation for downlink or uplink. The average current consumption is at around 8.65 mA in both cases, respectively, the average current consumption of plaintext is slightly lower at 8.61 mA.

The relative battery lifetime reduction can be calculated using the average current measured over 10 ms (i.e., six wireless cycles) with AES-CCM or AES-CCM* compared to the plaintext average current consumption. Thus, these cryptographic algorithms have no significant impact on battery lifetime, as the relative battery lifetime reduction is 0.46 %.

Table 4.20.: Measured values of suitable cryptographic algorithms with one DSLOT for IOLW.

Configuration [14 octets]	Time Duration [μs]	Average Current [mA]	Relative Battery Lifetime Reduction [%]
plaintext	0.5	8.61	-
confidential using AES-CCM*	69.6	8.65	0.46
authenticated & confidential using AES-CCM	72.9	8.65	0.46

For two DSLOTs with 28 bytes in 10 ms including 2 retries for each DSLOT, the package configuration and the power consumption as well as the time duration are presented in Fig. 4.22.



Note: For AES-CCM, the MAC is encrypted within the ciphertext (ct).

Figure 4.22.: Messages of two DSLOTs with confidential and/or authenticated data.

In Table 4.21, the time duration and average current consumption of the plaintext and cryptographic algorithms using two DSLOTs are presented. Compared with processing only one single DSLOT operating the cryptographic accelerator of the wireless microcontroller unit (MCU), there is no significant increase in time or current consumption.

Table 4.21.: Measured values of suitable cryptographic algorithms with two DSLOTs for IOLW.

Configuration [28 octets]	Time Duration [μs]	Average Current [mA]	Relative Battery Lifetime Reduction [%]
plaintext	0.5	8.63	-
confidential using AES-CCM*	70.3	8.65	0.46
authenticated & confidential using AES-CCM	74.0	8.65	0.46

The measured values for one DSLOT and two DSLOTs payload length show that energy consumption and timing are feasible for real-time applications using a generic authenticated encryption block cipher mode to provide confidentiality and through CBC-MAC message integrity and authentication. The following Chapter 5 clarifies that because of the black channel principle only the layer above the IOLW physical and data link layer is adjusted in this contribution regarding security-for-safety. Furthermore, the data exchange is focused on and presented as prototype implementation in Chapter 6, because of a lack of hardware cryptographic accelerator support for asymmetric algorithms such as ECC for the initial connection negotiation of the IO-Link Wireless Device (IOLWD). Testing a software implementation of an asymmetric algorithms (mbedTLS) for the initial connection negotiation being applied on the IOLWD showed that the memory of the transceiver chip (CC2650) is not sufficient.

CHAPTER 5

Resulting Safety Requirements for IO-Link Wireless Safety

This chapter describes an enhancement of IOLW with an additional safety communication layer employing the black channel principle to fulfill safety requirements with respect to IEC 61784-3 [29]. An extended channel model based on uniformly distributed segments (UDS) superimposed with the BSC is applied to simplify the REP calculation, to detect additional error patterns (see 1.2.6), and to consider BSC-preserved cryptographic algorithms [40]. Also, the REP with respect to the underlying security layer as well as the PFH are quantified.

Various safety-related communication protocols have been devised for factory automation in Chapter 2. But only a few solutions offer the option to integrate smart and simple sensors and actuators in safety-related applications on the shop-floor. One option as already mentioned is IOLS as the failsafe extension of IO-Link satisfying the requirements of [29] for functional safety fieldbuses. To realize an easier assembly with wired and wireless combinations, IOLW shall be extended with a safety and security layer, abbreviated as IO-Link Wireless Safety (IOLWS) with a similar approach as for IOLS [30]. In addition, the current discussion on the relationship between safety and security shall be considered, e.g., that a maximum BEP of 0.5 shall be taken into account for future-proofed safety protocols [40, 95]. Until now, no other wireless protocol on the market has used this method and consideration.

Therefore, this Chapter describes the safety requirements for IOLWS necessary to receive a positive concept evaluation for its usage within safety-related applications.

5.1. General Requirements

A future IOLWS specification shall describe a conceptual model for functional safe communication using the IOLW communication stack. Therefore, the black channel concept is employed with the prerequisite of a one-to-one connection between W-Master and W-Device (IOL specific) as well as with the necessary infrastructure for parameterization of the safety communication layer and the technology of a functional safety wireless device/bridge (FS-W-Device/Bridge) using the IODD safety extensions and dedicated tools. The design of safety communication contains according to [25] and [29] e.g., the following:

- Functional safety management (FSM)
- Failure mode and effects analysis (FMEA)
- Residual error considerations and calculations

The main focus of the above mentioned safety evaluation are the residual error considerations and calculations taking into account the implemented security layer and BSC-preserving algorithms. Here, functional safety management (FSM) and FMEA are only partially discussed, because these parts are more product specific.

For consideration of a pre-certification of the protocol design, two different configurations are considered:

I: Regular SPDU, which is illustrated in Fig. 5.2 with optional MAC.

II: Cascading two SPDUs (Fig. 5.3), which results in sending the identical safety information twice and may result in an increased cycle time.

5.2. Strategy to fulfill Safety Requirements

Here, a conceptual model for the transmission of safety IO data on top of IO-Link Wireless stack as black channel is provided. The machinery directive 2006/42/EC [142] states: “Essential health and safety requirements for machinery to ensure that the safety communication for use in the machinery complies with the requirements before placing it on the market or putting it into service.”

Therefore, a positive assessment report and a corresponding certificate from an official assessment body is beneficial. Figure 5.1 illustrates the potential systematic and stochastic errors to be considered for the cyclic safety communication. Systematic and human errors are considered within:

- safety measures,
- operational modes,
- protocol design (unified modeling language (UML)), and
- specification.

And stochastic errors necessary to get acceptance for are based on:

- proper generated polynomials,
- PFH monitor,
- RER calculations,
- timeliness, and
- authenticity.

Within this chapter, the mentioned stochastic errors are quantified and the possible systematic and human errors are partially contemplated since this might rather be part of further working groups (here: experts of companies in the field of interest) and not part of scientific organizations.

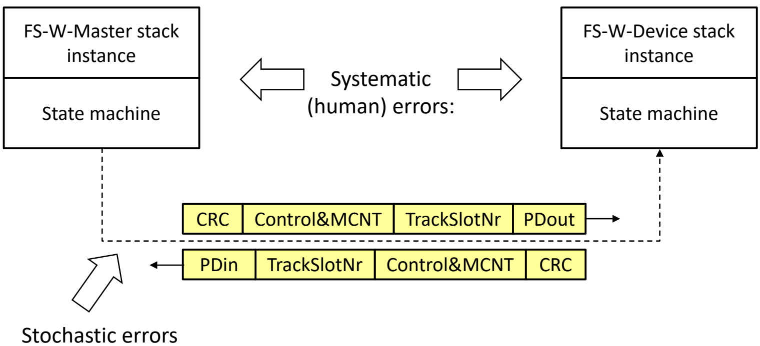


Figure 5.1.: Systematic and stochastic errors based on [30].

5.3. Safety Process Data Unit (SPDU)

The design of the SPDU follows IOLS and [29] with the concept of explicit transmission of the safety measures for timeliness and authenticity and not the implicit transmission via inclusion in the overall CRC signature calculation [29]. Furthermore, the point-to-point connection is guaranteed by using a cryptographic algorithm with sufficient entropy (Section 4.1) as well as adjustment of port number to track/slot number and employing an IOLWS CRC. In general, a MAC is employed to detect manipulations (guarantees integrity and authentication of the message) and a CRC to detect (stochastical) errors (data integrity). A MAC will be implemented in the SeCL and a CRC in the SCL, respectively. With respect to the safety requirements, the timeliness measure is represented by a 5-bit counter within the SPDU. With respect to authenticity next to the MAC, the FS-W-Master track/slot number is included in cyclic checking due to requested usage of unchanged SDCI implementations (black channel). However, complete authenticity checking is performed during commissioning and at start-up. The design follows the "de-energize to trip principle" [30], where in case of a timeout, a CRC or MAC error, or a counter error, or a track/slot number error, the associated qualifier bit will be set to enter a safe state. It will be only released after an explicit operator acknowledgment or the FS-W-Master. In the case of a CRC or MAC error, a warm start shall be possible.

5.3.1. SPDU using one DSLOT

Fig. 5.2 shows the structure of the FS-W-Master and FS-W-Device SPDUs excluding standard IO data. The concept of explicit transmission of the safety measures for timeliness and authenticity according to IEC 61784-3 [29] is obeyed. A MAC is used across the FS-W-Output data, track and slot number (TrackSlotNr), the control and counting, and the CRC signature to guarantee message integrity and authenticity using a secret only known to both communication ends. The track and slot number (TrackSlotNr) is used as an additional measure for identification. As used in IOLS, a counter value is communicated in combination with the local watchdog timer to achieve timeliness. The feedback signal from the FS-W-Device employs the inverted counter value for the timeliness check to prevent loop-back errors (e.g., as in [30]).

For this configuration, it is also possible to communicate non-safety wireless process data (W-PDout) from the FS-W-Master using one track per FS-W-Device. Here, the functional safety wireless process data output (FS-W-PDout) length is limited to 24 octets. For the input data, it is also feasible to separate the six octets of the functional safety wireless process data input (FS-W-PDin) and respectively non-safety wireless process data (W-PDin). In this case, the W-PDin data are not included in the calculation of the MAC and CRC.

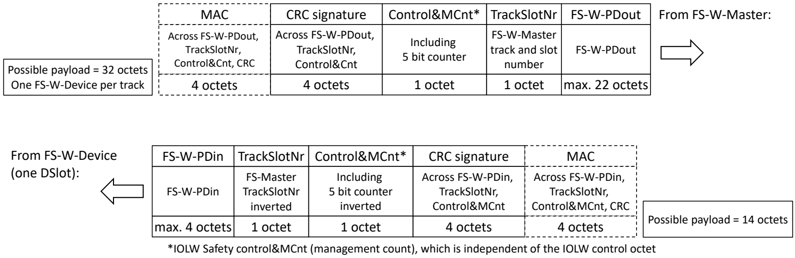


Figure 5.2.: IOLW Safety PDUs with one DSLOT and cycle time of 5 ms (2 retries), fullpage view in Appendix D.2.

5.3.2. SPDU using two DSLOTs

Fig. 5.3 presents the structure of the FS-W-Master and FS-W-Device SPDUs if a cycle time of 10 ms is configured. For this configuration, 64 octets are available for the FS-W-Master SPDU if only one FS-W-Device with DSLOT per track is connected. If four FS-W-Devices with DSLOT per track are connected, 16 octets payload are feasible resulting in maximum of eight octets FS-W-PDout data. Depending on the FS-W-PDout data length, the length of the CRC signature and MAC shall be adjusted. For FS-W-PDin/FS-W-PDout data of up to three octets a CRC signature of two octets (16 bit CRC) and if the FS-PDin/FS-PDout data is up to 25 octets, a CRC signature shall be four octets (32-bit CRC), which is employed in IOLS. Thus, also a larger MAC may be used.

The FS-W-PDin data length is max. 20 octets depending again on the length of the CRC and MAC of the SPDU. W-PDout and W-PDin data may be added to the payload. The parameterization within the domain of safety for machinery shall be configurable in a “Dedicated Tool” per FS-W-Device or FS-W-Bridge.

5.3.3. Length Limitations of IOLW Safety

IOLW limits the application dependent payload to be 32 octets as maximum. Since IOLWS is designed to be an extension of IOLW in similar manner as IOLS to IOL, the IOLW Safety PDU could in maximum transfer three DSLOTs within 15 ms resulting in 26 octets FS-W-PDin from a FS-W-Device to a FS-W-Master. From a FS-W-Master to a FS-W-Device 96 octets are possibe, which results in 24 octets/FS-W-Device if four FS-W-Devices share slots equally per track. Handling of timing adjustments

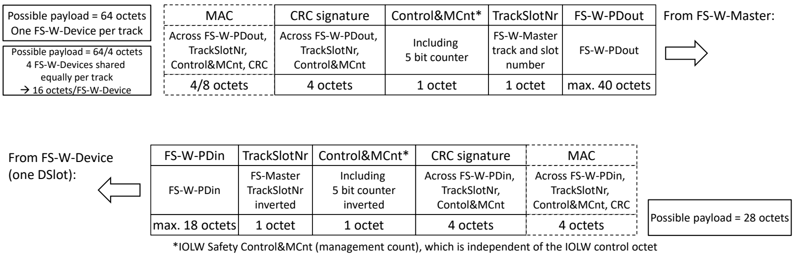


Figure 5.3.: IOLW Safety PDU with two DSLOTs and cycle time of 10 ms (2 retries for each DSLOT package), fullpage view in Appendix D.3.

between IOLS and IOLWS to find a configuration of minimum jitter time might be a challenge and will only add 3 octets additionally. Within the scope of this thesis, only one and two DSLOTs are considered.

5.4. Status/Control and Sequence Counter

Similar to IOLS [30], one octet shall be used in both transmission directions for the protocol flow of IOLWS data. Therefore, Table 5.1 illustrates the signals to control the protocol layer of a FS-W-Device and a counter value for the timeliness check together with a local watchdog timer being configurable from the user application.

Table 5.1.: Control and counting bits CB0...CB7 based on [30].

CB7, CB6, CB5, CB4, CB3	CB2	CB1	CB0
Sequence counter bit 4, bit 3, bit 2, bit 1, bit 0	Reserved (“0”)	Activate safe state	Channel fault acknowledge request (indication)
MCount4 to MCount0	-	SetSD	ChFAckReq

The feedback of the protocol layer of an FS-W-Device and the inverted counter for the timeliness check is presented in Table 5.2. The safe state is activated using `CB1/SB2` controlled by the application. `DTimeout` of the FS-W-Device reports a timeout of its SCL via Status&DCnt byte and `DCommErr` of the FS-W-Device reports a CRC error (incl. counter and TrackSlotNr error) by its SCL via the Status&DCnt byte.

Table 5.2.: Status and counting mirror based on [30].

SB7, SB6, SB5, SB4, SB3	SB2	SB1	SB0
Sequence counter bit 4, bit 3, bit 2, bit 1, bit 0 inverted	Safe state activated	Comm. error CRC or counter incorrect	Comm. fault timeout
DCount4_i to DCount0_i	SDset	DCommErr	DTimeout

Note: "Comm." - Communication.

5.5. Timings

IOLW times and safety times are illustrated in Fig. 5.4 with the IOLW communication channel, treated here as a black channel, transmitting SPDUs within the "MasterCycleTime" from the FS-W-Master to the FS-W-Device and vice versa. The same SPDU, e.g., with `MCount = 3`, may be sent several times before the SCL starts the next SCL cycle with `MCount = 4`. Meanwhile, the FS-W-Master received the response SPDU from the FS-W-Device with `DCount_i = 28`.

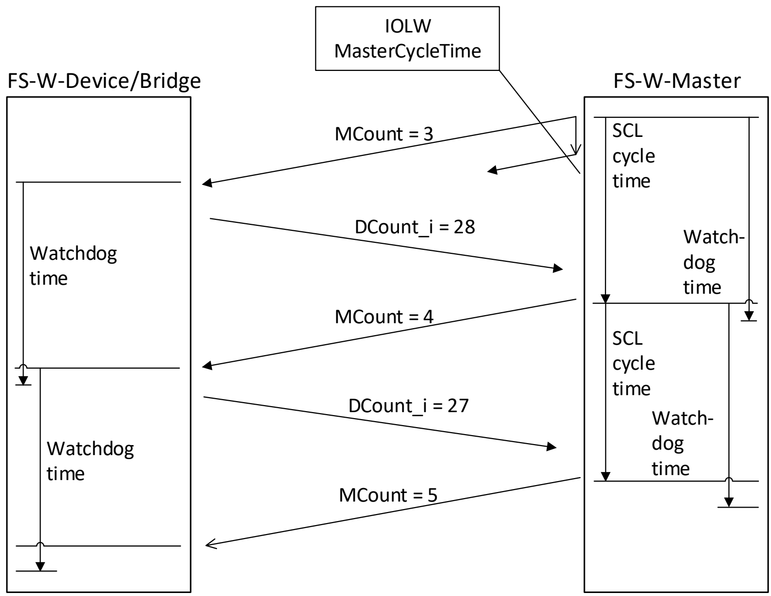


Figure 5.4.: Monitoring of the SCL cycle time based on [30].

Different timing constraints exist (similar to IOLS [30]), such as:

- Synchronization: `MCount = 0` is used at each start-up and after an FS-W-Master timeout.
- SCL cycle time: comprises the transmission time of the FS-W-Master SPDU, the FS-W-Device processing time, the transmission time of the FS-W-Device response SPDU, and the FS-W-Master processing time until the next FS-W-Master SPDU (see Fig. 5.4).
- Watchdog time: monitors the entire SCL cycle time.
- Counter check: counter values are included in the cyclic CRC signature and MAC calculation. An incorrect CRC signature or MAC (with watchdog timer) value leads immediately to a safe state. Counter check is also used for discarding outdated SPDUs.
- Repetition: in case of detected incorrect CRC signatures or MACs, repetition is detected by means of timing measure.
- PFH-Monitor: as presented in Table 5.2, the FS-W-Master holds the information of both SPDU transmissions from and to the FS-W-Device. Therefore, the FS-W-Master monitors the average rate of a dangerous failure within a given time frame (PFH-Monitoring time) [30,44].

5.6. CRC Signature Considerations

Designing the CRC mechanism and calculating the REP (or RER) requires various parameters and assumptions:

- Usage of security algorithms being BSC-preservative and viewed as part of the black channel.
- No multi-drop or multi-channel is allowed in IOLW
- Explicit transmission of safety measures as opposed to implicit transmission (see IEC 61784-3:2021 [29]).
- The transmission rate of SPDUs is assumed to be a maximum of 200 sampled SPDUs per second (assuming 5 ms transmission time including two retries). Here, a PFH-Monitor is used. Therefore, the transmission rate is not relevant as long as the transmission rate is below 200/s. If the transmission rate is higher and the channel is erroneous, the communication will not work.
- The monitoring times for errors in SPDUs are 10 h in case of 32-bit CRC signatures (CRC 32). Any detected CRC error within the SCL triggers the corresponding safety function resulting in a safe state. During the monitoring time only one nuisance trip is permitted and maintenance is required.

- The generator polynomials in use shall be proven to be proper within the SPDU range (IOLW uses `0x4C11DB7` and IOLWS `0x1EDC6F41`).
- The seed value to be used for the CRC signature calculation is “1”.
- In case the result of the CRC signature leads to a “0”, a “1” shall be sent and evaluated.
- The assumed BEP for calculations applying a SeCL is 0.5 and without SeCL 10^{-2}.

Calculations under the following conditions have shown its validity:

- In case of one DSLOT message (SPDU length = 14 octets), four octets of process data, one octet of `TrackSlotNr` and one octet of `Control&MCnt` are “secured” by the proper CRC 32 polynomial (`0x1EDC6F41`).
- Or using two DSLOT messages (SPDU length = 28 octets), 18 octets of process data, one octet of `TrackSlotNr` and one octet of `Control&MCnt` are “secured” by the proper CRC 32 polynomial (`0x1EDC6F41`).

