IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 8, 2021, accepted November 15, 2021, date of publication November 16, 2021,
date of current version January 10, 2022.

Digital Object Identifier 10.1109/ACCESS.2021.3128758

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

THOMAS R. DOEBBERT, CHRISTOPH CAMMIN, (Member, IEEE), AND GERD SCHOLL, (Member, IEEE)
Electrical Measurement Engineering, Helmut Schmidt University, 22043 Hamburg, Germany

Corresponding author: Thomas R. Doebbert (thomas.doebbert@hsu-hh.de)

This work was supported in part by the Federal Ministry of Defense under the dtec.bw Program as "Digital Sensor-2-Cloud Campus Platform (DS2CCP)," in part by the Federal Ministry for Economic Affairs and Energy (BMWi) and the Project Management Juelich (PTJ) under the Wissens- und Technologietransfer durch Patente und Normen (WIPANO) Program, and in part by the Open Access Fund of Helmut Schmidt University/the University of the Federal Armed Forces Hamburg.

ABSTRACT In the field of production automation, IO-Link Wireless (IOLW) offers energy-efficient and cost-effective solutions for networking wireless sensors and actuators close to the machines on the industrial shop-floor. In this paper, a concept is presented to enhance IOLW with security-for-safety and safety features in order to make safety critical systems in industrial environments with performance characteristics dedicated to demanding applications feasible. As data security is of paramount importance, security mechanisms already implemented in other wireless protocols are investigated and security-for-safety mechanisms for IOLW are introduced. Potential cryptographic algorithms are evaluated for IOLW with respect to energy consumption and timing. Taking performance parameters into account, which are crucial for industrial manufacturing processes, a safety protocol data unit (SPDU) is described and evaluated for different payload length and cycle times. Finally, an outlook towards the implementation of a demonstrator setup completes this work.

INDEX TERMS IO-Link Wireless, IO-Link, functional safety, wireless safety, wireless security, industrial wireless networks, wireless sensor networks, safety critical systems, IIoT, industry 4.0.

I. INTRODUCTION

To enhance the IO-Link Wireless (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 [1]. In the last decades, wireless communication systems have become a fundamental pillar of modern industrial communication realizations (e.g. [2]–[8]). Even though cellular mobile communication like 2G, 3G, 4G and in particular 5G or beyond are proposed, e.g. in [9]–[13], 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 [14], e.g. building automation (ZigBee [15], EnOcean [16]), process automation (wirelessHART [17], [18], ISA 100a [18], [19], WIA-PA [20], [21]) or factory automation (IO-Link Wireless [22], [23], WIA-FA [21], [24]). 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 [25]. 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. Moreover, no further contribution towards a IOLW Safety concept is known to have been established or published yet. To the authors' best knowledge, no further contribution towards a IOLW Safety concept is neither known as established nor been published. As main aspect, the IOLW Safety concept shall be fully compatible with IO-Link Safety and the safety communication model IEC 61784-3 [50] 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.

This work begins in Section II with potential applications for IOLW Safety and is followed by Section III with a detailed description of IO-Link Wireless (IOLW) [22], [23], as it offers prerequisites to be enhanced for functional safety

The associate editor coordinating the review of this manuscript and approving it for publication was Diana Gratiela Berbecaru.

applications in the field of factory automation. In Section IV, the most important requirements for real-time wireless safety and security applications are evaluated. Other wireless technologies are characterized with respect to their security measures and potential to be integrated into a IOLW security concept in Section V. An assessment of the automation environment, including the automation hierarchy of IOLW, IO-Link Safety, and potentially IOLW Safety is described and elaborated in Section VI. Out of the obtained findings, necessary prerequisites for demanding safety applications are presented, such as a one-to-one connection in Section VII as well as suitable cryptographic algorithms including their implementation and measurements of the influence on timing and power consumption in Section VIII. These preliminary considerations create the basis to specify prerequisites for demanding safety applications. In Section IX, a safety protocol data unit (SPDU) is proposed. The paper ends with a summary of the main ideas and results.

II. APPLICATIONS FOR IOLW SAFETY

Wireless communication technologies open up great potential in the context of flexible, reconfigurable architecture, for example in the context of Industry 4.0, CPS or the Industrial Internet of Things (IIoT).

In the application field of factory automation, there are already strict requirements, such as extremely low latency times in the range of a few milliseconds and high sensor densities in the order of hundred sensors/actuators per production cell [3], [14], [26]. As outlined e.g. in [27, 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.

Some of these typical factory automation applications are safety-relevant, especially when people and machines interact. Examples include AGVs (e.g in [28]) or an exoskeleton that helps workers process heavy components (e.g. [29], [30]) and can be controlled wirelessly.

As indicated in [27], existing wireless solutions often cannot offer sufficient performance with respect to real-time and reliability requirements. Furthermore, energy concerns of wireless safety proposals [31]–[33] as well as the joint transmission of safety and non-safety data are significant. As a result, the extension of IOLW as a wireless safety solution will be presented here.

III. IO-LINK WIRELESS

Key aspects of IOLW with focus on wireless capabilities, its uniqueness in comparison to other wireless communications protocols are presented in [23, Table 1] and [27, Table 3].

General surveys of IOLW are given in [23], [25], [27], [34], [35] with a focus on roaming in [36], antenna planning in [37], coexistence in [5], [38], [39], security enhancement in [40], [41] or on IOLW testing in [42]–[46]. 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 was developed as an extension of the proven IO-Link standard [47], also known as single-drop digital communication interface (SDCI) or IEC 61131-9 [48]. Therefore, IOLW is mainly intended for sensor/actuator communication below the field-bus level of abstraction within the factory automation structure [23], [47], [48]. IOLW was released in v1.1 in early 2018 [22]. A revised version will be published soon and is currently prepared for an IEC standard [49].

IOLW offers bidirectional wireless communication for (cyclic) process data and (acyclic) on-request data between a wireless master (‘‘W-Master’’) and wireless devices (‘‘W-Devices’’) in a star-shaped topology [22], [23]. The physical layer (PL) is based on Bluetooth Low Energy (BLE) 4.2 and therefore utilizes the 2.4 GHz ISM band with gaussian frequency shift keying (GFSK) modulation [22], [23]. 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 [23], [39]. Wireless bridges (‘‘W-Brides’’) are also standardized to act 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 the parenthesis include 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 [22], [23]. Additionally, roaming capabilities between different W-Masters are implemented [22], [36].

One key feature of IOLW compared to other wireless protocols is its deterministic media access, which is shown in Fig. 1. The communication is divided into cycles and sub-cycles. A cycle lasts at least 5 ms and contains at least three sub-cycles, each of which lasts 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 robustness. In the organization interval (OI), there is a switchover between transmitting and receiving, or vice versa. Five tracks with simultaneous downlinks (DL) followed by an OI and four uplink slots (UL) each (numbered evenly starting from zero) are shown, which corresponds to the maximum configuration level of a W-Master for pure DSlots.