5.7. Measures for Safety Requirements

According to the [25] series, any electrical, electronic or programmable electronic system performing safety-related functions must be developed under functional safety management to reduce the risks to people, equipment or the environment to an acceptable level. The required risk reduction is measured by the SIL scaled with four steps having necessary measures and values for key factors assigned. The required SIL is determined by the risk analysis as the first step of the validation and verification process, which describes the entire safety life cycle. Further aspects are, for example, the definition of the SRS, the system, hardware and software design, test concepts for each step, verification through testing and finally the validation of the safety system against the SRS.

The corresponding standard [29] contains requirements that must be met for the exchange of safety-related data in a distributed network. Based on the black channel principle as defined in [25], no safety validation of the communication channel used is necessary when appropriate safety measures are applied to the SCL and the FSCP. This is advantageous for wireless connections over time-varying and frequency-selective radio channels as the wireless channel can only be described stochastically. The standard [29] requires that the sum of probabilities of undetectable errors contributed by communication remains below one percent of the accepted probability of a PFH of the corresponding target SIL. To comply with [29], communication errors related to repetition, deletion, insertion, incorrect sequence, corruption, delay, masquerade and incorrect addressing have to be considered. Typical defenses against these communication errors are counter/inverted counter, timeout with receipt, time expectation, communication authenticity, receipt, data integrity and e.g., redundancy with cross-check. Furthermore, models are introduced to quantify values for error rates in the domain of authenticity, timeliness, masquerade and data integrity resulting in the total RER (λ_{SC}) for the safety channel.

5.8. Effectiveness of Safety Measures

Table 5.3 shows the communication errors to be considered and the chosen safety and security measures applied to IOLWS.

Table 5.3.: Communication errors, safety and security-for-safety measures based on [30, p. 66] and [29].

Communication error	Protocol safety measures					Protocol security-for-safety measures	
	Counter/inverted counter	Timeout with receipt	Authenticity (Track/Slot number and inverted track/slot number)	Cyclic redundancy check (CRC)	Redundancy with cross checking (only for cascading SPUs)	Encryption root key to create session key	Message authentication code (MAC)
Data corruption				X	X	X	X
Unintended repetition	X	X					
Incorrect sequence	X						
Packet loss	X	X					
Unacceptable delay		X					
Packet/data insertion	X		X				X
Masquerade	X	X	X	X		X	X
Wrong addressing			X				X
Loop-back of message	X		X				X

All communication errors must be detectable by at least one safety or security measure. Most of the communication errors are detectable applying safety measures such as the counter/inverted counter, timeout with receipt, and the usage of the track/slot number. Data corruption is detectable by using a suitable CRC for data integrity (see 5.10.4.2).

To guarantee the point-to-point connection between a FS-W-Master and a FS-W-Device (authenticity) and the integrity of each message, the implemented security measure of the MAC is applied, which detects data corruption, packet/data insertion, masquerade, wrong addressing, and loopback of messages. Furthermore, within the IOLWS communication path between FS-W-Master and FS-W-Bridge/Device, no storing element is allowed. Therefore, a 5-bit counter is sufficient as a safety measure.

Note that unintended repetition may result from an error, fault or interference while messages are repeated. Possible countermeasures to prohibit this behavior are transferring data cyclically within the black channel. The proposed "message send and receive concept" of IOLWS allows the implementation of a simple watchdog timer and message receipt safety measure concept corresponding to the de-energize to trip principle.

5.9. Protocol Phases considered within SCL

According to IEC 61784-3:2021 [29] principle protocol phases shall be considered for the design, such as:

- initialization,
- setup or change,
- operation,
- restart after transition from fault,
- warm start after transition from fault, and
- shutdown.

Fig. 5.5 illustrates the protocol phases and its principle access dependencies, which will be considered in the prototype implementation of Chapter 6.

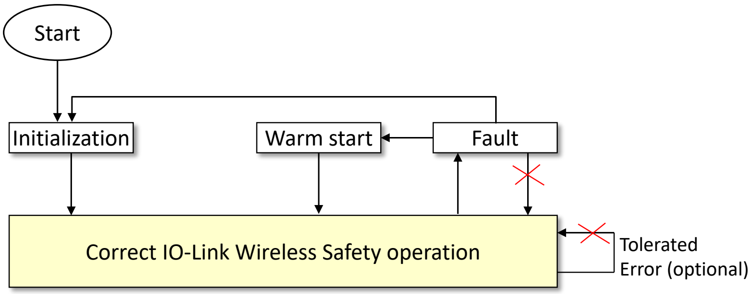


Figure 5.5.: Considered protocol phases based on [30].

5.10. Residual Error Probability Considerations

In the following, REP and RER for authenticity, timeliness, masquerade and data integrity are determined for a regular SPDU as well as for a cascaded SPDU (explained in Section 5.1).

5.10.1. Authenticity

To guarantee authenticity, only correctly addressed messages from authenticated sources should be accepted. In the functional safety domain, this could be achieved by using connection-IDs as authentication-code (A-code) transmitted with every data package. The RER for authenticity errors is calculated using [29] as follows:

$$RR_A = RP_I \cdot 2^{-LA} \cdot R_A \cdot RP_{FSCP\_A}, \tag{5.1}$$

where: RR_A : Residual error rate for authenticity,
RR_I : Residual error probability for data integrity,
LA : Bit length of the connection's authenticity code,
R_A : Rate for misrouted SPDUs,
RR_{FSCP_A} : Additional residual error probability of FSCP-specific measures.

But since the A-code is explicitly secured by integrity measures and the fact that the rate of misrouted messages shall not exceed the message rate of the system (v), the value for the RER for authenticity errors ($\mathrm{RR_A}$) may be assumed with [29]:

$$RR_A = 0. \tag{5.2}$$

Here, also the point-to-point connection is applied being established by the security layer.

5.10.2. Timeliness

Communication errors, like delay or deletion, should be detected to achieve the generic safety property of timeliness. Suitable methods are watchdogs, timestamps or counter values identifying the message with the timeliness-code (T-code). The contribution to λ_{SC} caused by timeliness errors is the RER for timeliness ($\mathrm{RR_T}$) is

$$RR_T = 2^{-LT} \cdot w \cdot R_T \cdot RP_{FCSP\_T}, \tag{5.3}$$

where:
RR_T : Residual error rate for timeliness,
LT : Bit length of the T-code,
w : Number of accepted sequence numbers or timestamps for a received SPDU,
R_T : Rate for non-up-to-date SPDUs,
RR_{FSCP_T} : Additional residual error probability of FSCP-specific measures.

according to [29]. The value of RR_T can be assumed to be “0” if no message storing element is involved, because the rate of occurrence of incorrect sequence SPDUs (R_T) could be assumed to “0”.

$$RR_T = 0. \tag{5.4}$$

5.10.3. Masquerade

If a non-safety message imitates a safety message and all other safety requirements for authenticity, timeliness and integrity are fulfilled by coincidence or accident. Thus, the RER for masquerade ($\mathrm{RR_M}$) will always be very small and is defined as [29]:

$$\begin{aligned} RR_M &= 2^{-LA} \cdot 2^{-LT} \cdot w \cdot 2^{-r} \cdot RP_u \cdot 2^{-LR} \cdot R_M, \\ RR_M &= 2^{-8} \cdot 2^{-5} \cdot w \cdot 2^{-32} \cdot 1 \cdot 2^{-0} \cdot \frac{10^{-3}}{\mathrm{h}}, \\ &\approx 2.8 \cdot \frac{10^{-17}}{\mathrm{h}}, \end{aligned} \tag{5.5}$$

where: RR_M : Residual error rate for timeliness,
LA : Bit length of the connection authentication,
LT : Bit length of the sequence number,
w : Number of accepted sequence numbers or timestamps for a received SPDUs,
r : Bit length of the CRC signature (if two CRC methods with different generator polynomials are used, r is the sum of the two-bit lengths),
RP_U : Residual error probability for the remaining fields that characterize a correctly formatted SPDU,
LR : Length of the repeated portion of the SPDU (in the case of redundancy with cross-matching),
R_M : Rate of occurrence for masqueraded SPDUs, which is set to 10^{-3}/h for every device by default (assumption).

If two SPDUs are cascaded the following RER for masquerade results in:

$$\begin{aligned} RR_M &= 2^{-8\cdot 2} \cdot 2^{-5\cdot 2} \cdot 1 \cdot 2^{-32\cdot 2} \cdot 1 \cdot 2^{-0} \cdot \frac{10^{-3}}{\mathrm{h}}, \\ &\approx 8.1 \cdot \frac{10^{-31}}{\mathrm{h}}. \end{aligned} \tag{5.6}$$

5.10.4. Data Integrity

Data integrity is the basic requirement for any safe decision in communication; therefore, it is necessary to ensure that corruption is detected with a high and determined probability by the SCL. In general, auxiliary redundancy must be added to double check the integrity of the data. Most popular are error-detecting codes such as CRC, which are also proposed by the standard. For the estimation of the RER for data integrity ($\mathrm{RR_I}$), the probability for an error in one bit must be assumed together with the likelihood, that errors could be detected by the selected safety measure.

5.10.4.1. Bit Error Probability

Since the black channel principle, according to [29], is based on the BSC model, the probability for a bit error is equal for the transmission of a digital one or digital zero at every position and could be assumed to be

$$0 \leq \mathrm{BEP} \leq 0.5. \tag{5.7}$$

Since there would be no communication possible with a higher error probability, the standard specifies a BEP of 10^{-2} to be considered unless a prove for a lower BEP is given. Within this field of study there is an ongoing discussion about the combination of safety and security measures within the scientific community. This is caused by the fact that some cryptographic algorithms change the probability distribution so that the assumed BSC is not preserved [40].

5.10.4.2. Properness of CRC Generator Polynomials

The likelihood that a CRC calculation for an erroneous message has the same result as the calculation for the original message is a degree for the properness of the CRC generator polynomial. This probability should explicitly be calculated for every possible data length of the FSCP. If the value never exceeds the so-called conservative limit of 2^{-r}, where r is the CRC-bit length, the generator polynomial is called proper and the REP follows the theoretical calculation results.

Hamming distance and properness for all required data lengths are key characteristics to select a particular generator polynomial. Double, triple and any odd number of errors can be detected [143] if the generator polynomial:

$$g(x) = p(x) \cdot (1 + x) \tag{5.8}$$

is used, where p(x) is a primitive polynomial of degree $(r - 1)$. Thus, the maximum total block length is $2^{(r-1)} - 1$. Then, the REP for the approved data length is 2^{-r}. It is be prohibited that the CRC generator polynomial used in the underlying transmission systems, which is in this case IOLW (using the CRC32 polynomial $0x4C11DB7$), matches the CRC generator polynomial employed in the safety layer.

Table 5.4.: CRC generator polynomials for SDCI-FS based on [144].

CRC32 Polynomial	Data length (bits)	Hamming distance	Properness	Remark
0x1EDC6F41 ("normal" representation of Castagnoli CRC polynomial)	≤177 ≤5243	≥8 ≥6	≤256 octets	Suitable for funct. safety with security layer in black channel

Note: High order bit is omitted in "Normal" representation.

This CRC32 is applicable for cyclic process data exchange (PDE) with a total SPDU length of up to 28 octets (two DSLOTs) including 6 to 10 octets of safety code and 18 to 22 octets safety process data, the transfer of up to 24 octets of FSP parameters at start-up or restart, and the transfer and data integrity of the complete FSP parameter set.

For 32-bit CRC polynomials, it is not realistically possible to determine its REP by calculating all possible combinations. Also, the use of approximate calculations has been proven to be too imprecise or even incor-

rect [145]. In addition, all data lengths used must be considered depending on the assumed bit error probabilities.
The evaluation of the CRC polynomial is realized using a high performance computing infrastructure with the help of a brute force approach [146]. For IOLWS, the Castagnoli CRC polynomial (`0x1EDC6F41`) is used and applied on different message lengths. Therefore, the Hamming weights of the CRC polynomial are calculated with the help of the McWilliams Identity [147] with the REP for individual data lengths being dependent on the BEP using the determined weights. The stored matrix of the different Hamming weights and data lengths are used to calculate the residual error probabilities according to the BEP (in Matlab). The procedure is validated using IEC 61784-3 [29] with the CRC reference polynomial `0x1F922815`.

Fig. 5.6 depicts the REP for message length between 80 bits (10 octets) and 480 bits (60 octets) presenting one or two DSLOTs as SPDU length. The REP is less than 2^{-32} for BEPs at a length of 14 and even up to 28 octets. If a cryptographic algorithm, which must fulfill the requirements of BSC, is used within the black channel (one and two DSLOTs) a required BEP of up to 0.5 must be achieved [40]. Here, the REP stays below 10^{-09} for a BEP of 0.5.

Further information regarding the CRC generator polynomial including the tools used for implementation and the residual error probability values are stated in Appendix B.

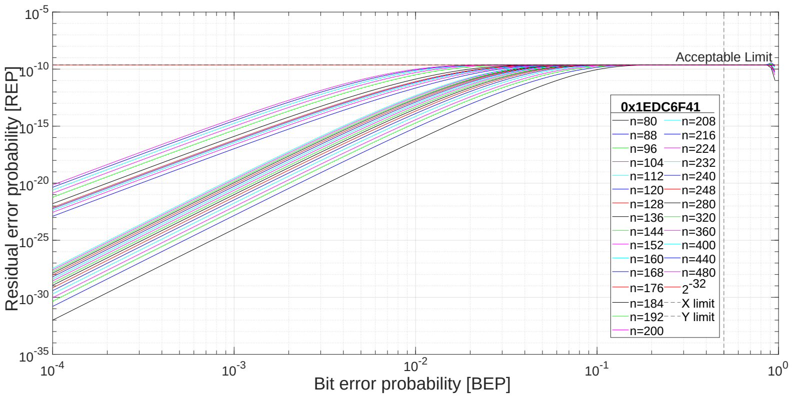


Figure 5.6.: CRC32 generator polynomial for n = 80 to n = 480.

5.10.4.3. Residual Error Rates

The REP for data integrity (RP_I) is given by the REP of the proper CRC with the specified BEP and the maximum message rate per hour (v). The equation for a regular SPDU

$$\begin{aligned} RR_I &= RP_I \cdot v \cdot RP_{FSCP\_I}, \\ &= 2^{-32} \cdot \frac{10^{-1}}{\mathrm{h}} \cdot RP_{FSCP\_I}, \\ &\approx 2.3 \cdot \frac{10^{-11}}{\mathrm{h}} \cdot RP_{FSCP\_I}, \end{aligned} \tag{5.9}$$

with the REP of additional safety measures for data integrity (RP_{FSCP_I}) is the last part to quantify the RER for the entire safety communication layer per hour (λ_{SCL}) as

$$\begin{aligned} \lambda_{SCL} &= (RR_T + RR_A + RR_M + RR_I) \cdot m, \\ \lambda_{SCL}(CRC32\,@\,0.5) &\approx \left(0 + 0 + 2.3 \cdot \frac{10^{-11}}{\mathrm{h}} + 2.8 \cdot \frac{10^{-17}}{\mathrm{h}} \cdot 1\right), \\ \lambda_{SCL}(CRC32\,@\,0.5) &\approx 2.3 \cdot \frac{10^{-11}}{\mathrm{h}}, \end{aligned} \tag{5.10}$$

with the maximum number of logical connections allowed (m) for the safety function.

If two SPDUs are cascaded the following residual error rate is calculated:

$$\begin{aligned} RR_{I2} &\approx 2^{-32 \cdot 2} \cdot \frac{7.2 \cdot 10^5}{\mathrm{h}} \cdot RP_{FSCP\_I2}, \\ &\approx 3.9 \cdot \frac{10^{-14}}{\mathrm{h}} \cdot RP_{FSCP\_I2}, \end{aligned} \tag{5.11}$$

and for the calculation of the total residual error rate of IOLWS communication as in [29, p. 41]:

$$\begin{aligned} \lambda_{SCL2}(CRC32\,@\,0.5) &\approx \left(0 + 0 + 3.9 \cdot \frac{10^{-14}}{\mathrm{h}} + 8.1 \cdot \frac{10^{-31}}{\mathrm{h}} \cdot 1\right), \\ \lambda_{SCL2}(CRC32\,@\,0.5) &\approx 3.9 \cdot \frac{10^{-14}}{\mathrm{h}}. \end{aligned} \tag{5.12}$$

5.11. Summary of the Safety Requirements of IO-Link Wireless Safety

Within this safety requirement specification, the concept of IOLWS is consistent with the applicable requirements presented and viewed by a certification organization see Appendix C. The safety concept for IOLWS meets the relevant requirements according to the functional safety standards IEC 61508:2010 (SIL 3), IEC 62061:2021 (Maximum SIL 3), EN ISO 13849-1:2015 (Category 4, PL e) and the industrial safety communication standard IEC 61784-3:2021.

The total residual error rate for regular SPDU and cascading two SPDUs is summarized in the following Table 5.5, whereas the first option is applicable if a PFH-Monitor is used and the second option if this is not possible because of patent rights of the PFH-monitor [44]. Both options are applicable for SIL 4.

Table 5.5.: Summary Total Residual Error Rate with SIL Classification.

#	SPDU config	Total Residual Error Rate λ_{SCL}	Applicable up to	Note
I	Regular SPDU	$\lambda_{SC}(PFH = 10h) \approx 2.3 \cdot \frac{10^{-11}}{h}$ $\lambda_{SC}(PFH = 1h) \approx 2.3 \cdot \frac{10^{-10}}{h}$	SIL 4*	If PFH-Monitor is used and $RR_T = 0$ and $RR_A = 0$
II	Cascading two SPDUs	$\lambda_{SC2} \approx 3.9 \cdot \frac{10^{-14}}{h}$	SIL 4*	If PFH-Monitor is not used and RR_{T2} and $RR_{A2} = 0$

*Note: Quantitative requirement.

Furthermore, the review of detailed design and the planning of verification and validation activities are partially necessary to demonstrate that safety components implementing IO-Link Wireless Safety fulfills the aforementioned standards. In case of the used standards for IOLWS (see Appendix C) only an additional safety certification of the software stack implementation is necessary, because of the used black channel principle. Of course, this is not part of this dissertation, but is necessary to offer a functional safety protocol as product.

CHAPTER 6

Prototype Implementation of the IO-Link Wireless Safety Protocol Proposal[1]

6.1. System Overview

In the following, an implementation of the IOLWS protocol proposal including its safe configuration of a FS-W-Master and a FS-W-Bridge/ Device with their authentication under stringent safety requirements is described. The implemented IOLWS protocol includes cyclic, safe process data exchange and its authentication, integrity, order, and timeliness of the process data.

The developed IOLWS library is very closely tied on the IOLS library [148, 149] to enable easy integration and combination of wired and wireless safety masters and devices. Within the consideration of the SRS (see Chapter 5), a black channel between FS-W-Device and FS-W-Master is established, whereas the black channel of the wired IOLS between FS-Master and FS-Device is in this case not examined. Fig. 6.1 presents the two concatenated black channels in the wired and wireless domain. Here, a FS-W-Bridge is used to map IOLS data to IOLWS and vice versa. Therefore, the FS-W-Bridge consists of a (wired) FS-Master as well as a (wireless) FS-W-Device. The FS-W-Master exchanges process data with a safety PLC using the SMI.

[1] based on [30, 148, 149]

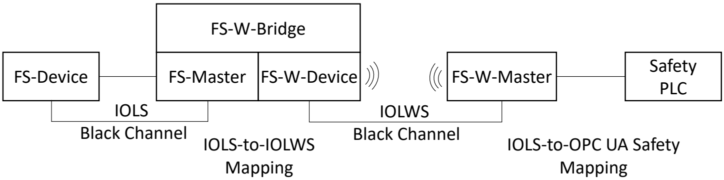


Figure 6.1.: Black Channel Principle using IOLS and IOLWS [29].

The system overview has already been shown in Chapter 5, but in 6.2 a simplified, schematic is presented with a more detailed description with respect to the system context of IOLWS system extension library (fullpage in Appendix D.4).

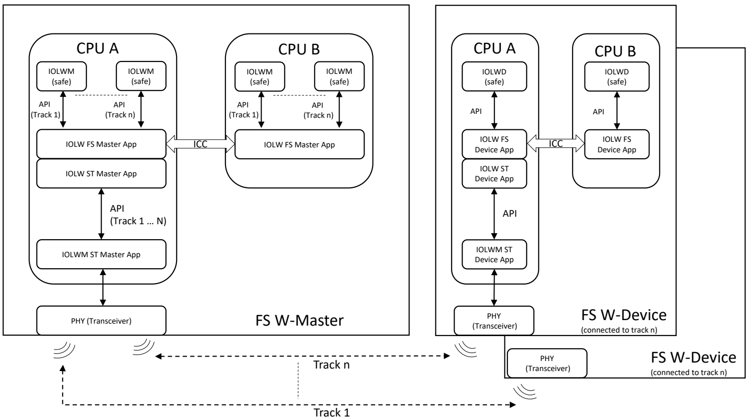


Figure 6.2.: System context of IOLW Safety system extension library [148, 149], fullpage view in Appendix D.4.

The software instances of IOLWS are illustrated as `IO-Link Wireless Master (IOLWM) (safe)` for the W-Master and `IOLWD (safe)` for the W-Device. A redundant control system is established using a FS-W-Master and a FS-W-Device with each of the CPUs respectively, whereas one or more instances of IOLWM or IOLWD are executed. An important design orientation was to create symmetric libraries such that the same code is executed in both channels [30]. Furthermore, the safety libraries shall never directly access system resources, e.g. for inter processor communication, memory allocation, timer handling, or persistent storage. Also, the safety libraries shall not require direct control of the IOLW black channel [148, 149].

6.2. Hardware Description

A prototype implementation based on the configuration depicted in Fig. 6.1 has been realized. Fig. 6.3 depicts a picture of the hardware setup.

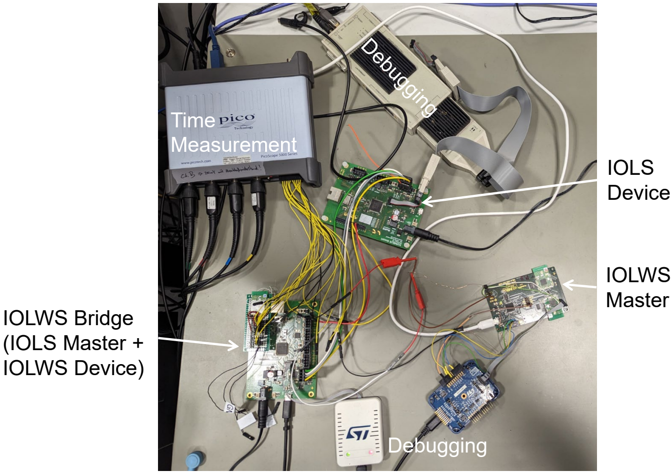


Figure 6.3.: Laboratory prototype implementation of IOLS-2-IOLWS.

The following hardware is used for the laboratory prototype:

- IOLS Master and Device: IO-Link DTK board [150] including
  - CPU: STM32F207vet6 [151]
  - Programmable GPIOs
  - Ethernet port, IO-Link port, debug interface, micro-USB connection, power supply, and status LEDs.
- IOLWS Device: Phytec module based on a CC2650 system-on-chip (SoC) radio transceiver [97].
- IOLWS Master: IO-Link Wireless One Track USB-Master [152]
  - CPU: STM32F205 [153]
  - IO-Link port, debug interface, power supply, and status LEDs.

6.3. IO-Link Wireless Safety Master[2]

Generally, one W-Master controls a number of W-Devices with each being connected individually to a physical wireless port, which in this case is an IOLW transceiver. For each wireless port, an individual IOLWM instance is required, which has the following tasks:

1. Safe configuration of IOLWM instance with functional safety protocol (parameter) (FSP) relevant for safe process data exchange
2. SPDE

If an error is detected in the safe configuration of the IOLWM instance in the initial management state, the safe process data exchange is prevented for the wireless port by the affected IOLWM instance. In this case, a FSP reconfiguration of the affected instance is required to proceed to normal operation and also any other application programming interface (API) call causes a system error until the reconfiguration is successful. The FS-W-Master is responsible for the setup of the necessary underlying non safe IOLW black channel as well as the safety related parameterization of the FS-W-Device. There is no interaction between the various IOLWM instances, which are trigger-able by the FS-W-Master regarding the management of the safe connection or the safe process data exchange. Only the FS-W-Master application itself may handle interactions between the wireless ports [148].

6.3.1. Execution Model and States

Two state machines are implemented using the IOLS Master library extended/enhanced for IOLWS:

1. Master management state machine
2. Safe process data exchange state machine [30]

The IOLWS Master API calls are used to control both state machines. A system error is triggered if the API call sequence is not adhered. The sequence of the API calls is illustrated in Fig. 6.4 showing the FS-W-Master sequence flow for FS communication and process data exchange.

[2] based on IOLS Master [148]

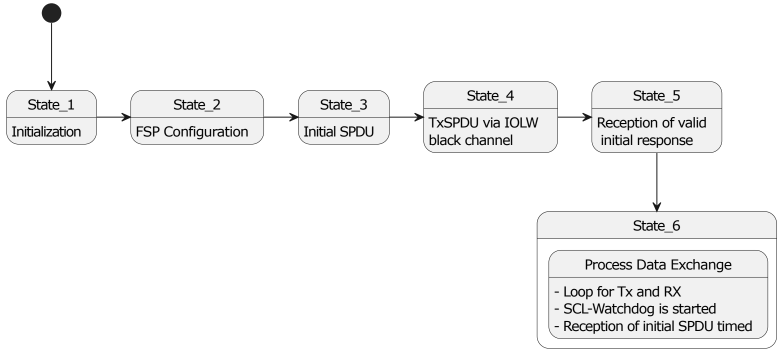


Figure 6.4.: FS-W-Master sequence flow for functional safety wireless (FS-W) communication and process data exchange [148].

The management state machine of a FS-W-Master is presented in Fig. 6.5 with the management state `Initialized`, which is realized after initialization of the instance and considered as a safe state, because no safe process data exchange occurs.

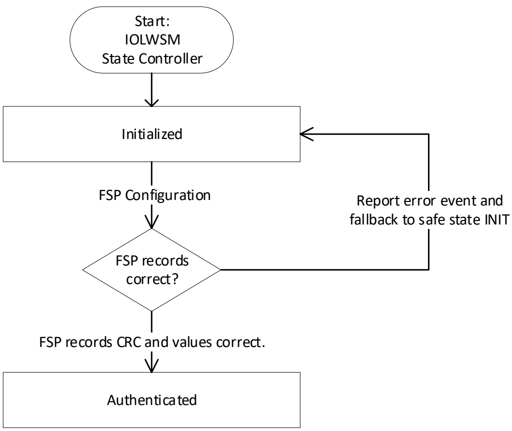


Figure 6.5.: FS-W-Master management states based on [148].

If the FSP records are correct and therefore the FSP configuration becomes valid, the management state `Authenticated` is entered to enable SPDE. As noted in [30], two different operation modes exist:

- Armed operation mode enabling regular safe process data exchange for normal operation, or
- monitored operation mode providing safe process data exchange for test purposes under operation supervision.

6.3.2. Initialization

First, the IOLWM instance data structure must be initialized to use its services and its sub-components being responsible for managing the IOLW track and slot to their initial state. Additionally, addresses and lengths of the Tx- and Rx-buffers holding the process data (SPDU) are set as well as the user pointer referencing the IOLW FS TrackSlotNr (here translated IOLS port number). If the initialization is successful, the IOLWM instance changes to the management state `Initialized`. To proceed with the FSP configuration, the FS-W-Master needs information regarding authentication, protocol configuration, and length of the Rx- and Tx-SPDU.

6.3.3. Functional Safety Process Configuration

The FSP configuration starts with the information relevant for FSP authenticity and FSP to the IOLWM user application and instance controlling the TrackSlotNr.

The FSP authenticity and FSP protocol parameter records are passed to the API function during the FSP configuration in order to verify the embedded CRC values. If the values are correct, the records are copied to the IOLWM instance. Also, cross comparison checks between pointer and buffer of the IOLWM instance are used to validate the correct program execution. If no error occurred during FSP parameter checks, the FSP configuration is successful and the IOLWM instance switches to the management state `Authenticated` and the user is allowed to start safe process data exchange with the FS-W-Device. If any other value than no error is returned, a safety error during FSP configuration occurred and the IOLWM instance remains in the management state `Initialized`. Therefore, safe process data exchange with the FS-W-Device and this IOLWM instance is prohibited. A reconfiguration of the FSP parameter or a complete reset of the IOLWM instance is necessary.

6.4. IO-Link Wireless Safety Bridge/Device[3]

In comparison to a FS-W-Master, a FS-W-Device only consists of one IOLWD instance, because only one single IOLW physical wireless port is able to connect the W-Device to the W-Master. The IOLWD instance processes the FSP authenticity and protocol parameter during parameterization and also controls the parameterization process of the FS-W-Device. At the end of the parametrization process of the FS-W-Device, a CRC based integrity check of the FSP and FS-W-Device specific functional safety technology (parameter) (FST) check is performed. Also, the authentication of the FS-W-Device during the establishment of the safe connection, such as safe process data exchange, must be realized.

If an error is detected during the CRC or authentication check, the IOLWD instance will forward to a `FAILSAFE` state preventing the FS-W-Device from exchanging safe process data. The `FAILSAFE` state can only be resolved if the FS-W-Device is restarted and e.g., the FS-W-Device is reconfigured. Any communication errors during the process data exchange are resolved by the SCL state machine and handled using a qualifier handler of the FS-W-Device as described in [149].

6.4.1. Execution Model and W-Device State Machines

All services offered by the FS-W-Device are only allowed to be accessed via the API functions of its instance. The API functions are included with the header file of the FS-W-Device. The IOLWS Device library offers several API functions such as:

- Initialization,
- FSP configuration,
- parameterization,
- process data handling,
- fault management,
- diagnosis, and
- other utilities (e.g., CRC calculations, memory set or compare, or stopping the watchdog timer).

[3] based on IOLS Device [149]

The API functions trigger the execution of the safety functions, such as process data exchange and parameterization. Accessible via API calls, three functional safety state machines (FSSM) are implemented by the IOLWS Device library:

- FSSM for common state
- FSSM for parameter management
- FSSM for safe process data exchange

6.4.2. IOLWS Device Management States

Fig. 6.6 presents the FSSM for common FS-W-Device management containing four states in a lifetime of an IOLWD instance. Before using the IOLWS Device library, all subcomponents handling the IOLWS Device must be set to their initial state and the following parameters must be provided:

- Addresses of Tx- and Rx-buffers containing complete SPDU
- Lengths of each buffer
- User reference pointer for the IOLWD instance

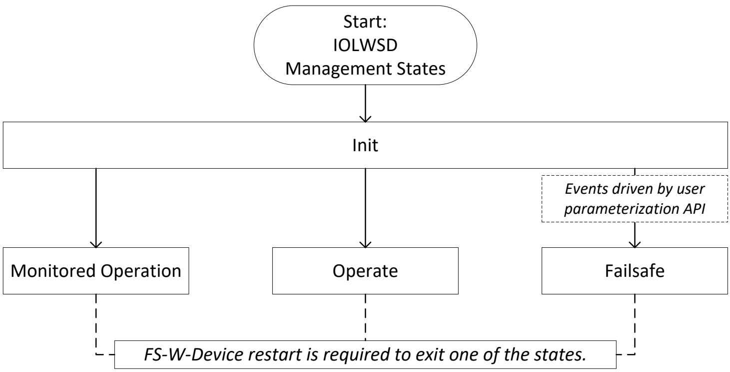


Figure 6.6.: FS-W-Device management states based on [149].

If the FSP parameter set, its consistency check, and the FS-W-Device authentication are successful, the IOLWD instance passes into state `Init` directly after initialization of the instance data. The commissioning (test) described in [30, Annex G], also named `Monitored Operation`, is entered if the IOLWD instance consists of valid FSP authenticity information and the FSP parameter set is unlocked. Locking state is reported after FSP configuration, and the FS-W-Device is authenticated. Next, the exchange of safe process data is possible with unlocked parameter and only under operator supervision. The `armed operation mode` [30, Annex G] is denoted here as state `Operate` and is entered if the IOLWD instance consists of

- valid FSP authenticity information,
- locked FSP parameter set,
- successful integrity and consistency check of the FS-W-Device FST parameter set, and
- a successful authenticated FS-W-Device.

Next, the exchange of safe process data is possible with locked parameter in `normal operation`.

If a fault is detected during the consistency check or the authentication of the FS-W-Device, the state `FAILSAFE` is entered. Then, a reconfiguration of the FST or FSP parameter set might be necessary and therefore, the FS-W-Device shall restart with subsequent reinitialization, FSP configuration, and authentication.

6.5. Process Data Exchange

In case of the IOLWM instance, process data exchange (PDE) is enabled after a successful FSP configuration. For the FS-W-Device, PDE is only enabled if the authentication was successful during the startup triggered by the IOLW configuration manager of the black channel (FS-W-Master) after port (translated from track/slot) mode `idle`. PDE starts by sending the initial SPDU, whereas the user needs to

- allocate the data exchange buffer,
- load Tx-process image data,
- prepare an initial Tx-SPDU,
- exchange the contents between buffers for cross checking, and
- transfer the prepared Tx-SPDU to the IOLW black channel within the next IOLW frame.

Now, the FS-W-Master PDE state machine waits for a response (Rx-SPDU) from the FS-W-Device. Invoking or subsequent sending of process data will result in a system error. If Rx-SPDU is transmitted, the IOLW black channel provides updated process data on an TrackSlotNr and the IOLWM instance is informed. Therefore, the instance will stop the SCL watchdog timer, safety protocol processing is started, and the new input is provided for cross checking and application-dependent operation. Additional Rx-SPDU calls are now prohibited and a Tx-SPDU call must be initiated. Similar to [30], status flags are used to interpret the SPDU processing results as follows:

- SCL transmission problems are resolved and an operator acknowledgment is necessary to proceed normal operation.
- Safe process data is applied in Rx and Tx direction, which may result from a user requesting safe process data or IOLWM / IOLWD instance reporting a transmission fault.
- Timeout or communication error of FS-W-Master or FS-W-Device, or general sequence, CRC, or TrackSlotNr error.

6.6. Security-for-Safety Communication Layer

6.6.1. Preliminaries

In the previous Chapters 3 and 4 and publications [3, 14, 16, 108] general IOLW security specific concepts and implementations are discussed. Regarding the cyclic communication, a symmetric pre-shared key is assumed to sustain the necessary one-to-one communication during cyclic communication for the IOLWS black channel.
Within the configuration, the security level setting must be set. Therefore, various well-established wireless protocols, such as BLE, Zigbee, WirelessHART, LoRaWAN, or EnOcean, are analyzed [3] and in this case an adoption from BLE [154] with the following security levels are itemized in Table 6.1 are employed.

Table 6.1.: Proposal for security level configuration of IOLW.

Security Level	User Interaction	Authentication	MITM Protection	Encryption Encryption
0	-	-	-	-
1	x	-	-	-
2	x	-	-	x
3	x	x	x	-
4	x	x	x	x

An error event must be called in case of an encryption, decryption, authentication, or verification error causing the IOLWS layer not to proceed.

6.6.2. MAC implementation

The security layer of the prototype focuses on the exemplified implementation of the MAC using Poly1305 [155, 156] to guarantee authenticity and integrity (Level 3). Here, the MITM protection is only mentioned, but is feasible by applying a combination of watchdog and MAC. For the used hardware platform (STMF32F205 and STMF32F207) of the IOLWS Bridge and IOLWS Master, no cryptographic accelerator is supported. Therefore, a software implementation of mbedTLS is applied.

Fig. D.6 in Appendix D illustrates the IOLW security layer for a MAC implementation using mbedTLS with Poly1305. The SPDE starts with the preparation of the SPDU parameter followed by the options that an IOLWS master or device transceives or receives a SPDU. Then, the security layer is called, and depending on the security level, different confidentiality, integrity, authenticity/availability (CIA) supporting algorithms may be chosen. In this case, the security level three is set and the platform security architecture (PSA) is initialized. Poly1305 with mbedTLS is chosen for MAC generation. The following functions are called within the mbedTLS library [157, 158]:

- mbedtls_poly1305_init: initializes the specified Poly1305 context
- mbedtls_poly1305_starts: sets the one-time authentication key
- mbedtls_poly1305_update: feds the SPDU data into the ongoing computation and may be called repeatedly (data stream)
- mbedtls_poly1305_finish: generates the MAC
- mbedtls_poly1305_free: releases and clears the specified Poly1305 context

The software library mbedtls_poly1305 generates a MAC of 16 bytes. Here, only the first 4 bytes of the computation (authentication length) are employed, because the security analysis of the birthday attack (see Chapter 4) showed that this is sufficient secure. Next, the SPDU is finalized with loading the MAC for transferring via IOLW.

Note, in case of an error within each step, error handling is called and processes are repeated or an error is written.

6.7. Error Handling

Errors may occur during PDE, such as SCL watchdog timeout, loss of IOLW black channel communication, or FS-W-Device replacement.
The watchdog timer is started during the preparation of a Tx-SPDU and stopped during Rx-SPDU processing. If the FS-W-Master did not receive a Rx-SPDU with a new sequence number during the watchdog time, a timeout is generated and the event is reported to the IOLWM instance. Next, the IOLWM instance enters the error handling of the SCL state machine and sends safe data in Rx- and Tx-direction until the error situation is resolved. Then, all bytes of the Rx-buffer for the process data input are set to zero.

A loss of the IOLW black channel communication may occur if a longer communication interruption appears between the FS-W-Master and the FS-W-Device. Therefore, the FS-W-Master may restart the IOLW black channel and initiates the power cycle of the interrupted connection while the FS-W-Device performs a cold start, similar to [30].

In case of a FS-W-Device replacement, the track and slot of the FS-W-Master is powered off and the old FS-W-Device is exchanged with the new replacement. Then, the track and slot is powered on again. The replacement of a FS-W-Device is similar to a temporary loss of IOLW black channel communication. Additional error handling is necessary, but is not the main focus of this contribution.