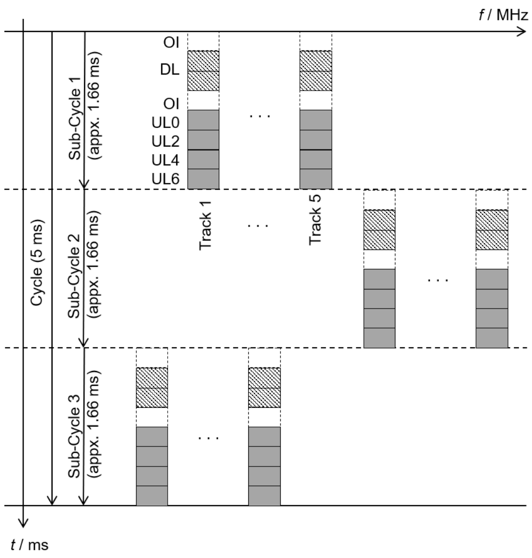

f / MHz
OI
DL
OI
UL0
UL2
UL4
UL6
Sub-Cycle 1 (appx. 1.66 ms)
Cycle (5 ms)
Sub-Cycle 2 (appx. 1.66 ms)
Sub-Cycle 3 (appx. 1.66 ms)
Track 1
. . .
Track 5
t / ms

FIGURE 1. Media access scheme of the IOLW protocol based on [23].

In case of a communication error, the protocol stack repeats the message a configurable number of retries. IOLW promises a latency time of 5 ms with a remaining probability of about 10^{-9} that this latency cannot be realized [22], [35]. However, IOLW is not suitable for safety and/or security applications, yet. In this paper, a conceptual approach to enhance IOLW towards a wireless safety communication solution for safety critical systems is presented.

IV. REQUIREMENTS FOR REAL-TIME WIRELESS SAFETY AND SECURITY APPLICATIONS

Besides functional safety and (cyber-)security requirements, real-time applications demand highly available and robust communication links. In the following, the requirements for a flexible, safe, and secure IOLW enhancement are adapted from IO-Link Safety and the safety communication model IEC 61784-3 [50].

A. WIRELESS ROBUSTNESS

Comprehensive surveys on IOLW addressing wireless robustness are already presented in e.g. [23], [27], [35]. However, a short overview of IOLW features contributing to robust communication is presented here:

- Typically, operation in the 2.4 GHz ISM band results in a high degree of robustness against traditional industrial interferers such as switch mode power supplies, induction heating and relays as the power level of the interfering signal fades out at GHz frequencies (e.g. [2], [3], [51]).
- The usage of narrow-band (in comparison with typical coherence bandwidths of wireless channels in industrial manufacturing environments, e.g. [2], [23], [39], [42]) receivers also employed in BLE systems result in a large system margin. The small bandwidth together with an optimized receiver design results in a narrow noise bandwidth and a high receiver sensitivity of around -94 dBm (e.g. [35], [52]). Thus, radio frequency (RF) messages can even be efficiently received in worst-case Rayleigh fading RF channels [2], [23], [39], [42], [45], [51].
- The PL, media access scheme and complete communication stack is optimized for a very fast exchange for RF messages so that an RF message can be resent twice within a time window of 5 ms (i.e. within the typical coherence time) at different frequencies.
- A 32 bit cyclic redundancy check (CRC) according to [22], which is quite long with respect to the message length, is utilized. This feature was implemented to guarantee that the possibility to receive false positive received messages will remain far below 10^{-9} (e.g [22], [35]).
- The use of a resource-efficient (energy, hardware, software, noise, bandwidth) narrow-band GFSK modulation [22], [23] in conjunction with an optimized frequency hopping algorithm to cope with industrial indoor radio channels and to increase coexistence with other RF communication and measurement systems operating in the same frequency band increases wireless robustness even more (e.g. [5], [22], [23], [35], [39]).

However, to operate especially within the crowded 2.4 GHz ISM band and ensuring wireless coexistence, i.e. to achieve a certain communication performance (e.g. [53]–[57]), is still a challenging task [5], [38], [39]. In [39] highly elaborated methods including tools specifically for the coexistence management for IOLW are described. These are based on the existing specification of IOLW [22] and thus can be directly applied without any modification of the specification or protocol stack. One additional component used to enhance wireless robustness and coexistence is a sophisticated antenna selection and placement for the link planning [37]. Additional methods to increase the coexistence behavior that could be applied to IOLW are e.g. the implementation of an adaptive frequency hopping (e.g. [58], [59]) or the usage of cognitive radio technologies (e.g. [38], [60]–[62]).

B. SECURITY

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 [63, pp. 3-16]. The three fundamental principles in information security are specified as confidentiality, integrity, and availability being commonly referred to as CIA triad, and describe a model to form the main objectives of classical security properties [64, pp. 12-14]. Additionally to the three fundamental principles, authenticity must also be considered. With a strong focus on safety applications, this paper 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

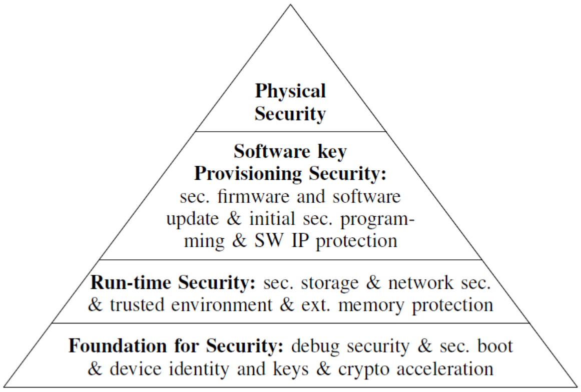

Physical Security
Software key Provisioning Security: sec. firmware and software update & initial sec. programming & SW IP protection
Run-time Security: sec. storage & network sec. & trusted environment & ext. memory protection
Foundation for Security: debug security & sec. boot & device identity and keys & crypto acceleration

FIGURE 2. Typical layers of an embedded processor, with or without wireless interface [65].

also be classified from a system access perspective in which an attacker can pose three main types of threats [65]: remote network access by, e.g. an unsecured gateway, access in close proximity, or physical access to a critical electronic module. The features, indicated in Fig. 2, 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 [65]. A perquisite for the security of wireless communication, especially also 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 need on the factory floor, where algorithms have to be implemented in a very resource efficient way. Therefore, cryptographic performance and timing for IOLW have recently been investigated in [40], [41] for AES-ECB, AES-CBC and AES-CTR with payload length of 8, 16, and 32 bytes.

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 [65].

C. FUNCTIONAL SAFETY

Typically, safety protocols shall support a safety integrity level (SIL) from at least SIL3 [66] or Category 4 and PL e [67]. Also a safety function response time (SFRT) of about 10 ms or less shall be feasible. Additionally, a combination of a safety protocol data unit (SPDU) addressing different SIL levels and a non-safety protocol 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 [50]. In IEC 61784-3, all (mentioned) safety protocols rely on the black channel principle, which is also adopted in the considerations of this paper. Table 1 lists adequate safety measures to cope with typical communication failures [68]. Also security measures are itemized. 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 for data integrity.

V. SECURITY MEASURES AND ENABLERS IN NARROW-BAND WIRELESS TECHNOLOGIES

Wireless technologies such as Bluetooth Low Energy, WirelessHART, Zigbee and other industrial wireless technologies have already specified detailed security mechanisms, which are reviewed in this section. Here, the focus lies on narrow-band (with respect to coherence bandwidth) wireless technologies with limited payload capacities (length).

A. BLUETOOTH LOW ENERGY (BLE)

Bluetooth Low Energy (BLE) with its current Core Specification 5.2 supports computational and storage-constrained devices with five basic security services [69], [70]:

- Authentication to identify communication partners based on their Bluetooth address.
- Confidentiality to prevent compromised information through eavesdropping.
- Authorization to allow the control of resources.
- Message integrity to guarantee that a message sent between two Bluetooth devices has not been altered.
- Pairing/bonding to create shared secrets and appropriate means for key storage.

Different security modes and levels are provided by BLE [70]. BLE relies on the Advanced Encryption Standard (AES) counter with CBC-MAC (AES-CCM) encryption offering native FIPS-140 validation [71]. Also, low energy "secure connections" features enhancing low energy pairing to utilize FIPS-approved algorithms (AES-CMAC (cipher-based message authentication code) and P-256 elliptic curve) are included in BLE specification 5.2 [70]. In BLE compared to other Bluetooth versions, a long term key (LTK) is used for low energy pairing, rather than a link key. BLE uses established cryptographic algorithms for pairing and message exchange and has elaborated features for key management.

B. ZIGBEE

The Zigbee standard employs the basic security elements as described in IEEE 802.15.4 [72] such as AES encryption and counter with CBC-MAC (AES-CCM) security modes. Additional security features with [15], [73] are: 128-bit AES encryption algorithms, defined key types (e.g. link and network keys), key setup and maintenance, keys can be hardwired into an application, AES-CCM* (Unified/simpler mode of operation), and trust center security that can be customized for the application. Zigbee employs ECDSA-P256-SHA256 to ensure a secure boot process and to guarantee authenticity and integrity [74]. For encryption purposes with authentication of messages, a simpler mode

TABLE 1. Communication errors and safety and security measures based on [68, p. 66] and being applied for IOLW.

Communication error	Protocol safety and security-for-safety measures					
	Counter/inverted counter	Timeout with receipt	Encryption root key to create session key	Integrity Message Integrity Code (MIC)	Authenticity Startup: ECC and symmetric key exchange Operate: Session key	Cyclic Redundancy Check
Data Corruption	-	-	X	X	-	X
Unintended repetition	X	X	-	-	-	-
Incorrect sequence	X	-	-	X	-	-
Packet Loss	X	X	-	-	-	-
Unacceptable delay	-	X	-	-	-	-
Packet/data Insertion	X	-	-	-	-	-
Masquerade	-	-	X	X	X	X
Wrong Addressing	-	-	-	-	-	X
Loop-back of messages	X	-	-	-	-	-

of CCM is used. A message integrity code (MIC) with 4-bytes is used to authenticate the message ensuring that the message has not been modified. The receiving device hashes the message and verifies the calculated MIC against the value appended to the original message. Zigbee also tailored the cryptographic algorithms to limited message length and application-dependent payloads.

C. WIRELESSHART

In WirelessHART 128-bit AES encryption can be used for the communication within the device mesh network and the gateway. Individual device session keys are employed to ensure end-to-end message authenticity, data integrity, receipt validation, and secrecy regarding devices. Message authentication and verification for the transmitting and receiving device is achieved by hop-by-hop CRC and MIC calculations. A set of security keys for different purposes (e.g. join key or network key) [75] is defined in the standard. The security of the WirelessHART protocol strongly depends on the secrecy of these keys, especially the pre-configured join key, which is used for communication initialization. Furthermore, white listing is used to allow join keys, whereas the entire communication is managed by a ‘‘Network Manager’’ [76]. Also WirelessHART adjusted its security means to the required payload length. For instance, a short MIC is used to guarantee integrity and authenticity. Focus is also laid on control access to the wireless network, wireless network infrastructure, and client integrity.

D. LORAWAN

LoRaWAN also incorporates security features, based on cipher-based message authentication code with 128-bit AES (AES-CMAC) [77] for integrity protection and AES counter mode (AES-CTR) for encryption [78]–[81]. Three different keys are specified, all for 128-bit AES encryption. Secure pairing utilizes the application key (AppKey) and AES-CMAC. The two session keys, application session key (AppSKey) and network session key (NwkSKey) are used for payload end-to-end encryption and integrity protection as well as encryption on network level, respectively [78].

E. ENOCEAN

The EnOcean Alliance also provides a distinct security specification [82]. Overall, a modular architecture of security features is described to account for standard line-powered devices, low-power energy harvesting devices and even ‘‘high security mode’’ applications. Furthermore, this specification describes among others CMAC, a rolling code (RLC) algorithm with 16 bits, 24 bits, or 32 bits as well as procedures like secure ‘‘Teach-In’’ (i.e. secure pairing) on the basis of a pre-shared key and optional data encryption. Variable AES (VAES), a 128-bit AES algorithm, is proposed for encryption. Near field communication (NFC) and quick response (QR) codes are suggested for pre-shared keys. Because of limited payload length, the EnOcean protocol uses a RLC as an additional secret to achieve a higher security level.

F. SUMMARY OF SECURITY ASPECTS OF WIRELESS TECHNOLOGIES

Most of the wireless protocols discussed use ‘‘state-of-the-art’’ block cipher modes (e.g. AES-CCM), cipher-based message authentication codes (e.g. CMAC), hashed-based message authentication codes (e.g. HMAC), and/or protocols for key exchange (e.g. ECDH). Recommendation e.g. stated in the BSI [83] or in NIST [84] shall be used for encryption algorithms, cipher block modes, key length, implementations, test vectors or e.g. hash algorithms. Also stated vulnerabilities of BLE during the pairing phase (CVE-2020-10134), the implementation of AES-CBC in EnOcean suggesting an all-zero IV (CVE-2018-5383), or e.g. that the password change function in Zigbee does not require knowledge of the old password (CVE-2019-20481) shall be considered to develop and use security features for IOLW.