6.7.1. SCL watchdog timeout

The watchdog timer is started during the preparation of a Tx-SPDU and respectively stopped during Rx-SPDU processing. The watchdog timeout is configured in the FSP parameter set of the FSP protocol parameter record. The timeout of the watchdog is reset on each successful reception of the Rx-SPDU with a correct sequence number. Therefore, the timer system is provided by the application-dependent equipment, which is in this case the used W-Master board. The watchdog timer is also started, stopped and synchronized for each connected safety device.

6.7.2. Authentication Fault

An authentication fault occurs if the MAC is incorrect and not verified against the created MAC. Depending on the SCL watchdog timeout, a new SPDU might be send and evaluated until the watchdog timer reaches its limit. In this case, the safety device goes into a safe state and the message is not transferred from the SeCL to the SCL layer.

6.8. Safety Function Response Time Measurement Evaluation

The safety function response time (SFRT) is measured by summing up time intervals of the IOLS transmission (t_{IOLS_trans}), the process of the IOLWS Bridge ($t_{IOLWSB\_process}$), and the IOLWS transmission depicted in Fig. 6.7. Here, the time required to transfer data from IOLWS Master to the PLC is not considered.

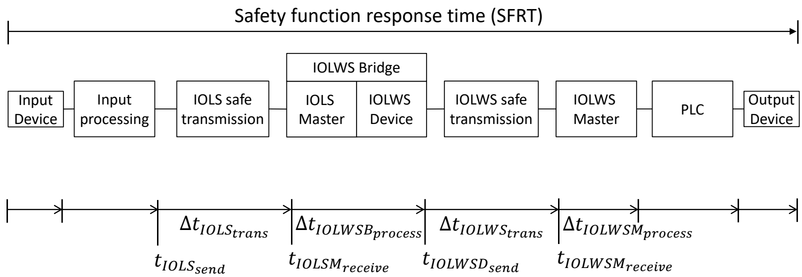


Figure 6.7.: Partial safety function response time of IOLS to IOLWS.

To measure the time duration of identical messages being sent and received, two bits are toggled and evaluated between IOLS Device and IOLWS Master. Therefore, both of the signal pairs of IOLSD and respectively IOLWSM must have similar falling or rising edges. An extract of the measurement for one DSLOT is depicted in Fig. 6.8.

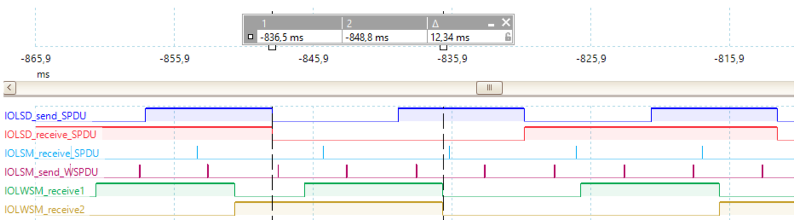


Figure 6.8.: Extract of safety function response time measurement for one DSLOT.

6.8.1. Transmission of one DSLOT

One DSLOT enables the usage of 14 bytes payload within the IOLWS channel, whereas the SPDU reserves 10 bytes as depicted in Fig. 5.2 resulting in 4 bytes for FS-W-PDin and FS-W-PDout data. There are several configuration parameter necessary to be set for IOLS and IOLWS connection. Table 6.2 lists only a few deciding parameter.

Table 6.2.: Configuration of IOLS and IOLWS for one DSLOT.

Configuration parameter	IOLS	IOLWSB	IOLWS
Port Mode	Mixed Safety	CYCLIC_AUTO	
Port	0	Slot:0, Track#:1	
Protocol version	1		
Protocol mode	2		
Supported transmission rate	COM 3		-
Minimal cycle time	3 ms	6 ms	1.644 ms
Process data input	-	-	MAC
Process data output	-	-	MAC
AuthCRC	24853		
TechParCRC	1		
IO-StructCRC	47413		
Protocol parameter CRC	52525		
Watchdog timeout	100 ms		
FS process data input	4 byte		
FS process data output	4 byte		
SPDU input length incl. MAC	14 byte		
SPDU output length incl. MAC	14 byte		

Note that configuration parameters regarding vendor ID, function ID, etc. must also be defined before startup. All parameters can be configured in a separate tool, which is sometimes called dedicated or configuration tool. Here, the parameters are configured directly within the code and displayed in the configuration tool. Exemplary, the IOLWS configuration tool for one DSLOT is presented in Fig D.5 attached in Appendix D.

The FS-W-Bridge is set to use a process cycle time of about 6 ms resulting with an IOLS cycle time of 3 ms and IOLW transmission time of 5 ms (including 2 retries if necessary) to the best configuration for the fastest and reliable outcome within the laboratory environment.

Fig. 6.9 depicts the histogram of the IOLS transmission (Δt_{IOLS_trans}) with its mean value of 3.7 ms and an experimental standard deviation of around 22 μs. Since the minimal cycle time of IOLS is set to 3 ms, the safety communication overhead is around 0.7 ms. The data set can be assumed to be `normally` distributed.

Fig. 6.10 shows the IOLWS Bridge process time ($\Delta t_{IOLWSB\_process}$) being uniformly distributed with its mean value of 7.51 ms and a standard deviation of 1.48 ms. The IOLWS Bridge process time ranges from 5 to 10 ms, because its cycle time is around 5 ms and the two protocols (IOLS and IOLWS) are not synchronized.

Fig. 6.11 presents the distribution of the IOLWS transmission time (Δt_{IOLWS_trans}) concentrated around the mean value of 1.86 ms with a standard deviation of 0.02 ms. The data set can be assumed to be `normal` distributed.

Fig. 6.12 shows the distribution of the overall transmission time from the IOLS Device to the IOLWS Master ($\Delta t_{IOLS-to-IOLWS\_trans}$) being uniformly distributed with a mean value of 12.84 ms and a standard deviation of 1.47 ms.

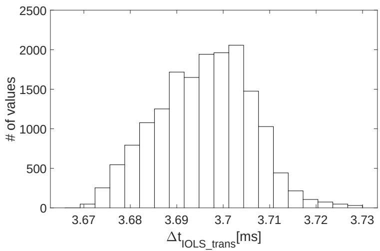


Figure 6.9.: IOLS transmission time using one DSLOT.

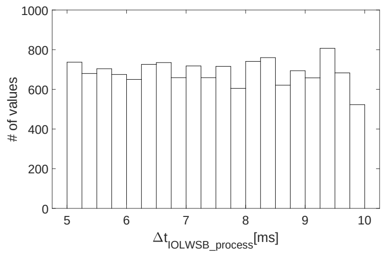


Figure 6.10.: IOLWS Bridge process time using one DSLOT.

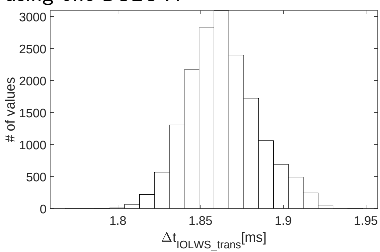


Figure 6.11.: IOLWS transmission time using one DSLOT.

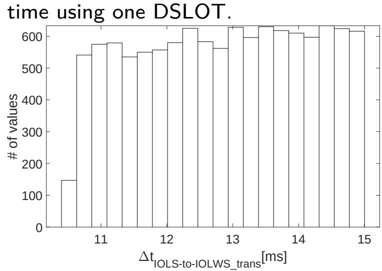


Figure 6.12.: IOLS-to-IOLWS transmission time using one DSLOT.

Table 6.3 reflects the mean values and experimental standard deviations of the transmission times and processing times using IOLS and IOLWS with 11,607 packets evaluated. The mean value of the IOLWS transmission time is 1.86 ms with an acceptable experimental standard deviation of 0.02 ms; also because no retries are necessary within the laboratory environment.

Table 6.3.: One DSLOT statistical measurement results.

	Mean value [ms]	Experimental standard deviation [ms]
Δt_{IOLS_trans}	3.70	0.022
$\Delta t_{IOLWSB\_process}$	7.51	1.48
Δt_{IOLWS_trans}	1.86	0.02
$\Delta t_{IOLS-to-IOLWS\_trans}$	12.96	1.35

Within a factory environment, evaluations regarding coexistence (such as [13] or [93]) might be necessary. In a only wireless production system, the additional IOLS transmission time (Δt_{IOLS_trans}) and IOLWS Bridge process time ($\Delta t_{IOLWSB\_process}$) is eliminable if the sensor is connected directly to the IOLWS communication channel.

6.8.2. Transmission of two DSLOTs

Two DSLOTs enable the usage of 28 bytes payload. The SPDU reserves 10 bytes as depicted in Fig. 5.3 resulting in 18 bytes for FS-W-PDin data. Several configuration parameter must be set for the IOLS and IOLWS connection. Table 6.4 presents the most relevant parameters.

Table 6.4.: Configuration of IOLS and IOLWS for two DSLOT.

Configuration parameter	IOLS	IOLWSB	IOLWS
Port Mode	Mixed Safety	CYCLIC_AUTO	
Port	0	Slot:0, Track#:1	
Protocol version	1		
Protocol mode	2		
Supported transmission rate	COM 3		-
Minimal cycle time	6 ms	12 ms	2x1.644 ms
Process data input	-	-	MAC
Process data output	-	-	MAC
AuthCRC	24853		
TechParCRC	1		
IO-StructCRC	18765		
Protocol parameter CRC	58355		
Watchdog timeout	100 ms		
FS process data input	18 byte		
FS process data output	18 byte		
SPDU input length incl. MAC	28 byte		
SPDU output length incl. MAC	28 byte		

The process cycle time of the IOLW Safety Bridge is set to 12 ms resulting in an IOLS cycle time of 6 ms and IOLW transmission time of two times 5 ms (including 2 retries if necessary) to the best configuration for the fastest and reliable outcome within the laboratory environment.

Fig. 6.13 depicts the histogram of the IOLS transmission (Δt_{IOLS_trans}) with its mean value of 7.26 ms and an experimental standard deviation of around 18 μs. Since the minimal cycle time of IOLS is set to 6 ms, the safety communication overhead is around 1.26 ms. The data set might be assumed to almost be `normal` distributed.

Fig. 6.14 shows the IOLWS Bridge process time ($\Delta t_{IOLWSB\_process}$) being uniformly distributed with its mean value of 17.89 ms and a standard deviation of 3.42 ms. The IOLWS Bridge process time ranges from 12 to 24 ms, because its cycle time is around 12 ms and the two protocols (IOLS and IOLWS) are not synchronized/coordinated.

Fig. 6.16 shows the distribution of the overall transmission time ($\Delta t_{IOLS-to-IOLWS\_trans}$) from the IOLS Device to the IOLWS Master being uniformly distributed between 23 ms and 33 ms with a mean value of 28.88 ms and standard deviation of 3.57 ms.

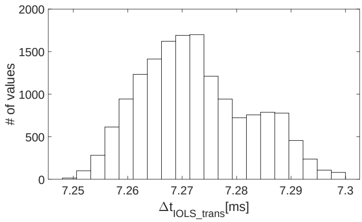


Figure 6.13.: IOLS transmission time using two DSLOTs.

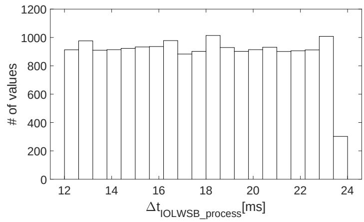


Figure 6.14.: IOLWS Bridge process time using two DSLOTs.

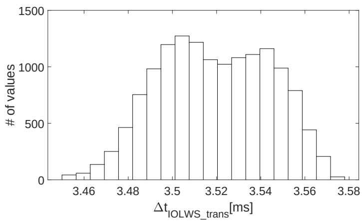


Figure 6.15.: IOLWS transmission time using two DSLOTs.

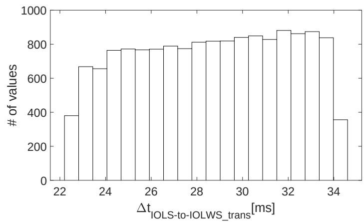


Figure 6.16.: IOLS-to-IOLWS transmission time using two DSLOTs.

Table 6.5 shows the mean values and experimental standard deviation of the transmission and processing using IOLS and IOLWS of 15,780 packets being evaluated. The mean value of the IOLWS transmission time is 3.68 ms with an acceptable experimental standard deviation of 0.49 ms; also because no retries are necessary within the laboratory environment. As mentioned before, within a only wireless production system, the IOLS transmission time (Δt_{IOLS_trans}) and the IOLWS Bridge process time ($\Delta t_{IOLWSB\_process}$) might be eliminable.

Table 6.5.: Two DSLOTs statistical measurement results.

	Mean value [ms]	Experimental standard deviation [ms]
t_{IOLS_trans}	7.26	0.018
$t_{IOLWSB\_process}$	17.89	3.42
t_{IOLWS_trans}	3.68	0.49
$t_{IOLS-to-IOLWS\_trans}$	28.88	3.57

CHAPTER 7

Summary and Outlook

7.1. Summary

In this thesis, a functional safety protocol for the low-latency sensor / actuator network IO-Link Wireless (IOLW) was developed. Relevant communication protocols, functional safety, partially channel coding, error types in communication, and (cyber-) security were introduced. Also, a selection of functional safety protocols and reaction times of safety communication protocols were outlined. By assessing the existing architecture of IOLW and IO-Link (IOL) Safety as extensions to IOL, a safety architecture proposal for IOLW Safety was developed to fit into the IOL stack architecture.

The safety requirements for IOLWS within the safety requirement specification (SRS) applying the black channel principle showed that the safety concept for IOLWS meets the relevant requirements according to the functional safety standards IEC 61508 [25] (SIL 3), IEC 62061 [28] (maximum SIL 3), EN ISO 13849-1 [27] (Category 4, PL e) and the industrial safety communication standard IEC 61784-3 [29]. A suitable functional safety extension proposal for IOLW was presented to fulfill the safety requirements involving an underlying security communication layer within its black channel. Therefore, the necessary functional safety measures were considered in the safety process data unit (SPDU) using an explicit implementation following a similar design concept as used in IO-Link Safety (IOLS). A regular SPDU with the required safety and security measures was proposed and the residual error rates were calculated. Additionally, a second option was suggested with cascading two SPDUs (transferring the same

SPDU twice), because this option is considered to work without implementing a PFH-Monitor, which monitors the average rate of a dangerous failure within a given time frame and has great influence on the calculation of the residual error rate (RER) (see Section 5.10). This option is considered if the patent for using the PFH-Monitor is not applicable [44].

The RERs for authenticity and timeliness are assumed to be zero, because a one-to-one connection without any storing element exists between a W-Master and W-Device/Bridge using the black channel principle. Even though IEC 61784-3 [29] requires residual error probability (REP) calculations up to a bit error probability (BEP) of 10^{-2}, the REP calculation for data integrity of the binary symmetric channel (BSC) extended by uniformly distributed segments for IOLWS was presented up to a BEP of 0.5, because of the implementation of an underlying security layer in the IOLWS black channel [40]. The SRS showed that the total residual error rate of IOLWS for a regular SPDU as well as for cascading two SPDUs is applicable for safety functions up to SIL 4, while no PFH-Monitor is needed for cascading two SPDUs.

Furthermore, the need for security to enable safe communication using IOLW was analyzed. A methodology to identify potential security issues of IOLW was applied and security measures were proposed for safety related IOLW applications. Because the current hardware used for IOLW is not capable to hold asymmetric keys, a proposal was made to establish an initial one-to-one connection. The focus was set on the security after commissioning to guarantee authentication and integrity or, if necessary, even confidentiality of each data packet. Therefore, possibilities to implement different cryptographic algorithms to accomplish confidentiality, integrity, and authentication for the IOLW protocol were evaluated and a suitable algorithm was proposed. The hardware accelerator driver of the transceiver chip as well as an open source software implementation were applied to encrypt plaintext during the uplink transmission of the IOLW Device. Also, authentication and integrity were implemented using the hardware security module (HSM) (such as AES-CCM) and the open source software implementation (such as Poly1305) with different payload lengths to simultaneously investigate timing issues.

Thus, a method was elaborated to precisely measure the application dependent additional current consumption caused by cryptographic algorithms of an IOLW transceiver. Current measurements showed that the current consumption of e.g., AES-CCM has no significant impact on the battery life time even if implemented as software.

A prototype implementation of the IOLWS protocol proposal was realized applying a regular SPDU. The hardware and software implementation was described including all individual components within the IOLS to IOLWS communication. Also, the security communication layer employs the necessary requirements of the authentication from the SRS. Representative measurements with two different payload lengths, one DSLOT and two DSLOT, were evaluated for the prototype implementation. The statistical evaluation for one DSLOT (14 octets payload) showed an IOLWS mean transmission time of 1.86 ms and an overall mean transmission time of IOLS to IOLWS of about 13 ms. For two DSLOTs (28 octets payload), an IOLWS mean transmission time of 3.68 ms and an overall mean transmission time of IOLS to IOLWS of about 29 ms were measured.

7.2. Outlook

As the IOLWS protocol concept evaluation is now completed with a positive approval, the next step is the negotiation of a specification for IOLWS. Then, a software stack implementation being certified by an accredited organization could lead to a safety protocol as a product.

As described within the conclusion, the current hardware used for IOLW is not capable to employ asymmetric cryptographic algorithms, therefore the successor of the current transceiver chip in use or another model shall be evaluated for IOLW resulting in secure initial exchange of the credentials for PDE or SPDE transmission of the IOLW/IOLWS to be implemented. Furthermore, holding asymmetric cryptographic keys and applying asymmetric cryptographic algorithms will make the secure transmission of the IOLW frequency hopping table during startup and commissioning feasible.

Another issue is that a functional safety protocol is not initially secure and vice versa a security protocol is not functionally safe, because functional safety mechanisms minimize residual errors whereas security mechanisms try to detect errors or manipulations injected purposely or created unintentionally. A particular problem evolves because some well-established assumptions for functional safety mechanisms may become incorrect using cryptographic algorithms if the BSC model is not applicable. Therefore, an authenticated and encrypted message may become secure, but the necessary risk reduction for a certain SIL classification cannot be proven any longer. In this case, functional safety and (cyber-)security are not independent from each other.

With the Cyber Resilience Act [159] being proposed in September 2022, economic operators will have two years after it became effective to adopt to the new (cyber-)security requirements and have to actively report exploited vulnerabilities and incidents within one year. Manufacturers have to ensure that their products sold have to handle vulnerabilities for the expected product lifetime or for a period of five years. Furthermore, security updates must be made available for at least five years [159]. This might also have a significant change of the philosophy how functional safety protocols are embedded into the overall system design and its security concept in general.

The logical consequence might be that a sustainable safety protocol must meet modern communication requirements including authentication and encryption with the worst possible BEP of 0.5 being stated in EN 50159 [96]. A guidance that both fields do not influence each other negatively shall be developed.

Furthermore also due to the field of artificial intelligence (AI), certain functional safety applications shall operate operational-safe in contrast to fail-safe. This perspective will also change safety and security concepts dramatically and emerge a future field of study.

APPENDIX A

Uncertainty Assessment

According to [160], two versions of the uncertainty expression exist:

- The simpler version has relatively small input quantity uncertainties and with inputs being uncorrelated.

- The second version applies to relatively small input quantity uncertainties with inputs being correlated to each other.