G. APPROACHES TOWARDS IO-LINK WIRELESS SECURITY

Security features are currently not implemented in IOLW [22, Sec. 3.1.46]. Within typical vulnerability scenarios, an attack on the PL of IOLW is rather unlikely as the attack has to be in close proximity to the machine or network, and thus the probability for detection is high. Therefore, an attack on higher layers e.g. attacking the programmable logic controller (PLC) or the port and device configuration tool (PDCT) is more likely. Another reason is the effort versus the outcome, because on the PL raw data are transmitted, whereas semantic data can easily be interpreted on higher layers. Furthermore, for eavesdropping or man-in-the-middle (MITM) attacks, the frequency hopping table has to be known by the attacker. In a secure implementation, the HT01 hopping table [22], [39] shall be kept confidential.

Recently, approaches to enhance IOLW by security features have been proposed. In the pending patent applications [85]–[87], well-known standard mechanisms and algorithms like elliptic-curve Diffie-Hellmann (ECDH), secure hash algorithm (SHA), symmetric encryption in the downlink as well as in the uplink, cryptographically secure pseudo-random number generator (CSPRNG) and 256-bit AES are suggested to enhance security features for IOLW. Thereby, secure key exchange, secure pairing and encryption/decryption can be achieved. But as shown above, other wireless protocols limited in payload length have also adapted secure algorithms to the practical use for information-heavy applications.

Lately, in [40], [41] the influence of different cryptographic algorithms like AES-Electronic Code Book Mode (AES-ECB), AES-CBC, and AES-CTR to accomplish confidentiality on the timing and energy consumption of IOLW equipment were analyzed. As a main outcome, the implementation of these algorithms results in no significant drawback, whether on the energy consumption or on timing.

VI. ASSESSMENT OF THE AUTOMATION ENVIRONMENT

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

A. IO-LINK WIRELESS ARCHITECTURE

The architecture of an automation topology with an IOLW system is presented in [22, p. 29] describing a 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 PDCT has been extended compared to the wired IO-Link Interface and System Specification [47] 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) IO-Link specification [47].

B. IO-LINK SAFETY ARCHITECTURE

The IO-Link Safety System Extensions, i.e. single-drop digital communication interface technology for functional safety (SDCI-FS) [68], 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 fieldbuses as well as for safety functions ‘‘locally’’ between a safety controller and safety sensors or actuators. Functional safety communication profiles (FSCP) on top of the fieldbuses support reduced wiring, 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 [68, p. 30]. Furthermore, IO-Link Safety 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.

C. IO-LINK WIRELESS SAFETY ARCHITECTURE PROPOSAL

Fig. 3 shows the proposed IOLW Safety architecture mainly based on IO-Link (IEC 61131-9) [47], [48]. All additional or modified components and features for fail-safe communication are depicted in bold to employ a fail-safe wireless master (FS-W-Master) and fail-safe wireless devices (FS-W-Device) as sensor/actuator node as well as a fail-safe wireless bridge (FS-W-Bridge) connected to a wired fail-safe device (FS-Device). Fail-safe IO device descriptions (FS-IODDs) are used as a digital data sheet. Currently, the IODD is not structured as a certificate using e.g. the X.509 certificate structure [88], which would be necessary to identify and to prove the integrity of individual FS-W-Devices or FS-W-Bridges. This can be solved using public key management including distribution between FS-W-Master and FS-W-Devices/FS-W-Bridges.

The architecture of the FS-W-Master includes the original standard master interface (SMI) and the FSCP gateway application (black channel) [68, 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.

A functional safety device shall always create a point-to-point or one-to-one connection. Therefore, specific configuration steps are necessary when connecting functional safety devices. This requirement can be fulfilled using cryptographic algorithms for integrity and authentication in combination with 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.

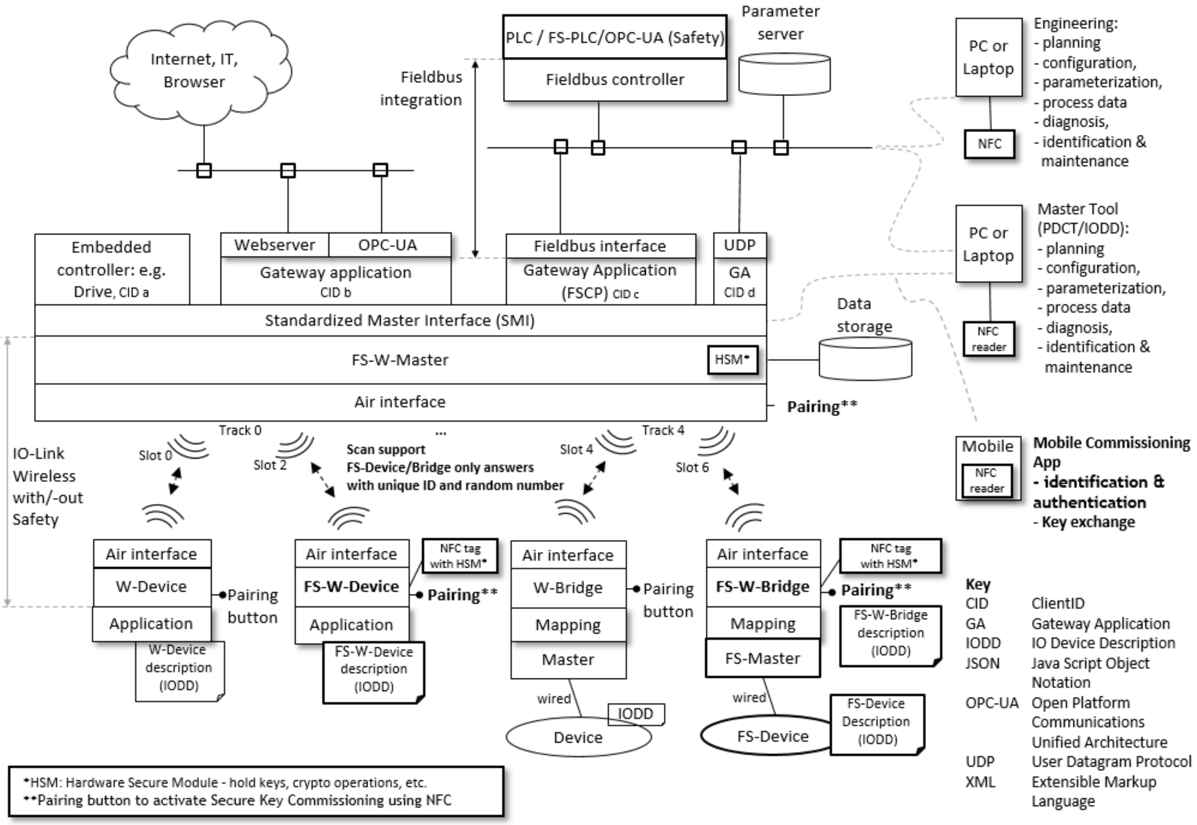


FIGURE 3. Proposed IOLW safety configuration (with added features in bold) within the automation hierarchy, based on [22].

Furthermore, the button has to be operated by a qualified safety person initializing the FS-W-Device to the dedicated tool of the IOLW 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 HF RFID standards [89]–[95]. 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 VII. Key management and organization is also a central point for secure operations, therefore, principles should be followed, such as [96]–[98].

1) PROTOCOL STACK ARCHITECTURE

The modified safety and security enhanced IOLW layered architecture of FS-W-Master and FS-W-Device is presented in Fig. 4. The PL as well as the data link layer of IOLW remain unchanged. System management (SM) services coordinate system startup and also allowing configuration of possible operational modes. SM services of FS-W-Master and FS-W-Device are significantly different when compared with the standard W-Master and W-Devices.

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.

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 safety communication layer (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 (API). 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 OPC UA Safety [99].

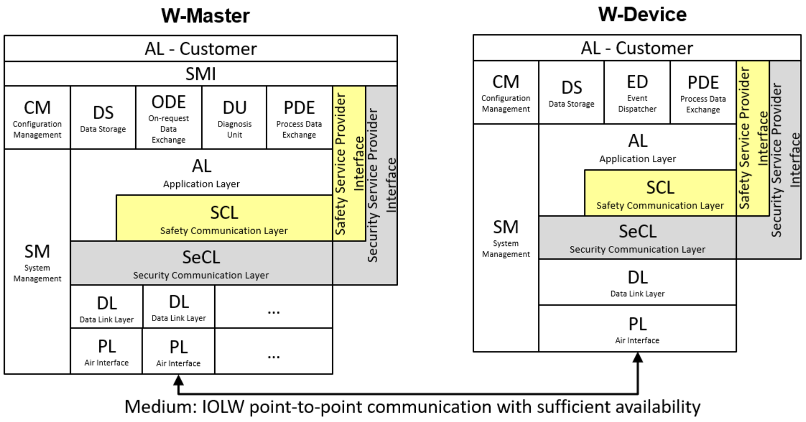


FIGURE 4. Proposed IOLW safe and secure data transfer architecture.

2) KEY MANAGEMENT

A key management system for FS-W-Master and FS-W-Devices is vital to securely hold a root or 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 AL. 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 MIC.
  - Further application-depend keys should be specified.

VII. ESTABLISHING A ONE-TO-ONE CONNECTION

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 [100], hence some are selected in the following subsection.

A. SECURITY DURING COMMISSIONING OF SECRETS

The following key establishment techniques are approved by FIPS [71] and the recommendations for cryptographic key generation shall be obeyed [101]. 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 and other small values [102].
- 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 [103].
- 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) [104]. 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 [83]. Public keys can be used as static or ephemeral, which are not authenticated and temporary [105].
  -- 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 [106].
  -- FourQ is a high-performance elliptic curve, which also targets a 128-bit security level, claiming to

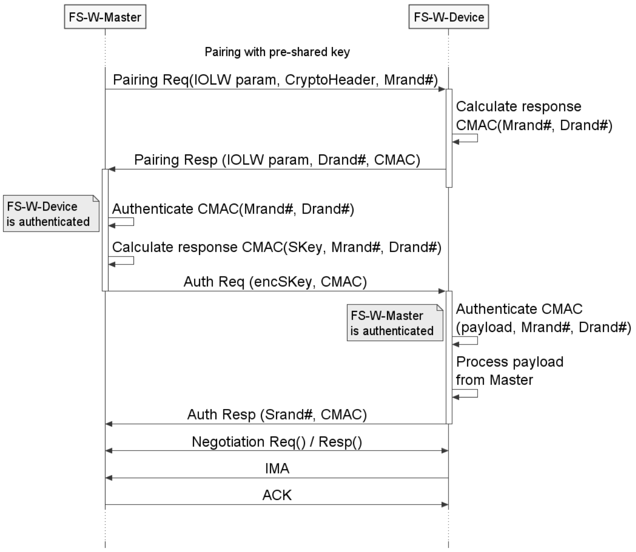
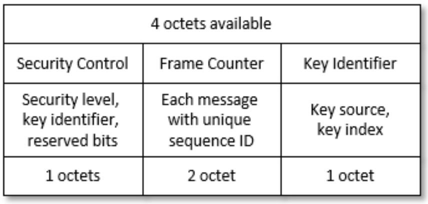

FS-W-Master
FS-W-Device
Pairing with pre-shared key
Pairing Req(IOLW param, CryptoHeader, Mrand#)
Calculate response CMAC(Mrand#, Drand#)
Pairing Resp (IOLW param, Drand#, CMAC)
FS-W-Device is authenticated
Authenticate CMAC(Mrand#, Drand#)
Calculate response CMAC(SKey, Mrand#, Drand#)
Auth Req (encSKey, CMAC)
FS-W-Master is authenticated
Authenticate CMAC (payload, Mrand#, Drand#)
Process payload from Master
Auth Resp (Srand#, CMAC)
Negotiation Req() / Resp()
IMA
ACK

FIGURE 5. Proposed secure IOLW pairing sequence, which is based on the original IOLW pairing sequence [22] and features taken from [82].



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 6. Structure of the proposed CryptoHeader.

be between four to five times faster than NIST P-256 curve and two to three times faster than Curve25519 [106], [107].

- Elliptic curve Menezes-Qu-Vanstone (ECMQV) key agreement is an authenticated protocol for key agreement based on the DH [108].
- Certificate-based pairwise key establishment (CPKE) [109].

In the pre-download phase, 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 MITM attacks unlikely, because of a very low range of about 10 cm [110]. 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 an optimal combination for fast short bursts of sensitive data exchange [111].

B. 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. 5, is proposed including security features from [82].

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.

Fig. 6 depicts the "CryptoHeader" with the available octets in the pairing sequence of IOLW. Further investigations shall show if the available length and configuration are sufficient.

The key identifier mode sets the kind of key (session/ application-dependent) being 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 [112]. 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 VIII. 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.

VIII. CRYPTOGRAPHIC ALGORITHMS FOR IOLW MESSAGE EXCHANGE

Suitable cryptographic algorithms for IOLW message exchange are examined in this section. For this purpose, exemplary implementations as well as measurements of power consumption and timing are shown.