Here, it can be assumed that the input quantities are uncorrelated, since the corresponding terms belong to the respective hardware components of the measurement setup being manufactured independently, and therefore causing independent “tolerances”. The general expression of the simpler version is given by [160]:

$$u^2(y) = \left(\frac{\partial y}{\partial x_1}^2\right) u^2(x_1) + \left(\frac{\partial y}{\partial x_2}^2\right) u^2(x_2) + \ldots + \left(\frac{\partial y}{\partial x_n}^2\right) u^2(x_n). \tag{A.1}$$

This expression is equal to the combined standard uncertainty being described by the GUM [113, 160] as:

$$u^2(y) = \sum_{i=1}^{n} \left(\frac{\partial y}{\partial x_i}^2\right) u^2(x_i) \tag{A.2}$$

where:	$u^2(y)$	: combined variance or squared combined standard uncertainty of y,
	$u(y)$	: combined standard uncertainty of y,
	y	: the measurand $y = f(x_1, x_2, x_3, \ldots, x_n)$,
	$x_1, x_2, x_3, \ldots, x_n$	: input quantities.

The squared combined standard uncertainty $u^2(y)$ of the messurand y is a weighted sum of the squared standard uncertainties $u^2(x_i)$ of the input quantities x_i (with $i = 1, 2, 3, \ldots, n$). These partial derivatives may be referred to as sensitivity coefficients [160].

Applying equation A.2 to the measurement of the uncertainty estimation of Subsection 4.3.3:

$$\begin{aligned}\sigma_I^2 &= \left(\frac{\partial i}{\partial u}\right) \cdot \sigma_{Measured}^2 + \left(\frac{\partial i}{\partial u}\right) \cdot \sigma_{Equipment}^2 \\ &\quad + \left(\frac{\partial i}{\partial r}\right) \cdot \sigma_{Rshunt}^2 + \left(\frac{\partial i}{\partial u}\right) \cdot \sigma_{other}^2 \\ &= \left(\frac{1}{R}\right)^2 \cdot \sigma_{Measured}^2 + \left(\frac{1}{R}\right)^2 \cdot \sigma_{Equipment}^2 \\ &\quad + \left(\frac{U}{R^2}\right)^2 \cdot \sigma_{Rshunt}^2 + \left(\frac{\partial i}{\partial u}\right) \cdot \sigma_{other}^2\end{aligned} \tag{A.3}$$

where:	σ_I^2	: combined variance or squared combined standard deviation of the current,
	$\sigma_{Measured}^2$	: variance or squared standard deviation of the measurement,
	$\sigma_{Equipment}^2$	: variance or squared standard deviation of the equipment (power probe see Sect. 4.3.3.1.4),
	σ_{Rshunt}^2	: variance or squared standard deviation of the shunt resistor (see Sect. 4.3.3.1.3),
	σ_{other}^2	: variance or squared standard deviation of further components (cabling, connectors).

When neglecting the uncertainty of further components, the combined uncertainty with small and uncorrelated input quantity uncertainties is derived as:

$$\sigma_I = \sqrt{\underbrace{\left(\frac{1}{R}\right)^2 \cdot \sigma^2_{Measured}}_{TypeA} + \underbrace{\left(\frac{1}{R}\right)^2 \cdot \sigma^2_{Equipment}}_{TypeB} + \underbrace{\left(\frac{U}{R^2}\right)^2 \cdot \sigma^2_{Rshunt}}_{TypeB}} \cdot \tag{A.4}$$

As described in Section 4.3.3, Type A uncertainty is obtained by statistical methods (measured) and Type B uncertainty is obtained from data sheets.

APPENDIX B

CRC Generator Polynomials[1]

Hamming distance and properness for all required data lengths are key characteristics to select a particular generator polynomial.

The applied generated polynomial (`0x1EDC6F41`) is able to detect up to seven and any odd number of bit errors [143] since the generator polynomial consists of a primitive polynomial of degree (r – 1) with the maximum total block length of $2^{r-1} - 1$:

$$g(x) = p(x) \cdot (1 + x). \tag{B.1}$$

The residual error probability for the approved data length is 2^{-r} if the properness is approved.

It shall be prohibited that the CRC generator polynomial used in the underlying transmission systems, for example SDCI, matches the CRC generator polynomial used for SDCI-FS [29,30]. Therefore, in IOLWS the CRC32 polynomial `0x1EDC6F41` and in the underlying IOLW transmission system the CRC32 polynomial `0x4C11DB7` is used.

[1] based on [30, p. 112ff]

Table B.1.: CRC generator polynomials for SDCI-FS based on [144].

CRC32 Polynomial	Data length (bits)	Hamming distance	Properness	Remark
0x1EDC6F41 (“normal” representation of Castagnoli CRC polynomial)	≤177 ≤5243	≥8 ≥6	≤256 octets	Suitable for funct. safety with security layer in black channel

Note: High order bit is omitted in “Normal” representation.

The CRC32 can be used

- to secure cyclic Process Data exchange with a total safety PDU length of up to 32 octets, i.e. 22 octets for safety Process Data (see 11.4.4), and 10 octets of safety code, and
- to secure the transfer of up to 16 octets of FSP parameters at start-up or restart, and
- to secure the transfer and data integrity of the entire FST parameter set.

Residual Error Probabilities

To calculate REPs, the so-called “forgotten backdoor” is used by brute forcing the dual code to calculate the CRC performance [146, 161].

Figure B.1 depicts the results of residual error probability (REP) calculations over bit error probabilities (BEP) for safety PDU lengths from 10 to 14 octets.

The REP is less than 2^{-32} for BEPs less than the required 0.5 at a length of 14 octets. And if a cryptographic algorithm fulfilling the requirements of BSC is used for one SPDU (one Double Slot) less than the required 0.5 at a length between 10 to 14 octets.

If using two double Slots as SPDU with up to 28 octets, the requirement of BEP being less than 0.5 is also fulfilled (B.1).

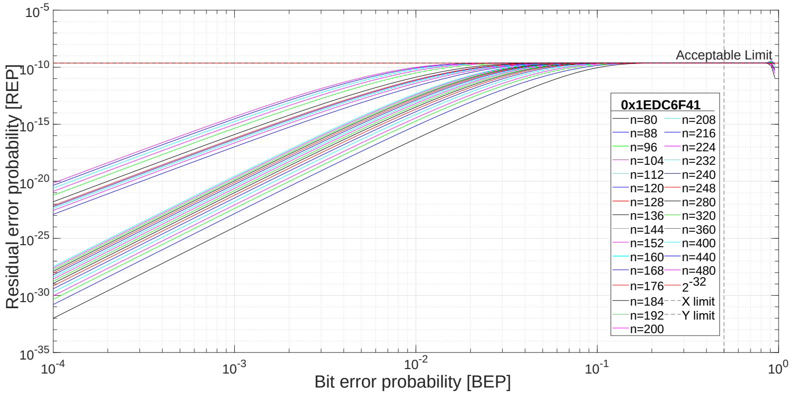


Figure B.1.: Residual error probability CRC32 for IOLWS generator polynomial for n=80 to n=480 using two DSLOTs

Tools for Implementation

The evaluation of the CRC polynomial is realized using a high-performance computing infrastructure with the help of a brute force approach [146]. For IOLWS, the Castagnoli CRC polynomial `0x1EDC6F41` is used and calculated with different message length up to n = 480 bits. Therefore, the Hamming weights of the CRC polynomial are calculated with the help of the McWilliams Identity [147] with the residual error probability for individual data lengths being dependent on the BEP using the determined weights. The saved matrix of the different Hamming weights and data lengths are used to calculate the residual error probabilities according to the bit error probabilities (in Matlab), which depends on the used CRC polynomial. The procedure is validated using [29] Annex H with the CRC reference polynomial `0x1F1922815`.

Residual Error Probability Values

Generator Polynominal: `0x1EDC6F41` (hexadecimal notation)
NOTE: This polynomial is named CRC32/8 in [162], and is referenced as CRC1 in B.2:

- Length (r) of the polynominal: 32
- Bit error probability (Pe): at “maximum of R_{CRC1}”; 2/n, 4/n; 0,01; 0,001; 0,0001; (n is number of Bit)
- SPDU length (octets); 10 - 28

Table B.2.: Residual error probabilities (R_{CRC1}) for example CRC32 polynomial (part 1)

SPDU (incl. CRC) (Octets)	SPDU (incl. CRC) (n Bits)	HD	Maximum or R__CRC1 P__e	Maximum or R__CRC1 Value of R__CRC1	R__CRC1 at Pe 2/n	R__CRC1 at Pe 4/n	R__CRC1 at Pe 0.01
12	96	8	0.15 - 0.5 (*pb)	2.328306436538696e-10	2.698241456705772e-13	1.228830845469424e-11	0.192228451920916e-15
13	104	8	0.15 - 0.5 (pb)	2.328306436538696e-10	2.89626704211409e-13	1.29765745451242e-11	3.668328304121486e-15
14	112	8	0.15 - 0.5 (pb)	2.328306436538696e-10	3.381622346885911e-13	1.4751636759206e-11	7.26922305502012e-15
18	144	8	0.09 - 0.5 (pb)	2.328306436538696e-10	3.90445255210991e-13	1.648271582311346e-11	4.724038109400062e-14
19	152	8	0.085 - 0.5 (pb)	2.328306436538696e-10	3.913838282105663e-13	1.647483158123194e-11	6.784107826120066e-14
20	160	8	0.08 - 0.5 (pb)	2.328306436538696e-11	3.906282502356025e-13	1.640506449186628e-11	9.484099027784112e-14
21	168	8	0.075 - 0.5 (pb)	2.328306436538696e-12	3.892585389623214e-13	1.631719247586103e-11	1.297178596782479e-13
22	176	8	0.075 - 0.5 (pb)	2.328306436538696e-13	3.894139750855001e-13	1.628894834290926e-11	1.748852399188199e-13
23	184	6	0.07 - 0.5 (pb)	2.328306436538696e-14	3.904439137224571e-13	1.629525798965322e-11	2.323989052325163e-13
24	192	6	0.07 - 0.5 (pb)	2.328306436538696e-15	3.908324606255827e-13	1.628098546660938e-11	3.036448775683795e-13
25	200	6	0.065 - 0.5 (pb)	2.328306436538696e-16	3.889174158076614e-13	1.618573773182253e-11	3.889174158076614e-13
26	208	6	0.06 - 0.5 (pb)	2.328306436538696e-17	3.875250689771754e-13	1.611173084847795e-11	4.924383368641103e-13
27	216	6	0.06 - 0.5 (pb)	2.328306436538696e-18	1.548749901895719e-12	2.6429447377795e-11	2.193189794033168e-12
28	224	6	0.06 - 0.5 (pb)	2.328306436538696e-19	2.468415617241979e-12	3.4627870246683e-11	4.013080396470456e-12

*Note: pb - proper behavior.

Table B.3.: Residual error probabilities (R_{CRC1}) for example CRC32 polynomial (part 2)

SPDU (incl. CRC)	SPDU (incl. CRC)	HD	Maximum or R__CRC1		R__CRC1 at Pe 0.001	R__CRC1 at Pe 0.0001
(Octets)	(n Bits)		P__e	Value of R__CRC1		
12	96	8	0.15 - 0.5 (*pb)	2.328306436538696e-10	4.212806582641252e-23	4.55970090037035e-31
13	104	8	0.15 - 0.5 (pb)	2.328306436538696e-10	8.631118938317472e-23	9.409244092133889e-31
14	112	8	0.15 - 0.5 (pb)	2.328306436538696e-10	1.838644688426793e-22	2.018895530690704e-30
18	144	8	0.09 - 0.5 (pb)	2.328306436538696e-10	1.585289080353439e-21	1.791471916915255e-29
19	152	8	0.085 - 0.5 (pb)	2.328306436538696e-10	2.441307664628087e-21	2.778701478654672e-29
20	160	8	0.08 - 0.5 (pb)	2.328306436538696e-11	3.65907042686269e-21	4.194760028883085e-29
21	168	8	0.075 - 0.5 (pb)	2.328306436538696e-12	5.364465597814436e-21	6.194109709330652e-29
22	176	8	0.075 - 0.5 (pb)	2.328306436538696e-13	7.751952648928019e-21	9.015284465182195e-29
23	184	6	0.07 - 0.5 (pb)	2.328306436538696e-14	1.104066987962213e-20	1.293240791603385e-28
24	192	6	0.07 - 0.5 (pb)	2.328306436538696e-15	1.545753608210117e-20	1.823639613648749e-28
25	200	6	0.065 - 0.5 (pb)	2.328306436538696e-16	2.120628139738018e-20	2.519859261450554e-28
26	208	6	0.06 - 0.5 (pb)	2.328306436538696e-17	2.87564031169051e-20	3.44158744264183e-28
27	216	6	0.06 - 0.5 (pb)	2.328306436538696e-18	1.057513538295603e-17	1.273029903260945e-23
28	224	6	0.06 - 0.5 (pb)	2.328306436538696e-19	2.336870938647801e-17	2.837523689662403e-23

*Note: pb - proper behavior.

APPENDIX C

Certified Concept Evaluation of IO-Link Wireless Safety

A positive concept evaluation of IOLWS has been developed in cooperation with TÜV SÜD Rail GmbH. The certified concept evaluation is attached below.

TÜV SÜD Rail GmbH· Barthstr. 16· D-80339 München· Germany

Choose certainty.
Add value.

Professur für Elektrische Messtechnik
Helmut-Schmidt-Universität, Universität der Bundeswehr Hamburg
Holstenhofweg 85
22043 Hamburg
Germany

Your reference/letter of	Our reference/name	Phone extension/e-mail	Fax extension	Date	Page
	PS Dr. P. Supavatanakul	+49 (89) 5791-2705 peerasan.supavatanakul@tuvsud.com	-2933	3rd August 2023	1 of 1

Re: Concept evaluation of IO-Link Wireless Safety

To whom it may concern:

we would like to inform you that the related review of the document

[A1]	IOLW Safety – Safety Requirement Specification	2.6	28.03.2023

has shown that the safety concept for **IO-Link Wireless Safety** is able to meet the requirements according to the functional safety standards IEC 61508:2010 (SIL 3), IEC 62061:2021 (Maximum SIL 3), EN ISO 13849-1:2015 (Category 4, PL e) and the industrial safety communication standard IEC 61784-3:2021.

For a future implementation of IO-Link Wireless Safety in a safety component, the execution of a respective safety lifecycle (safety management, requirements, design, implementation, V&V activities) shall be demonstrated to show compliance to the aforementioned standards.

Yours sincerely,

Günter Greil
Technical Certifier

Dr. Peerasan Supavatanakul
Project engineer

Walter Schlögl
Project engineer

Technical Report

on the evaluation of the

Safety Communication Protocol Specification Proposal
IO-Link Wireless Safety

Applicant

Professur für Elektrische Messtechnik
Helmut-Schmidt-Universität, Universität der Bundeswehr Hamburg
Holstenhofweg 85
22043 Hamburg
Germany

Report No.: HH101102T

Version 1.4 of 2023-10-26

Test Body

TÜV SÜD Rail GmbH

Rail Automation
Barthstraße 16
D-80339 München

Table of Contents page

List of Tables page

List of Figures page

Modification History

Rev.	Status	Date	Author	Modification / Description
0.1	Replaced	2023-04-06	Dr. P. Supavatanakul	Initial
1.0	Replaced	2023-06-08	Dr. P. Supavatanakul	
1.1	Replaced	2023-07-28	Dr. P. Supavatanakul	Formal update
1.2	Replaced	2023-08-07	Dr. P. Supavatanakul	Update figures
1.3	Replaced	2023-08-24	Dr. P. Supavatanakul	Typo corrections
1.4	Active	2023-10-26	Dr. P. Supavatanakul	Update figures

Table 1: Modification history

List of Abbreviations

Abbreviation	Description
DC	Diagnostic Coverage
FMEDA	Failure Mode, Effects and Diagnosis Analysis
FR	Failure Rate (number of corrupted / wrong packets per hour)
PFD	Probability of Dangerous Failure on Demand
PFH	Average Frequency of Dangerous Failure per hour (h^{-1})
QMS	Quality Management System
SFF	Safe Failure Fraction
SIL	Safety Integrity Level
ToE	Target of Evaluation
FSCP	Functional Safety Communication Profile
MAC	Message Authentication Code
IOL	IO-Link
IOLW	IO-Link Wireless
IOLS	IO-Link Safety
IOLWS	IO-Link Wireless Safety
W-Device	Wireless Device
W-Master	Wireless Master
SDCI	Single Drop Digital Communication Interface
SCL	Safety Communication Layer
SPDU	Safety Protocol Data Unit

Table 2: Abbreviations

1 Target of Evaluation (ToE)

In September 2021, Helmut-Schmidt Universität requested TÜV SÜD Rail GmbH to evaluate the safety network protocol specification IO-Link Wireless Safety according to the standards listed in clause 3 of this report. The specification proposes the requirements for IO-Link Wireless Safety as input for system design and a functional specification. The project number related to this Technical Report is 717524449.

This technical report summarizes the evaluation results of the concept and the proposal of implemented safety measures in IO-Link Wireless Safety.

2 Scope of Evaluation

2.1 Evaluation Specimen

IO-Link Wireless (IOLW) is the extension to the IO-Link standard IEC 61131-9 known as Single Drop Digital Communication Interface (SDCI), which extends the traditional switching input and output interfaces towards a point-to-point communication link using coded switching. The main application of IOLW is the communication of sensors and actuators within an automation system. IOLW supports bidirectional wireless communication for process data and on-request data between a Wireless Master (W-Master) and Wireless Devices (W-Device). The IOLW Safety specifies the functional safety communication model across IOLW communication. The proposal of the IOLW Safety specification from Helmut-Schmidt Universität describes the safety measures to be implemented in the safety-related communication for sensors and actuators which are necessary to enhance the IOLW communication stack for exchange of safety related data. IO-Link Wireless is used as a “black channel” for an additional Safety Communication Layer (SCL) allowing the safety data to be transmitted between the W-Master and its connected W-Devices or W-Bridge.

Figure 1 depicts an example architecture of an automation topology with an IOLW Safety System.

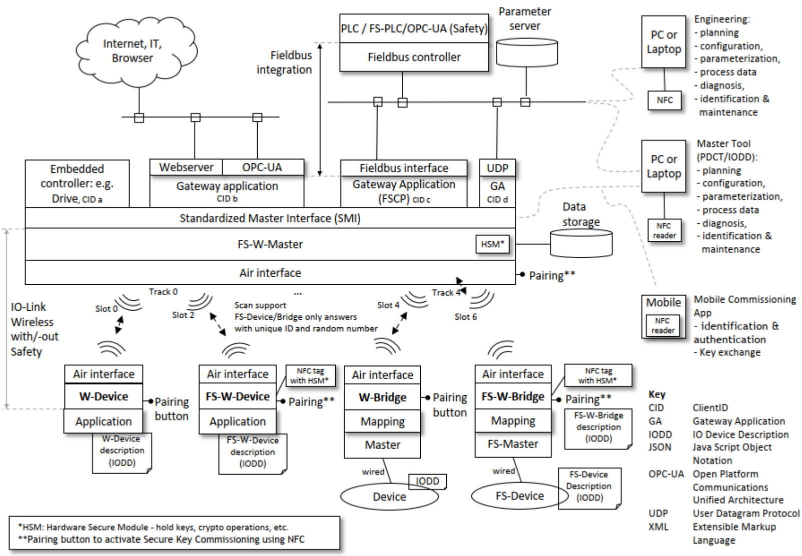


Figure 1: IOLW Safety System

2.2 Evaluation scope

The evaluation scope of the IOLW Safety protocol in this report concerns the specification of safety communication using the IO-Link Wireless protocol (as a Black Channel) between FS-IOLWS Master and FS-IOLWS Device (see Figure 2). The proposal from Helmut-Schmidt Universität specifies essential safety requirements for functional safety, communication integrity and interoperability of IOLW Safety.