After commissioning, regular communication is established transmitting messages in SSlots and/or DSlots. As only two octets are possibly transmitted in SSlots and compatibility with IOLW and IO-Link Safety is mandatory, con-

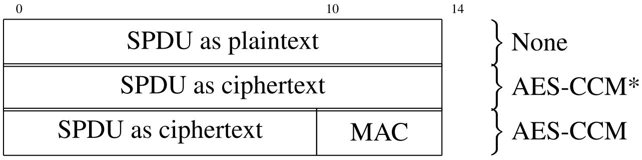


FIGURE 7. One DSlot message with confidential and /or authenticated data.

TABLE 2. 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

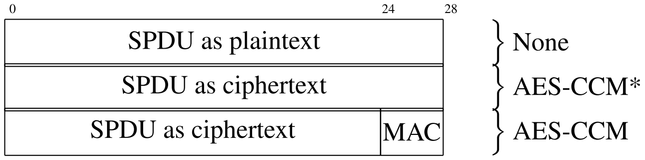


FIGURE 8. Messages of two DSlots with confidential and /or authenticated data.

TABLE 3. 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

fidentiality cannot be established for SSlot data exchange. Therefore, only DSlot transmission is considered.

As already mentioned in Section III, 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 [113]. Here, 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 [114]. Further details on the implementation are given in [114] and [115].

Exemplary realizations and measurements of security features on CC2650 transceiver chips are shown in [52]. This transceiver was chosen, because it is widely used for IOLW implementations, as demonstrated in [39]–[41]. 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 [115] and the AES-CCM* variant used in IEEE 802.15.4 [72]. 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* [114]. Different return behaviors for calling the cryptographic operations are possible such as callback, blocking, and polling, which are described in [40]. 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 [113] were used for verification of the parameter for the algorithm used.

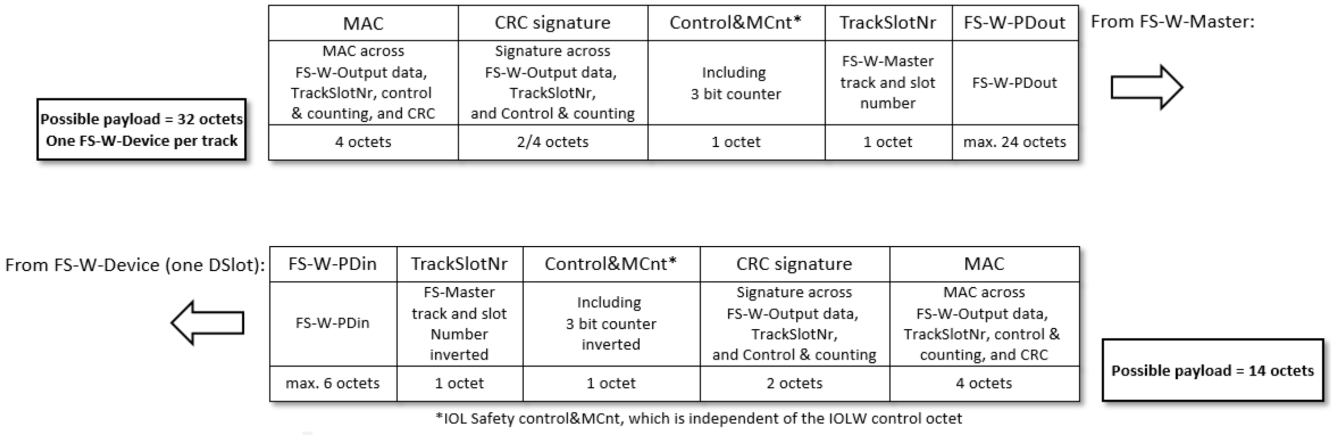
Fig. 7 depicts the configurations of the SPDU using plaintext, AES-CCM* (14 bytes decrypted), and AES-CCM (ten bytes decrypted and four bytes MAC).

Table 2 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 [40], [41]. 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 %.

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. 8

In Table 3, 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.

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



From FS-W-Master:

MAC	CRC signature	Control&MCnt*	TrackSlotNr	FS-W-PDout
MAC across FS-W-Output data, TrackSlotNr, control & counting, and CRC	Signature across FS-W-Output data, TrackSlotNr, and Control & counting	Including 3 bit counter	FS-W-Master track and slot number	FS-W-PDout
4 octets	2/4 octets	1 octet	1 octet	max. 24 octets

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

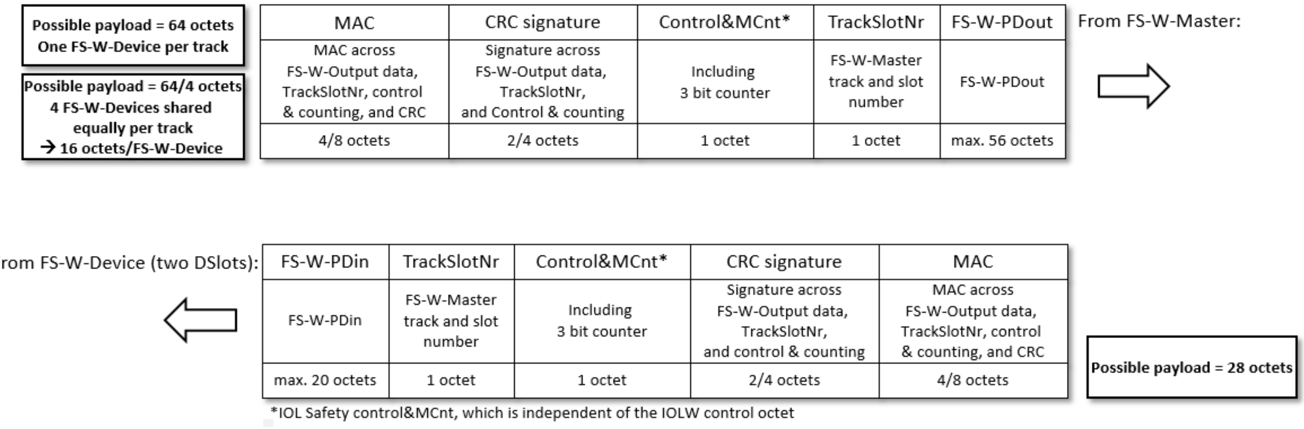
From FS-W-Device (one DSlot):

FS-W-PDin	TrackSlotNr	Control&MCnt*	CRC signature	MAC
FS-W-PDin	FS-Master track and slot Number inverted	Including 3 bit counter inverted	Signature across FS-W-Output data, TrackSlotNr, and Control & counting	MAC across FS-W-Output data, TrackSlotNr, control & counting, and CRC
max. 6 octets	1 octet	1 octet	2 octets	4 octets

Possible payload = 14 octets

*IOL Safety control&MCnt, which is independent of the IOLW control octet

FIGURE 9. IOLW safety PDUs with one DSlot and cycle time of 5 ms (2 retries).



From FS-W-Master:

MAC	CRC signature	Control&MCnt*	TrackSlotNr	FS-W-PDout
MAC across FS-W-Output data, TrackSlotNr, control & counting, and CRC	Signature across FS-W-Output data, TrackSlotNr, and Control & counting	Including 3 bit counter	FS-W-Master track and slot number	FS-W-PDout
4/8 octets	2/4 octets	1 octet	1 octet	max. 56 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 (two DSlots):

FS-W-PDin	TrackSlotNr	Control&MCnt*	CRC signature	MAC
FS-W-PDin	FS-W-Master track and slot number	Including 3 bit counter	Signature across FS-W-Output data, TrackSlotNr, and control & counting	MAC across FS-W-Output data, TrackSlotNr, control & counting, and CRC
max. 20 octets	1 octet	1 octet	2/4 octets	4/8 octets

Possible payload = 28 octets

*IOL Safety control&MCnt, which is independent of the IOLW control octet

FIGURE 10. IOLW safety PDU with two DSlots and cycle time of 10 ms (2 retries for each DSlot package).

encryption block cipher mode to provide confidentiality and through CBC-MAC message integrity and authentication.

IX. PROPOSAL FOR AN IOLW SAFETY PDU

In this section, a new lean functional safety communication protocol on top of the existing IO-Link architecture system [47] is proposed being based on IO-Link Safety [68] with additional features to support wireless safety-related communication. To keep the safety communication layer as simple as possible, protocol segmentation and packaging shall be realized in the DL of IOLW and parts of the SPDU shall not be aggregated in a layer higher than the data link layer. Nevertheless, this is also feasible if longer message lengths accompanied by longer transmission times, are necessary. In this case, it is important that no storing elements are within the point-to-point communication of IOLW Safety. Data types of safety messages (process data) are typically expressed in SPDU input and output data. The process data of the sensor or actuator are addressed by the FS-W-PDin data and is different depending on the application requirement as well as the process data information sent by the FS-W-Master (FS-W-PDout). In the following subsections, two possible configurations of an IOLW SPDU are proposed depending on cycle time and SPDU length.

A. SPDU USING ONE DSLOT

Fig. 9 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 [50] 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 IOL Safety, 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 [68]).

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

FS-W-PDout length is limited to 24 octets. For the input data, it is also feasible to separate the six octets of the 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.

B. SPDU USING TWO DSLOTs

Fig. 10 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-PDin/FS-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 IOL Safety. 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.

X. CONCLUSION

A safety architecture proposal for low-latency sensor/actuator networks using IOLW has been described. Therefore, requirements regarding wireless robustness, (cyber-)security, and functional safety have been evaluated and were tailored to IOLW by considering security measures and enablers of other narrow-band wireless technologies. The proposed IOLW safety architecture takes also into account the specific features of IO-Link Safety being adapted for IOLW. Also the specific properties of IOLW were assessed to combine both standards to a comprehensive approach.

A protocol architecture, including a safety and security communication layer, has been introduced including services to provide features to the application layer.

With regards to functional safety, it is fundamental to establish a one-to-one connection between a FS-W-Master and a FS-W-Device. Therefore, out-of-band commissioning, using NFC in combination with cryptographic algorithms, is proposed to securely exchange keys for cyclic IOLW communication. Before communicating in IOLW cyclic mode, a secure IOLW pairing sequence has been introduced. Two possible IOLW DSlot message lengths have been evaluated concerning their time duration, average current and relative battery lifetime reduction.

An IOLW SPDU was suggested, and it has been shown that the SPDU length of the IOLW DSlot message varies depending on its cycle time. The evaluation has shown that FS-W-PDout data with different FS-W-PDin data length are feasible. IOLW Safety protocol measures were based on IO-Link Safety and complemented with security features as well as architecture improvements.

In the next step, a model for protocol verification will be developed in combination with a full system demonstrator including a FS-W-Master and a FS-W-Device to be tested for validation and further measurements. This process shall guarantee that the demonstrator is valid for IOLW deterministic data transmission and timing of safety applications. In general, a system model also requires a functional hazard analysis and (cyber-)security analysis, which are often very application dependent and may only be abstracted to different groups or requirements of safety applications.

Another field of interest is authentication over proximity, whereby the received signal strength indicator (RSSI) is used for security and safety constraints. RSSI is the indication of signal strength observed by the receiver. RSSI might be used as an additional safety measure for FS-W-Devices. A signal strength monitor could extract the distance between a FS-W-Master and FS-W-Device, which must be within a predefined range of RSSI only.

ACKNOWLEDGMENT

The authors would like to acknowledge R. Sperrer, D. Krush, H. Wattar, D. Krueger, and R. Heynicke for their continuous support and rich discussions.

REFERENCES

[1] D. Etz, T. Frühwirth, A. Ismail, and W. Kastner, ‘‘Simplifying functional safety communication in modular, heterogeneous production lines,’’ in *Proc. 14th IEEE Int. Workshop Factory Commun. Syst. (WFCS)*, Jun. 2018, pp. 1–4.

[2] H.-J. Korber, H. Wattar, and G. Scholl, ‘‘Modular wireless real-time sensor/actuator network for factory automation applications,’’ *IEEE Trans. Ind. Informat.*, vol. 3, no. 2, pp. 111–119, May 2007.

[3] G. Scholl, R. Heynicke, D. Krueger, and R. Hornung, ‘‘Wireless automation,’’ in *Proc. SENSOR*, May 2013, pp. 379–383.

[4] 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 *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, Jun. 2014, pp. 67–72.

[5] 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 *Proc. IEEE 21st Int. Conf. Emerg. Technol. Factory Automat. (ETFA)*, Sep. 2016, pp. 1–4.

[6] *Aspects of Dependability Assessment in ZDKI Technical Group 1*, ifak e. V. Magdeburg, Germany, 2017.

[7] *Requirement Profiles in ZDKI Technical Group 1*, ifak e. V. Magdeburg, Germany, 2017.

[8] J. Jasperneite, T. Sauter, and M. Wollschlaeger, ‘‘Why we need automation models: Handling complexity in industry 4.0 and the Internet of Things,’’ *IEEE Ind. Electron. Mag.*, vol. 14, no. 1, pp. 29–40, Mar. 2020.

[9] *VDE Position Paper—Wireless Technologies for Industrie 4.0*, VDE ITG Informationstechnik, 2018.