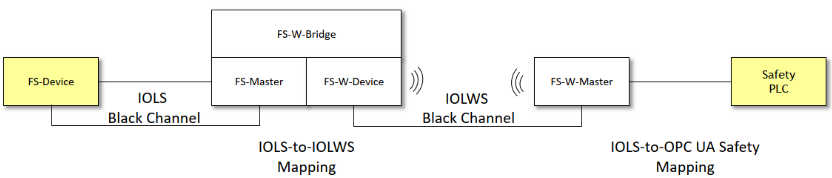


Figure 2: Black Channel, FS-W-Master/ FS-W-Device

Figure 3 illustrates the structure of the FS-W-Master and FS-W-Device SPDUs excluding standard IO data. A 32- bit MAC (based on AES-128 CCM) is used across the FS-W-Output data, Track/SlotNr, the control and counting, and the CRC signature to guarantee message integrity and authenticity using a secret only known to both communication ends. The Track/SlotNr is used as an additional measure for identification. Although in IOL Safety a 3-bit counter is used, the IOLW Safety specifies the use of a 5-bit counter in combination with the local watchdog timer to achieve timeliness. The feedback signal from the FS-W-Device employs the inverted counter value for the timeliness check to prevent loop-back errors.

The FS-W-PDout length is limited to 22 octets and the input data to 4 octets for the FS-W-PDin.

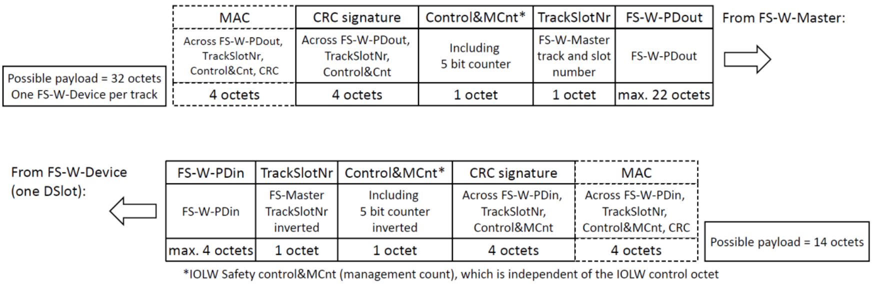


Figure 3: IOLW Safety PDUs

The proposal of the IOLW Safety follows the principle of "de-energize to trip". When encountering a fault or communication error such as a timeout, a CRC or MAC error, a counter error, a Track/SlotNr error, the associated qualifier bit will be set. It will be only released after an explicit operator acknowledgment on the FS-W-Master side. After a CRC or MAC error a warm start is possible (cf. /N2/).

2.3 Evaluation

The design of IOLW Safety was examined by TÜV SÜD Rail GmbH with respect to the following evaluation segments:

Functional safety

- analysis of the defined safety measures according to IEC 61508-2:2010
- analysis of the defined safety measures according to IEC 61784-3:2021
- analysis of the defined safety measures according to IEC CD 61784-3:2021/ AMD1.

3 Standards and Guidelines

The regulations and guidelines which form the basis of the evaluation are listed below.

3.1 Functional Safety Standards

No.	Reference	Description
/N1/	IEC 61508-2:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 2: Hardware
/N2/	IEC 61784-3:2021	Industrial communication networks – Profiles Part 3: Functional safety fieldbuses – General rules and profile definitions
/N3/	IEC CD 61784-3:2021/AMD1	Industrial communication networks – Profiles Part 3: Functional safety fieldbuses – General rules and profile definitions Amendment 1

Table 3: Functional safety standards

3.2 Quality Management System

No.	Reference	Description
[M1]	QMS	Quality Management System TÜV SÜD Rail GmbH
	TR_RA_P_04.50	Test Program Functional Safety TR_RA_P_04.51 Definition Scope of testing TR_RA_P_04.07 Product modification TR_RA_P_04.52 Concept Phase & Safety Lifecycle TR_RA_P_04.55 Safety Manual TR_RA_P_04.56 Result of Testing (R)
[M2]	D-PL-11190-08-00	DAkkS accreditation according to DIN EN ISO 17025:2018 / EN ISO/IEC 17025:2017

Table 4: Quality Management System

4 Documents provided for Evaluation

Following document was provided for checking by Helmut-Schmidt Universität:

No.	Title	Document-No./File identifier	Rev.	Date
[D1]	IOLW Safety- Safety Requirement Specification	IOLW-Safety	2.6	28.03.2023

Table 5: Documents provided for evaluation

5 Evaluation Documents

Following test reports were issued by TÜV SÜD Rail GmbH:

No.	Title	Document-No./File identifier	Rev.	Date
[R1]	Review Protocol	717524449_Review_Protocol_HSU_DTEC_SRS	1.5	26.07.2023
[R2]	Checklist safety communication IEC 61508-2	717524449_Checklist_Communication	1.0	16.07.2023

Table 6: Evaluation results

6 Performance and Result of the Evaluation

IOLW Safety Specification was inspected regarding the consistency compared with /N1/, /N2/, and comprehensibility of the individual descriptions.

The error models (see /N2/) for communication considered in IOLW Safety include:

- Data corruption
- Unintended repetition
- Incorrect sequence
- Loss
- Unacceptable delay
- Insertion
- Masquerade
- Addressing
- Loop-back of messages
- Errors considered as uniformly distributed segment (UDS) /N3/

The SCL including the requirements for safety measures defined by IOLW Safety were analyzed to fulfil the requirements to ensure safe transmission of data in accordance with /N1/, /N2/ and /N3/.

The quantitative analysis for each failure scenario of the communication was performed by Helmut-Schmidt-Universität and reviewed by TÜV SÜD Rail GmbH based on the options given in the table below.

#	Option	Note
I	Regular SPDU	SPDU as described in Figure 3 with optional MAC
II	Cascading two SPDUs	Cycle time may increase as described in Figure 3 with optional MAC

Table 7: Options including measures for SPDU considerations

The applied 32-bit CRC polynomial as well as the PFH monitor have been considered in the probabilistic calculations, which were analyzed in accordance with the probabilistic requirements of /N2/ and /N3/. The total residual error rate for each option has been determined in [D1] and summarized in the following table.

#	Option	Total Residual Error Rate (λ_{SC})	Applicable for	Note
I	Regular SPDU	$\lambda_{SC}(PFH = 10h) \approx 2.3 * \frac{10^{-11}}{h}$ $\lambda_{SC}(PFH = 1h) \approx 2.3 * \frac{10^{-10}}{h}$	SIL 4	If PFH-Monitor is used and $RR_T \& RR_A = 0$
II	Cascading two SPDUs	$\lambda_{SC2} = 3.9 * \frac{10^{-14}}{h}$	SIL 4	If PFH-Monitor cannot be used and $RR_{T2} \& RR_{A2} = 0$

Table 8: Summary of total residual error rate

The residual error probability calculation for data integrity of the binary symmetric channel extended by uniformly distributed segment (UDS) for IOLW Safety was presented up to a bit error probability of 0.5 due to the implementation of a underlying security layer in the IOLW Safety black channel (cf. /N3/). Security algorithms in the black channel affect randomly generated error patterns in the communication and BSC can still be applied if the bit error probability up to 0.5 is used.

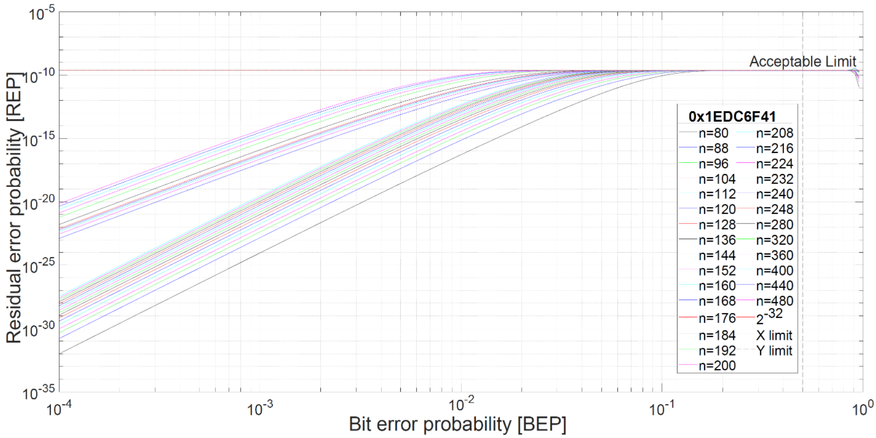


Figure 4: Residual error probability CRC-32 for IOLW Safety generator polynomial for n = 80 to 480.

For the parameter transfer, the residual error rate has been determined based on the assumption that the average transmission rate is 1/day and the residual error rate for the configuration and parameterization errors during e.g. download can be calculated using the residual error probability of the chosen CRC multiplied by the transmission rate.

Evaluation result:

According to the safety standards in Chapter 3.1 the error models in combination with the required integrity measures for communication via black channel have been inspected. The safety layer for IOLW Safety proposed can detect typical communication errors defined in /N2/, i.e. repetitions, deletion, insertion, resequencing, corruption, delay and masquerade. The specified safety measures provide the required coverage of the communication error models.

The calculated residual error rate for the communication using IOLW Safety is sufficiently low compared to the required safety characteristic data. The residual error rate of IOLW Safety communication consumes less than 1% of the maximum PFH for SIL 3 of the overall safety function according to /N1/ and /N2/.

The evaluation showed that the proposal for IOLW the Safety specification is consistent with the applicable requirements given in /N1/, /N2/ and /N3/. It provides implementation guidance for the design level with sufficient clarity for system implementators.

The detailed evaluation results of IOLW Safety are documented in the review protocol [R1].

7 Application Conditions

The IOLW Safety requirement specification assumes the use of IO-Link Wireless as a black channel and does not place any requirements on the development of the hardware and software of a particular device. The technical measures of IOLW Safety shall be implemented within safety communication layer in safety devices designed in accordance with IEC 61508 and shall meet the target SIL. /N2/ specifies the requirements for electrical, environmental and electromagnetic stress which shall be fulfilled for a functional communication system. These requirements might need modification as required by specific application standards.

8 Testing Body

This report is based on the accreditation of the testing laboratory for safety components; see table “Quality Management System”.

9 Summary

The evaluation results of clause 4 showed that the proposal for IOLW Safety, as specified in clause 2.1, can fulfil the requirements of the standards and guidelines referenced in clause 3.

Dr. Peerasan Supavatanakul Walter Schlögl

APPENDIX D

Enlarged Figures

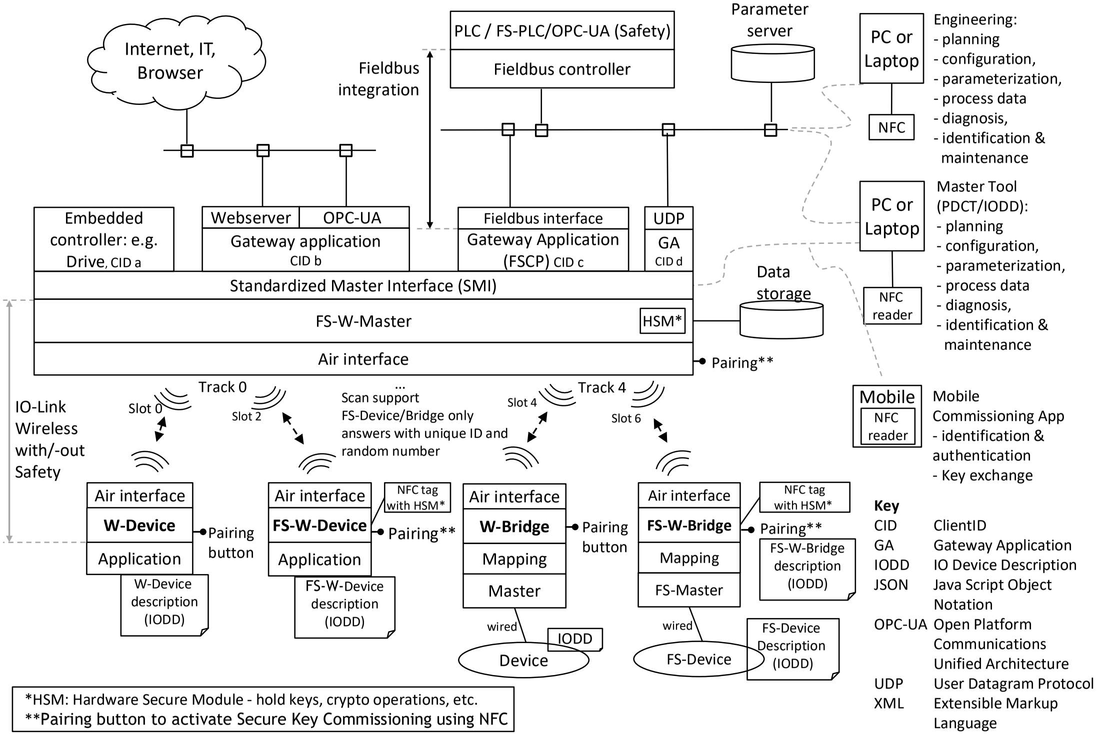


Figure D.1.: Proposed IOLW Safety configuration (with added features in bold) within the automation hierarchy based on [22], back to embedded Fig. 3.1.

From FS-W-Master:

MAC	CRC signature	Control&MCnt*	TrackSlotNr	FS-W-PDout
Across FS-W-PDout, TrackSlotNr, Control&Cnt, CRC	Across FS-W-PDout, TrackSlotNr, Control&Cnt	Including 5 bit counter	FS-W-Master track and slot number	FS-W-PDout
4 octets	4 octets	1 octet	1 octet	max. 22 octets

Possible payload = 32 octets
One FS-W-Device per track

From FS-W-Device (one DSlot):

FS-W-PDin	TrackSlotNr	Control&MCnt*	CRC signature	MAC
FS-W-PDin	FS-Master TrackSlotNr inverted	Including 5 bit counter inverted	Across FS-W-PDin, TrackSlotNr, Control&MCnt	Across FS-W-PDin, TrackSlotNr, Control&MCnt, CRC
max. 4 octets	1 octet	1 octet	4 octets	4 octets

Possible payload = 14 octets

*IOLW Safety control&MCnt (management count), which is independent of the IOLW control octet

Figure D.2.: IOLW Safety PDUs with one DSLOT and cycle time of 5 ms (2 retries), back to embedded Fig. 5.2.

From FS-W-Master:

MAC	CRC signature	Control&MCnt*	TrackSlotNr	FS-W-PDout
Across FS-W-PDout, TrackSlotNr, Control&MCnt, CRC	Across FS-W-PDout, TrackSlotNr, Control&MCnt	Including 5 bit counter	FS-W-Master track and slot number	FS-W-PDout
4/8 octets	4 octets	1 octet	1 octet	max. 40 octets

Possible payload = 64 octets
One FS-W-Device per track

Possible payload = 64/4 octets
4 FS-W-Devices shared
equally per track
→ 16 octets/FS-W-Device

From FS-W-Device
(one DSlot):

FS-W-PDin	TrackSlotNr	Control&MCnt*	CRC signature	MAC
FS-W-PDin	FS-Master TrackSlotNr inverted	Including 5 bit counter inverted	Across FS-W-PDin, TrackSlotNr, Contol&MCnt	Across FS-W-PDin, TrackSlotNr, Control&MCnt, CRC
max. 18 octets	1 octet	1 octet	4 octets	4 octets

Possible payload = 28 octets

*IOLW Safety Control&MCnt (management count), which is independent of the IOLW control octet

Figure D.3.: IOLW Safety PDU with two DSLOTs and cycle time of 10 ms (2 retries for each DSLOT package), back to embedded Fig. 5.3.

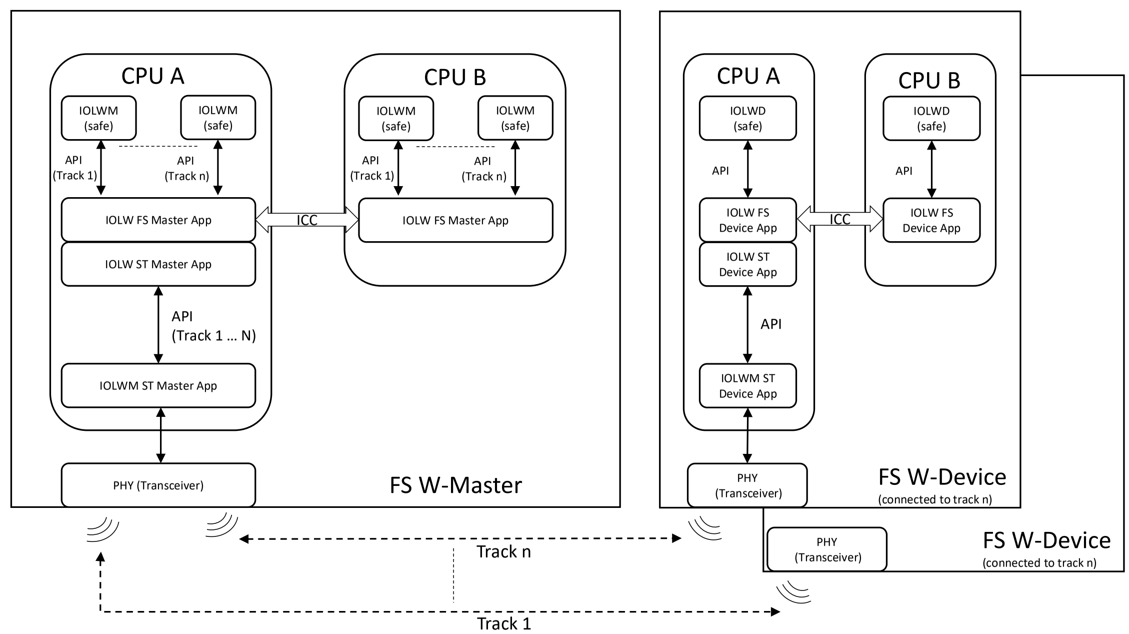


Figure D.4.: System context of IOLW Safety system extension library [148, 149], back to embedded Fig. 6.2.

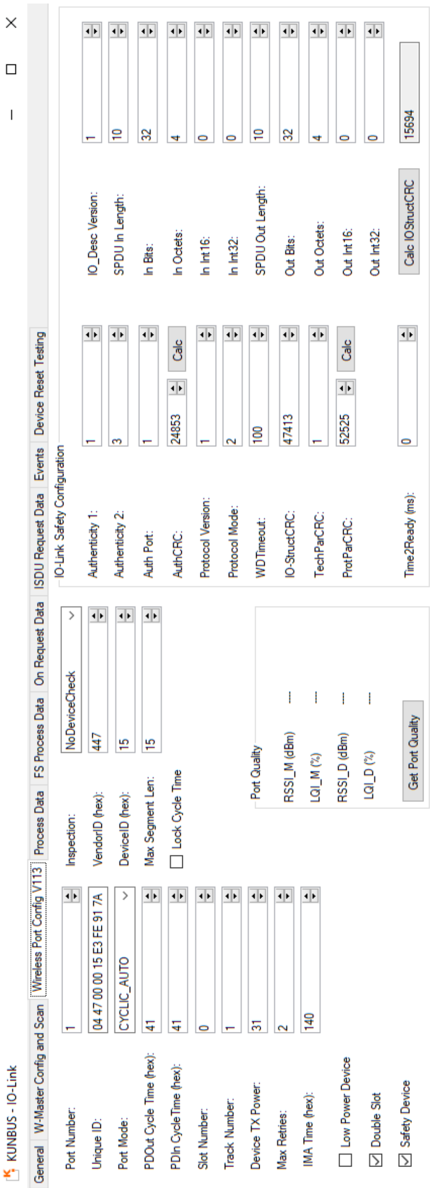


Figure D.5.: IOLWS Dedicated tool configuration for one DSLOT [152].

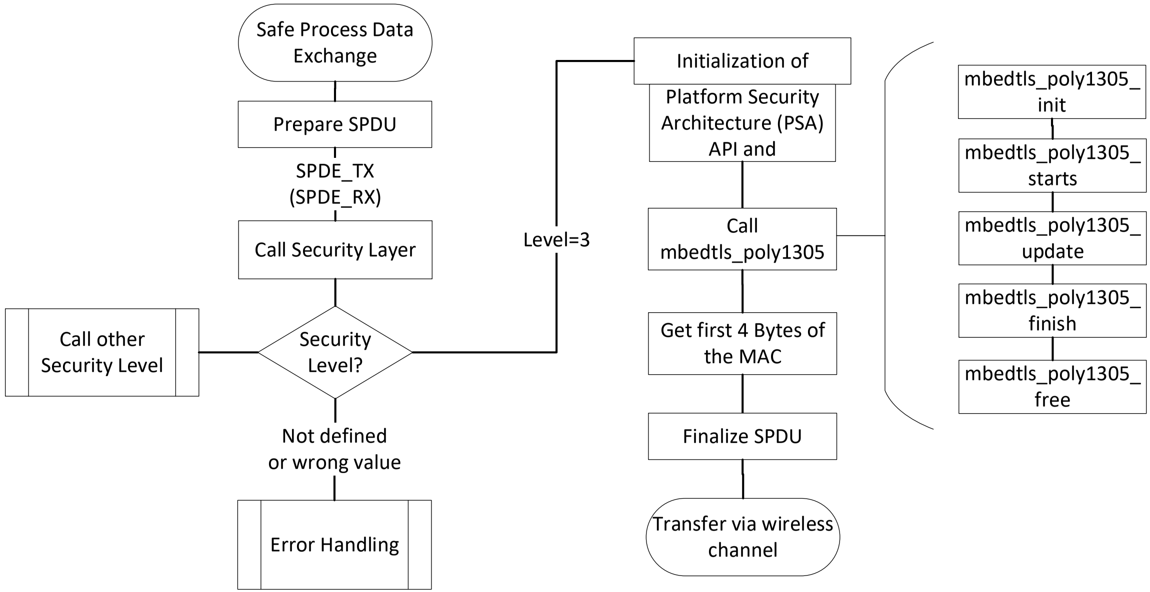


Figure D.6.: IOLW security layer example for a MAC implementation using mbedTLS with Poly1305.

Bibliography

[1] IO-Link Interface and System - Specification Version 1.1.3, June 2019, Order No: 10.002. [Online]. Available: https://io-link.com/share/Downloads/Package-2020/IOL-Interface-Spec_10002_V113_Jun19.pdf

[2] PROFIBUS Nutzerorganisation e.V., "IO-Link System Description – Technology and Application," 2018. [Online]. Available: https://io-link.com/share/Downloads/At-a-glance/IO-Link_System_Description_eng_2018.pdf

[3] T. R. Doebbert, C. Cammin, and G. Scholl, "Safety Architecture Proposal for Low-Latency Sensor/Actuator Networks using IO-Link Wireless," *IEEE Access*, vol. 10, pp. 3030–3044, 2022.

[4] R. Heynicke, D. Krush, C. Cammin, G. Scholl, B. Kaercher, J. Ritter, P. Gaggero, and M. Rentschler, "IO-Link Wireless enhanced factory automation communication for Industry 4.0 applications," *Journal of Sensors and Sensor Systems*, vol. 7, p. 131–142, 2018. [Online]. Available: https://www.j-sens-sens-syst.net/7/131/2018/

[5] M. Rentschler, W. Ladruner, P. Gaggero, E. Zigman, D. Wolberg, O. Blonsky, R. Kaptur, G. Scholl, R. Heynicke, J. Ritter, and B. Kaercher, "IO-Link Wireless: The new Standard for Factory Automation," in *2018 Wireless Congress*, 2018, pp. 1–13.

[6] R. Heynicke, D. Krush, G. Scholl, B. Kaercher, J. Ritter, P. Gaggero, and M. Rentschler, "IO-Link Wireless Enhanced Sensors and Actuators for Industry 4.0 Networks," in *Proceedings - AMA Conferences 2017 with SENSOR and IRS2*, 2017, p. 134–138.

[7] D. Wolberg, M. Rentschler, and P. Gaggero, “Simulative performance analysis of IO-Link Wireless,” in *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)*, 2018, pp. 1–10.

[8] Doebbert, Thomas Robert and Cammin, Christoph and Scholl, Gerd and Kärcher, Bernd, “Study of a Safe and Secure Ecosystem based on IO-Link Wireless and a 5G Campus Network,” in *2021 26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2021, pp. 01–04.

[9] M. Rentschler, “Roaming in wireless factory automation networks,” in *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2017, pp. 1–4.

[10] C. Cammin, D. Krush, H. Wattar, R. Heynicke, and G. Scholl, “Base Station Antenna Placement of Wireless Sensor/Actuator Networks in Manufacturing Cells,” in *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2019, pp. 1317–1320.

[11] C. Cammin, D. Krush, R. Heynicke, G. Scholl, C. Schulze, S. Thiede, and C. Herrmann, “Coexisting Wireless Sensor Networks in Cyber-Physical Production Systems,” in *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2016, pp. 1–4.

[12] T. Solzbacher, R. Heynicke, and G. Scholl, “Parallel processing of RSSI signals for gapless monitoring of the 2.45 GHz ISM band,” *tm - Technisches Messen*, vol. 85, pp. s124 – s128, 01 Sep. 2018. [Online]. Available: https://www.degruyter.com/view/journals/teme/85/s1/article-ps124.xml

[13] D. Krush, C. Cammin, T. R. Doebbert, R. Heynicke, and G. Scholl, “Coexistence Management Methods and Tools for IO-Link Wireless,” in *2021 17th IEEE International Conference on Factory Communication Systems (WFCS)*, 2021, pp. 151–158.

[14] T. R. Doebbert, D. Krush, C. Cammin, J. Jockram, R. Heynicke, and G. Scholl, “IO-Link Wireless Device Cryptographic Performance and Energy Efficiency,” in *2021 22nd IEEE International Conference on Industrial Technology (ICIT)*, vol. 1, 2021, pp. 1106–1112.

[15] T. R. Doebbert, C. Cammin, and G. Scholl, “Precision Measurement of the Application-dependent Current Consumption of a Wireless Transceiver Chip,” in *SMSI 2021 - Measurement Science*, May 2021, pp. 281–282.

[16] T. R. Doebbert, F. Fischer, D. Merli, and G. Scholl, "On the Security of IO-Link Wireless Communication in the Safety Domain," in *2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2022, pp. 1–8.

[17] C. Cammin, D. Krush, R. Heynicke, and G. Scholl, "Test method for narrowband F/TDMA-based wireless sensor/actuator networks including radio channel emulation in severe multipath environments," *Journal of Sensors and Sensor Systems*, vol. 7, p. 183–192, 2018. [Online]. Available: https://www.j-sens-sens-syst.net/7/183/2018/

[18] ——, "Employing correlation for wireless components and device characterization in reverberation chambers," *Journal of Sensors and Sensor Systems*, vol. 8, p. 185–194, 2019. [Online]. Available: https://jsss.copernicus.org/articles/8/185/2019/

[19] ——, "Reproducibility of Fading Propability in a Reverberation Chamber for Wireless Device Testing," in *2019 IEEE Radio and Antenna Days of the Indian Ocean (RADIO)*, 2019, pp. 1–2.

[20] ——, "Deep Fading in a Reverberation Chamber for Wireless Device Testing," *IOP Conference Series: Materials Science and Engineering*, vol. 766, p. 012004, Mar. 2020. [Online]. Available: https://doi.org/10.1088/1757-899x/766/1/012004

[21] ——, "Sensing Reverberation Chamber Loading for IO-Link Wireless Testing," in *2021 International Conference on Electromagnetics in Advanced Applications (ICEAA)*, 2021, pp. 87–91.

[22] IO-Link Wireless System Extensions - Specification Version 1.1.3, June 2023, Order No: 10.112. [Online]. Available: https://io-link.com/share/Downloads/System-Extensions/IOLW-Spec_V1.1.3Jun23+Corrigendum_1.pdf

[23] IEC 61131-9:2022, *Programmable controllers - Part 9: Single-drop digital communication interface for small sensors and actuators (SDCI)*, 2022. [Online]. Available: https://webstore.iec.ch/publication/68534

[24] International Electrotechnical Commission. (last access: 19 September 2023). [Online]. Available: https://www.iec.ch/functional-safety

[25] IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems*, 2010. [Online]. Available: https://webstore.iec.ch/publication/5515

[26] ISO 26262-1:2018, *Road vehicles — Functional safety — Part 1: Vocabulary.* Vernier, Geneva, Switzerland: International Organization for Standardization, 2018. [Online]. Available: https://www.iso.org/standard/68383.html

[27] ISO 13849-1:2023, *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*, 2023. [Online]. Available: https://www.iso.org/standard/69883.html

[28] IEC 62061:2021, *Safety of machinery - Functional safety of safety-related control systems*, 2021. [Online]. Available: https://webstore.iec.ch/publication/59927

[29] IEC 61784-3:2021, *Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions*, 2021. [Online]. Available: https://webstore.iec.ch/publication/62095

[30] IO-Link Safety System Extensions with SMI - Specification V1.1.3, March 2022, Order No: 10.092. [Online]. Available: https://io-link.com/share/Downloads/System-Extensions/IO-Link_Safety_System-Extensions_10092_V113_Mar22.pdf

[31] M. Ghadhab, J. Kaienburg, M. Süßkraut, and C. Fetzer, "Is software coded processing an answer to the execution integrity challenge of current and future automotive software-intensive applications?" in *Advanced Microsystems for Automotive Applications 2015: Smart Systems for Green and Automated Driving.* Springer, 2016, pp. 263–275.

[32] M. Süßkraut, A. Schmitt, and J. Kaienburg, "Safe program execution with diversified encoding," in *Proceedings of the 13th embedded world conference*, 2015.

[33] D. Kleidermacher and M. Kleidermacher, *Embedded Systems Security: Practical Methods for Safe and Secure Software and Systems Development*, 1st ed. USA: Newnes, 2012.

[34] IEC 62443-3-3:2013, "Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels," 2013. [Online]. Available: https://webstore.iec.ch/publication/7033

[35] Ross Anderson, *What Is Security Engineering?* John Wiley & Sons, Ltd, 2020. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119644682.ch1

[36] J. Horalek and V. Sobeslav, "Cybersecurity analysis of IoT networks," in *Computational Collective Intelligence: 11th International Conference, ICCCI 2019, Hendaye, France, September 4–6, 2019, Proceedings, Part II 11*. Springer, 2019, pp. 488–499.

[37] Texas Instruments. Building your application with security in mind - Guide to embedded security. Application Note. [Online]. Available: https://www.ti.com/lit/ml/swpb020e/swpb020e.pdf?ts=1611941696435&ref_url=https%253A%252F%252Fwww.ti.com%252Ftechnologies%252Fsecurity%252Foverview.html

[38] S. Lin and D. Costello Jr, "Low Density Parity Check codes," in *Error Control Coding*. Prentice hall, Pearson Education Inc., 2004, pp. 871–875.

[39] William Wesley Peterson and Edward J Weldon, *Error-correcting codes*. MIT press, 1972.

[40] F. Schiller, D. Judd, P. Supavatanakul, T. Hardt, and F. Wieczorek, "Enhancement of safety communication model: Preserving the black channel concept," *at - Automatisierungstechnik*, vol. 70, p. 38–52, 2022. [Online]. Available: https://doi.org/10.1515/auto-2021-0098

[41] M. Bossert, *Kanalcodierung*, ser. Informationstechnik Series. Vieweg+Teubner Verlag, 1998. [Online]. Available: https://books.google.de/books?id=BmxGCF9wsGcC

[42] H. Wacker and J. Boercsoek, "Binomial and monotonic behavior of the probability of undetected error and the 2-r-bound," in *WTOC*, vol. 7. Citeseer, 2008, pp. 188–197.

[43] PROFIBUS Nutzerorganisation e.V. Profisafe – Profile for Safety Technology on PROFIBUS and PROFINET. Draft in PI Review. [Online]. Available: www.profibus.com

[44] H. Barthel (Siemens AG), "System, device and method for determining the reliability of data carriers in a failsafe system network," Patent US6 907 542B2. [Online]. Available: https://patentimages.storage.googleapis.com/c3/22/2e/7acc1d540c54aa/US6907542.pdf

[45] IEC 61784-3-3:2021, *Industrial communication networks - Profiles - Part 3-3: Functional safety fieldbuses - Additional specifications for CPF 3*, 2021.

[46] IEC 61131-2:2017, *Industrial-process measurement and control - Programmable controllers - Part 2: Equipment requirements and tests*, 2017. [Online]. Available: https://webstore.iec.ch/publication/31007

[47] ETG.5100 Safety over EtherCAT Specification V1.2, March 2011. [Online]. Available: https://www.ethercat.org/en/downloads/downloads_E42C804F25A140149603A793EA42297E.htm

[48] H.T. Hannen, "Beitrag zur Analyse sicherer Kommunikationsprotokolle im industriellen Einsatz," Ph.D. dissertation, 2012. [Online]. Available: https://kobra.uni-kassel.de/bitstream/handle/123456789/2012092641851/DissertationHeinrichTheodorHannen.pdf?sequence=3

[49] D. Etz, T. Frühwirth, A. Ismail, and W. Kastner, "Simplifying functional safety communication in modular, heterogeneous production lines," in *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)*, 2018, pp. 1–4.

[50] H. J. Koerber, H. Wattar, and G. Scholl, "Modular Wireless Real-Time Sensor/Actuator Network for Factory Automation Applications," *IEEE Transactions on Industrial Informatics*, vol. 3, p. 111–119, May 2007.

[51] G. Scholl, R. Heynicke, D. Krueger, and R. Hornung, "Wireless automation," in *Proceedings SENSOR 2013*, May 2013, pp. 379–383. [Online]. Available: https://www.ama-science.org/proceedings/details/1529

[52] A. Frotzscher, U. Wetzker, M. Bauer, M. Rentschler, M. Beyer, S. Elspass, and H. Klessig, "Requirements and current solutions of wireless communication in industrial automation," in *2014 IEEE International Conference on Communications Workshops (ICC)*, Jun. 2014, p. 67–72.

[53] ifak e.V. Magdeburg, "Aspects of Dependability Assessment in ZDKI Technical Group 1," 2017. [Online]. Available: https://industrial-radio-lab.eu/download/812/

[54] ——, "Requirement Profiles in ZDKI Technical Group 1," 2017. [Online]. Available: https://industrial-radio-lab.eu/download/807/

[55] J. Jasperneite, T. Sauter, and M. Wollschlaeger, "Why We Need Automation Models: Handling Complexity in Industry 4.0 and the Internet of Things," *IEEE Industrial Electronics*

Magazine, vol. 14, pp. 29–40, 2020. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9044672

[56] VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V., "Position Paper - Wireless Technologies for Industrie 4.0," 2018. [Online]. Available: https://shop.vde.com/de/vde-positionspapier-funktechnologien-fuer-industrie-40

[57] Dionísio, R. and Lolić, T. and Torres, P., "Electromagnetic Interference Analysis of Industrial IoT Networks: From Legacy Systems to 5G," in *2020 IEEE Microwave Theory and Techniques in Wireless Communications (MTTW)*, vol. 1, 2020, pp. 41–46.

[58] A. Alabbasi, T. Dudda, Z. Zou, and J. Kronander, "5G Toolbox for Realizing Industrial Automation," in *2019 IEEE 2nd 5G World Forum (5GWF)*, 2019, pp. 512–515.

[59] A. Aijaz, "Private 5G: The Future of Industrial Wireless," *IEEE Industrial Electronics Magazine*, vol. 14, no. 4, pp. 136–145, 2020.

[60] M. Baker and M. Poikselkä, "5G Releases 16 and 17 in 3GPP," Nokia Bell Labs CTO, Standardization & Research, Tech. Rep., 2020-04-20.

[61] VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V., "VDI/VDE 2185 Blatt 1:2020-08 Radio based communication in industrial automation - Requirements and principles," 2020, (last access: 19th September 2023). [Online]. Available: https://www.beuth.de/de/technische-regel/vdi-vde-2185-blatt-1/319538762

[62] ZigBee Alliance Board of Directors, "ZigBee Specification," 2015-08-05. [Online]. Available: https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf

[63] EnOcean Alliance, "Building Smarter Connectivity," (last access: 19th September 2023). [Online]. Available: https://www.enocean-alliance.org/

[64] IEC 62591:2016, *Industrial networks - Wireless communication network and communication profiles - WirelessHART*, 2016. [Online]. Available: https://webstore.iec.ch/publication/24433

[65] Emerson Automation Solutions, "A Comparison of WirelessHART and ISA100.11a," 2012, (last access: 19th September 2023). [Online]. Available: http://www2.emersonprocess.com/siteadmincenter/PM%20Central%20Web%20Documents/wirelesshart-vs-isa-WP.pdf

[66] IEC 62734:2019, *Industrial networks - Wireless communication network and communication profiles - ISA 100.11a*, 2019. [Online]. Available: https://standards.globalspec.com/std/13394469/iec-62734

[67] IEC 62601:2015, *Industrial networks - Wireless communication network and communication profiles - WIA-PA*, 2015. [Online]. Available: https://standards.globalspec.com/std/10041133/din-en-62601

[68] I. Verhappen, "WIA-PA and WIA-FA to be added to IEC wireless standards," 2016, (last access: 19th September 2023). [Online]. Available: https://www.controlglobal.com/articles/2016/wia-pa-and-wia-fa-to-be-added-to-iec-wireless-standards/

[69] IEC 62948:2017, *Industrial networks - Wireless communication network and communication profiles - WIA-FA*, 2017. [Online]. Available: https://webstore.iec.ch/publication/32718

[70] S. Dietrich, G. May, O. Wetter, H. Heeren, and G. Fohler, "Performance indicators and use case analysis for wireless networks in factory automation," in *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2017, pp. 1–8.

[71] W. Liang, M. Zheng, J. Zhang, H. Shi, H. Yu, Y. Yang, S. Liu, W. Yang, and X. Zhao, "WIA-FA and Its Applications to Digital Factory: A Wireless Network Solution for Factory Automation," *Proceedings of the IEEE*, vol. 107, pp. 1053–1073, 2019.

[72] B. M. Otten, R. Weidner, and A. Argubi-Wollesen, "Evaluation of a Novel Active Exoskeleton for Tasks at or Above Head Level," *IEEE Robotics and Automation Letters*, vol. 3, pp. 2408–2415, 2018.

[73] Z. Yao, C. Linnenberg, R. Weidner, and J. Wulfsberg, "Development of A Soft Power Suit for Lower Back Assistance," in *2019 International Conference on Robotics and Automation (ICRA)*, 2019, pp. 5103–5109.

[74] J. Wollert, "Wireless systems for machinery safety," in *2015 16th International Conference on Research and Education in Mechatronics (REM)*, 2015, pp. 88–91.

[75] J. Hoffmann, D. Kuschnerus, T. Jones, and M. Hubner, "Towards a Safety and Energy Aware Protocol for Wireless Communication," in *2018 13th International Symposium on Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC)*, 2018, pp. 1–6.

[76] F. Kaestner, D. Kuschnerus, C. Spiegel, B. Janssen, and M. Huebner, “Design of an efficient Communication Architecture for Cyber-Physical Production Systems,” in *2018 IEEE 14th International Conference on Automation Science and Engineering (CASE)*, 2018, pp. 829–835.

[77] “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” 2008. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc5280

[78] ISO/IES 18092:2013, “Information technology — Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1),” 2013.

[79] ISO/IEC 14443-1:2018, “Identification cards — Contactless integrated circuit cards — Proximity cards — Part 1: Physical characteristics,” 2018. [Online]. Available: https://www.iso.org/standard/73596.html

[80] ISO/IEC 14443-2:2020, *Cards and security devices for personal identification — Contactless proximity objects — Part 2: Radio frequency power and signal interface — Technical Corrigendum 1*, 2020. [Online]. Available: https://www.iso.org/standard/73597.html

[81] ISO/IEC 15693-1:2018, “Cards and security devices for personal identification — Contactless vicinity objects — Part 1: Physical characteristics,” 2018. [Online]. Available: https://www.iso.org/standard/70837.html

[82] ISO/IEC 15693-2:2019, *Cards and security devices for personal identification — Contactless vicinity objects — Part 2: Air interface and initialization*, 2019. [Online]. Available: https://www.iso.org/standard/73601.html

[83] ISO/IEC 15693-3:2019, *Cards and security devices for personal identification — Contactless vicinity objects — Part 3: Anticollision and transmission protocol*, 2019. [Online]. Available: https://www.iso.org/standard/73602.html

[84] NIST, “Recommendation for Key Management - Part 1: General,” May 2020, NIST Special Publication 800-57 Part 1 Revision 5. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

[85] ——, “Recommendation for Key Management - Part 2: Best Practices for Key Management Organizations,” May 2019, NIST

Special Publication 800-57 Part 2 Revision 1. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt2r1.pdf

[86] ——, “Recommendation for Key Management - Part 3: Application-Specific Key Management Guidance,” January 2015, NIST Special Publication 800-57 Part 3 Revision 1. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf

[87] PROFIBUS Nutzerorganisation e.V. (2018-12-01) OPC Unified Architecture for IO-Link Companion Specification, Release 1.0. [Online]. Available: https://io-link.com/share/Downloads/OPC_UA/OPC-UA_for_IO-Link_10212_V10_Dec18.pdf

[88] NXP Semiconductors. Whitepaper Functional Safety and Security, Essential and Complementary Disciplines for Modern Systems. (last access: 19th September 2023). [Online]. Available: https://www.nxp.com/docs/en/white-paper/SAFETYSECWPA4.pdf

[89] NIST, “Approved Key Establishment Techniques for FIPS PUB 140-2 Draft,” 2021-10-12, Security Requirements for Cryptographic Modules. [Online]. Available: https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402annexd.pdf

[90] ——, “Recommendation for Cryptographic Key Generation,” June 2020, NIST Special Publication 800-133 Revision 2. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-133r2

[91] F. Wieczorek, F. Schiller, R. Fiat, and T. Störtkuhl, “Zusammenhang von Security und Funktionaler Sicherheit,” *atp magazin*, vol. 55, no. 06, pp. 40–46, 2013.

[92] N. Ferguson, B. Schneier, and T. Kohno, *Cryptography engineering: design principles and practical applications.* John Wiley & Sons, 2011. [Online]. Available: https://onlinelibrary.wiley.com/doi/book/10.1002/9781118722367

[93] B. Solzbacher, T. Doebbert, C. Cammin, and G. Scholl, “Fast Spectrum Monitoring System for the 2.45 GHz ISM-Band Based on Standard RF-Transciever Chips,” in *Sensors and Measuring Systems; 21th ITG/GMA-Symposium*, 2022, pp. 1–7.

[94] F. Schiller, F. Wieczorek, “Safety-Analyse für Security-geschützte Kommunikation,” *atp magazin*, p. 86–92, Apr. 2020, (in German).

[95] A. Horch, H. Hannen, S. Ditting, H. Schween, K. Wagner, and Hima, "Verschlüsselung sicherer Kommunikation: Ein Widerspruch?" *atp magazin*, vol. 61, no. 6-7, pp. 93–99, 2019.

[96] IEC 62280:2014, *Railway applications - Communication, signalling and processing systems - Safety related communication in transmission systems*, 2014, (last access: 11 October 2023). [Online]. Available: https://webstore.iec.ch/publication/6749

[97] PHYTEC, *phyWAVE-CC26xx Hardware Manual*, Aug. 2018, Manual. [Online]. Available: https://www.phytec.eu/fileadmin/user_upload/images/content/1.Products/IoT/L-824e_1.pdf

[98] Texas Instruments, "Cryptographic Performance and Energy Efficiency on SimpleLink CC13x2/CC26x2 Wireless MCUs," Tech. Rep., 2020, Application Report SWRA667. [Online]. Available: https://www.ti.com/lit/an/swra667/swra667.pdf

[99] ——. SimpleLink CC2650 wireless MCU LaunchPad Development Kit. [Online]. Available: https://www.ti.com/tool/LAUNCHXL-CC2650?keyMatch=CC26X2R%20LAUNCHPAD%20DEVELOPMENT%20KIT

[100] Keysight, *N6700 Modular Power System Family*, datasheet. [Online]. Available: https://www.keysight.com/de/de/assets/7018-05460/data-sheets/5992-1880.pdf

[101] Rohde & Schwarz, "RT-ZVCxx Multi-Channel Power Probe Specifications," June 2018. [Online]. Available: https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_common_library/dl_brochures_and_datasheets/pdf_1/RT-ZVCxx_dat-sw_en_5214-7058-22_v0501.pdf

[102] ——, "RT-ZVC Multi-Channel Power Probe User Manual - Version 03," 2018. [Online]. Available: https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_common_library/dl_manuals/gb_1/r/rt_zvc/RT-ZVC_UserManual_en_03.pdf

[103] Lawrence E. Basshamm III, "The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)," Computer Security Devision, Tech. Rep., Nov. 2002, Algorithm Validation Testing Requirements - Block Ciphers - Advanced Encryption Standard Algorithm (AES). [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Algorithm-Validation-Program/documents/aes/AESAVS.pdf

[104] S. Frankel, R. Glenn, S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPsec," RFC 3602, Sep. 2003. [Online]. Available: https://www.rfc-editor.org/rfc/rfc3602

[105] R. Housley, "Using Advanced Encryption Standard (AES) Counter Mode with IPsec Encapsulating Security Payload (ESP)," RFC 3686, Jan. 2004. [Online]. Available: https://www.rfc-editor.org/rfc/rfc3686

[106] NIST, "Recommendation for Block Cipher Modes of Operation: Methods and Techniques," 2001, NIST Special Publication 800-38A. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

[107] D. Whiting, R. Housley, and N. Ferguson, "Counter with CBC-MAC (CCM)," RFC 3610, Sep. 2003. [Online]. Available: https://rfc-editor.org/rfc/rfc3610.txt

[108] T. R. Doebbert, C. Cammin, and G. Scholl, "Precision measurement of the application-dependent current consumption of a wireless transceiver chip in the time and frequency domain," *Journal of Sensors and Sensor Systems*, vol. 11, p. 149–159, 2022. [Online]. Available: https://jsss.copernicus.org/articles/11/149/2022/

[109] S. Ziegler, R. C. Woodward, H. H.-C. Iu, and L. J. Borle, "Current Sensing Techniques: A Review," *IEEE Sensors Journal*, vol. 9, no. 4, pp. 354–376, Apr. 2009, conference Name: IEEE Sensors Journal.

[110] M. Sanoh, A. Mikata, K. Tokuno, M. Hanazawa, and H. Kakitani, "A calibration method for a commercial coaxial shunt at high pulse current," in *29th Conference on Precision Electromagnetic Measurements (CPEM 2014)*, Aug. 2014, pp. 630–631, ISSN: 2160-0171.

[111] Rohde & Schwarz, "R&S NGM200 Power Supply Series Data Sheet-Version 4.00," 2023, (last access: 2021-10-05). [Online]. Available: https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/pdm/cl_brochures_and_datasheets/data_sheet/3609_1685_32/NGM200_dat_en_3609-1685-32_v0400.pdf

[112] Keysight, "Keysight 3458A Multimeter User's Guide," 2023, (last access: 2023-10-24). [Online]. Available: https://www.keysight.com/de/de/assets/7018-06796/data-sheets/5965-4971.pdf

[113] JCGM 100:2008, *Guide to the Expression of Uncertainty in Measurement*, 2008.

[114] F. Wolf, J. Kruse, and R. Ernst, “Timing and power measurement in static software analysis,” *Microelectronics Journal*, vol. 33, no. 1, pp. 91–100, Jan. 2002. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0026269201001082

[115] T. Laopoulos, P. Neofotistos, C. Kosmatopoulos, and S. Nikolaidis, “Measurement of current variations for the estimation of software-related power consumption [embedded processing circuits],” *IEEE Transactions on Instrumentation and Measurement*, vol. 52, no. 4, pp. 1206–1212, Aug. 2003, Conference Name: IEEE Transactions on Instrumentation and Measurement.

[116] D. Macii and D. Petri, “Accurate Software-Related Average Current Drain Measurements in Embedded Systems,” *IEEE Transactions on Instrumentation and Measurement*, vol. 56, no. 3, pp. 723–730, Jun. 2007, conference Name: IEEE Transactions on Instrumentation and Measurement.

[117] R. Jevtic and C. Carreras, “Power Measurement Methodology for FPGA Devices,” *IEEE Transactions on Instrumentation and Measurement*, vol. 60, no. 1, pp. 237–247, Jan. 2011, conference Name: IEEE Transactions on Instrumentation and Measurement.

[118] Z. Nakutis, “A Current Consumption Measurement Approach for FPGA-Based Embedded Systems,” *IEEE Transactions on Instrumentation and Measurement*, vol. 62, no. 5, pp. 1130–1137, May 2013, conference Name: IEEE Transactions on Instrumentation and Measurement.

[119] Stackpole Electronics, Inc., “RNCF Series - Precision Thin Film Chip Resistor - Data sheet,” 2021, (last access: 2021-10-15). [Online]. Available: https://www.seielect.com/catalog/sei-rncf.pdf

[120] C. Boyd, A. Mathuria, and D. Stebila, *Protocols for Authentication and Key Establishment*, ser. Information Security and Cryptography. Springer Berlin Heidelberg, 2019. [Online]. Available: https://books.google.de/books?id=T8-8DwAAQBAJ

[121] E. Milanov, “The RSA Algorithm,” 2009-06-03. [Online]. Available: https://sites.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf

[122] R. L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” *Commun. ACM*, vol. 21, p. 120–126, Feb. 1978. [Online]. Available: https://doi.org/10.1145/359340.359342

[123] A. Menezes, "The Elliptic Curve Discrete Logarithm Problem: State of the Art," *IWSEC*, p. 218, 2008.

[124] Bundesamt für Sicherheit in der Informationstechnik (BSI), "BSI TR-02102-1 Cryptographic Mechanisms: Recommendations and Key Lengths," 2021, Version: 2023-1. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf

[125] N. Mehibel and M. Hamadouche, "A new approach of elliptic curve diffie-hellman key exchange," in *2017 5th International Conference on Electrical Engineering - Boumerdes (ICEE-B)*, 2017, pp. 1–6.

[126] R. Alvarez, C. Caballero-Gil, J. Santonja, and A. Zamora, "Algorithms for Lightweight Key Exchange," *Sensors*, vol. 17, 2017. [Online]. Available: https://www.mdpi.com/1424-8220/17/7/1517

[127] C. Costello and P. Longa, "FourQ: four-dimensional decompositions on a Q-curve over the Mersenne prime," Cryptology ePrint Archive, Report 2015/565, 2015. [Online]. Available: https://ia.cr/2015/565

[128] Certicom Research, E. Buckley, "SEC 4: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV)," 2014. [Online]. Available: https://www.secg.org/draft-sec4-1.2.pdf

[129] P. Porambage, P. Kumar, C. Schmitt, A. Gurtov, and M. Ylianttila, "Certificate-Based Pairwise Key Establishment Protocol for Wireless Sensor Networks," in *2013 IEEE 16th International Conference on Computational Science and Engineering*, 2013, pp. 667–674.

[130] Lee, Eric and Defence Science and Technology Organisation Fishermans Bend (Australia) Aearospace DIV, "Investigation of using Radio Frequency Identification (RFID) system for gear tooth crack detection," 2014.

[131] C. Govender and B. van Niekerk, "Secure Key Exchange by NFC for Instant Messaging," in *2021 Conference on Information Communications Technology and Society (ICTAS)*, 2021, pp. 27–33.

[132] EnOcean Alliance, "System Specification - Security of EnOcean Radio Networks V 3.01," 2020, (last access: 19th September 2023). [Online]. Available: https://www.enocean-alliance.org/sec/

[133] J. Song, R. Poovendran, J. Lee, and T. Iwata, "The AES-CMAC Algorithm," Internet Requests for Comments, Network Working Group, Tech. Rep., Jun. 2006. [Online]. Available: https://www.rfc-editor.org/rfc/rfc4493.txt

[134] S. Kent, "Security Architecture for the Internet Protocol," RFC 2401, Nov. 1998. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc2401

[135] T. Ylonen, "The Secure Shell (SSH) Protocol Architecture," RFC 4251, Jan. 2006. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc4251

[136] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," RFC 8446, Aug. 2018. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc8446

[137] Seuss, Dr, *Horton hatches the egg*, 1st ed., 1940.

[138] Texas Instruments. (2019) CC26XX SimpleLink Multistandard Wireless MCU header and source files. [Online]. Available: https://software-dl.ti.com/lprf/ble5stack-docs-latest/docs/tidrivers/doxygen/html/dir_f384823999e2fe69d74391b31d1a0001.html

[139] NIST, "Recommendation for Block Cipher Mode of Operation: The CCM Mode for Authentication and Confidentiality," May 2004, nIST Special Publication 800-38C. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf

[140] Texas Instruments, "CC2650 SimpleLink Multistandard Wireless MCU datasheet (Rev. B)," 2016. [Online]. Available: https://www.ti.com/document-viewer/CC2650/datasheet

[141] IEEE Std 802.15.4-2020 (Revision of IEEE Std 802.15.4-2015), *Low-Rate Wireless Networks*, 2020.

[142] European Parliament and the Council of the European Union. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 - on machinery, and amending Directive 95/16/EC (recast). [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0042

[143] P. Koopman and T. Chakravarty, "Cyclic redundancy code (crc) polynomial selection for embedded networks," in *International Conference on Dependable Systems and Networks, 2004*, 2004, pp. 145–154.

[144] J. Ray and P. Koopman, "Efficient high hamming distance crcs for embedded networks," in *International Conference on Dependable Systems and Networks (DSN'06)*, 2006, pp. 3–12.

[145] Wolf, J.K. and Blakeney, R.D., “An exact evaluation of the probability of undetected error for certain shortened binary CRC codes,” in *MILCOM 88, 21st Century Military Communications - What’s Possible?'. Conference record. Military Communications Conference*, 1988, pp. 287–292 vol.1.

[146] Endresen, Jan and Vallestad, Anne Elisabeth, “CRC Performance Calculations Brute Forcing the Dual Code -the Forgotten Backdoor,” 10 2014.

[147] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes.* Elsevier, 1977, vol. 16.

[148] Pilz GmbH & Co. KG, “Integration Manual of IOLS Master version v.1.1.1.2673,” 2021.

[149] ——, “Integration Manual of IOLS Device version v.1.1.1.2673,” 2021.

[150] Kunbus GmbH, *Quick Start Guide IO-Link Development Toolkit Master and Device*, 2021.

[151] STMicroelectronics, *STM32F207VE - High-performance Arm Cortex-M3 MCU with 512 Kbytes of Flash memory, 120 MHz CPU, ART Accelerator, Ethernet.* [Online]. Available: https://www.st.com/en/microcontrollers-microprocessors/stm32f207ve.html

[152] Kunbus GmbH, *Quick Start Guide IO-Link Wireless Development Toolkit Device*, 2021.

[153] STMicroelectronics, *STM32F205RE - High-performance Arm Cortex-M3 MCU with 512 Kbytes of Flash memory, 120 MHz CPU, ART Accelerator*. [Online]. Available: https://www.st.com/en/microcontrollers-microprocessors/stm32f205re.html

[154] J. Padgette, J. Bahr, M. Batra, R. Smithbey, L. Chen, and K. Scarfone, “Guide to Bluetooth Security,” 2022-01-19 05:01:00 2022. [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934038

[155] Bernstein, Daniel J, “The Poly1305-AES message-authentication code,” in *International workshop on fast software encryption.* Springer, 2005, pp. 32–49.

[156] ——. A state-of-the-art message-authentication code. [Online]. Available: https://cr.yp.to/mac.html

[157] Mbed TLS Documentation. C library implementing the PSA Cryptography API, cryptographic primitives, X.509 certificate manipulation and the SSL/TLS and DTLS protocols. [Online]. Available: https://mbed-tls.readthedocs.io/projects/api/en/development/api/file/poly1305_8h/

[158] Mbed TLS Github. C library implementing the PSA Cryptography API, cryptographic primitives, X.509 certificate manipulation and the SSL/TLS and DTLS protocols. [Online]. Available: https://github.com/Mbed-TLS/mbedtls/tree/development/library

[159] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020," 2022. [Online]. Available: https://eur-lex.europa.eu/resource.html?uri=cellar:864f472b-34e9-11ed-9c68-01aa75ed71a1.0001.02/DOC_1&format=PDF

[160] I. Farrance and R. Frenkel, "Uncertainty of Measurement: A Review of the Rules for Calculating Uncertainty Components through Functional Relationships." vol. 33, pp. 49–75.

[161] A. E. Vallestad and J. Endresen, "Exact Probability of Undetected Error (Pude) for shortened linear block codes. Brute-force calculation in FPGA logic," 2015.

[162] G. Castagnoli, S. Brauer, and M. Herrmann, "Optimization of cyclic redundancy-check codes with 24 and 32 parity bits," *IEEE Transactions on Communications*, vol. 41, no. 6, pp. 883–892, 1993.