[10] R. Dionísio, T. Lolić, and P. Torres, ‘‘Electromagnetic interference analysis of industrial IoT networks: From legacy systems to 5G,’’ in *Proc. IEEE Microw. Theory Techn. Wireless Commun. (MTTW)*, vol. 1, Oct. 2020, pp. 41–46.

[11] A. Alabbasi, T. Dudda, Z. Zou, and J. Kronander, ‘‘5G toolbox for realizing industrial automation,’’ in *Proc. IEEE 2nd 5G World Forum (5GWF)*, Oct. 2019, pp. 512–515.

[12] A. Aijaz, ‘‘Private 5G: The future of industrial wireless,’’ *IEEE Ind. Electron. Mag.*, vol. 14, no. 4, pp. 136–145, 2020, doi: 10.1109/MIE.2020.3004975.

[13] M. Baker and M. Poikselk, ''5G Releases 16 and 17 in 3GPP,'' Nokia Bell Labs CTO, New York, NY, USA, Tech. Rep., 2020.

[14] *VDI/VDE 2185 Blatt 1:2020-08 Radio Based Communication in Industrial Automation—Requirements and Principles*, VDI/VDE, Berlin, Germany, 2020. Accessed: Jan. 26, 2021. [Online]. Available: https://www.beuth.de/de/technische-regel/vdi-vde-2185-blatt-1/319538762

[15] *ZigBee Specification*, ZigBee Alliance Board Directors, Davis, CA, USA, Aug. 2015. [Online]. Available: https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf

[16] *Enocean Alliance—Building Smarter Connectivity*, EnOcean Alliance, San Ramon, CA, USA, 2021. Accessed: Aug. 2, 2021. [Online]. Available: https://www.enocean-alliance.org/

[17] *Industrial Networks—Wireless Communication Network and Communication Profiles—WirelessHART*, Standard IEC 62591:2016, 2016.

[18] M. Nixon, ''A comparison of WirelessHART and ISA100.11a,'' Emerson Process Manage., Round Rock, TX, USA, Tech. Rep., 2012. Accessed: Jan. 28, 2021.

[19] *Industrial Networks—Wireless Communication Network and Communication Profiles—ISA 100.11a*, Standard IEC 62734:2014, 2014.

[20] *Industrial Networks—Wireless Communication Network and Communication Profiles—WIA-PA*, Standard IEC 62601:2015, 2015.

[21] I. Verhappen, ''WIA-PA and WIA-FA to be added to IEC wireless standards,'' Tech. Rep., 2016. Accessed: Dec. 7, 2017. [Online]. Available: https://www.controlglobal.com/articles/2016/wia-pa-and-wia-fa-to-be-added-to-iec-wireless-standards/

[22] *IO-Link Wireless System Extensions—Specification Version 1.1*, IO-Link Community, Karlsruhe, Germany, Mar. 2018. [Online]. Available: https://io-link.com/en/index.php

[23] 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,'' *J. Sensors Sensor Syst.*, vol. 7, no. 1, pp. 131–142, 2018, doi: 10.5194/jsss-7-131-2018.

[24] *Industrial Networks—Wireless Communication Network and Communication Profiles—WIA-FA*, Standard IEC 62948:2017, 2017.

[25] T. R. Doebbert, C. Cammin, G. Scholl, and B. Kärcher, ''Study of a safe and secure ecosystem based on IO-Link Wireless and a 5G campus network,'' in *Proc. 26th IEEE Int. Conf. Emerg. Technol. Factory Automat. (ETFA)*, 2021, pp. 1–4, doi: 10.1109/ETFA45728.2021.9613484.

[26] S. Dietrich, G. May, O. Wetter, H. Heeren, and G. Fohler, ''Performance indicators and use case analysis for wireless networks in factory automation,'' in *Proc. 22nd IEEE Int. Conf. Emerg. Technol. Factory Automat. (ETFA)*, Sep. 2017, pp. 1–8.

[27] 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 *Proc. Wireless Congr.*, Nov. 2018, pp. 1–13.

[28] 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,'' *Proc. IEEE*, vol. 107, no. 6, pp. 1053–1073, Jun. 2019.

[29] B. M. Otten, R. Weidner, and A. Argubi-Wollesen, ''Evaluation of a novel active exoskeleton for tasks at or above head level,'' *IEEE Robot. Autom. Lett.*, vol. 3, no. 3, pp. 2408–2415, Jul. 2018.

[30] Z. Yao, C. Linnenberg, R. Weidner, and J. Wulfsberg, ''Development of a soft power suit for lower back assistance,'' in *Proc. Int. Conf. Robot. Automat. (ICRA)*, May 2019, pp. 5103–5109.

[31] J. Wollert, ''Wireless systems for machinery safety,'' in *Proc. 16th Int. Conf. Res. Educ. Mechatronics (REM)*, Nov. 2015, pp. 88–91.

[32] J. Hoffmann, D. Kuschnerus, T. Jones, and M. Hubner, ''Towards a safety and energy aware protocol for wireless communication,'' in *Proc. 13th Int. Symp. Reconfigurable Commun.-Centric Syst. Chip (ReCoSoC)*, Jul. 2018, pp. 1–6.

[33] F. Kaestner, D. Kuschnerus, C. Spiegel, B. Janssen, and M. Huebner, ''Design of an efficient communication architecture for cyber-physical production systems,'' in *Proc. IEEE 14th Int. Conf. Automat. Sci. Eng. (CASE)*, Aug. 2018, pp. 829–835.

[34] 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 *Proc. AMA Conf. SENSOR IRS*, Jun. 2017, pp. 134–138.

[35] D. Wolberg, M. Rentschler, and P. Gaggero, ''Simulative performance analysis of IO-Link Wireless,'' in *Proc. 14th IEEE Int. Workshop Factory Commun. Syst. (WFCS)*, Jun. 2018, pp. 1–10.

[36] M. Rentschler, ''Roaming in wireless factory automation networks,'' in *Proc. 22nd IEEE Int. Conf. Emerg. Technol. Factory Automat. (ETFA)*, Sep. 2017, pp. 1–4.

[37] C. Cammin, D. Krush, H. Wattar, R. Heynicke, and G. Scholl, ''Base station antenna placement of wireless sensor/actuator networks in manufacturing cells,'' in *Proc. 24th IEEE Int. Conf. Emerg. Technol. Factory Automat. (ETFA)*, Sep. 2019, pp. 1317–1320.

[38] T. Solzbacher, R. Heynicke, and G. Scholl, ''Parallel processing of RSSI signals for gapless monitoring of the 2.45 GHz ISM band,'' *Technisches Messen*, vol. 85, no. s1, pp. s124–s128, Sep. 2018.

[39] D. Krush, C. Cammin, T. R. Doebbert, R. Heynicke, and G. Scholl, ''Coexistence management methods and tools for IO-Link Wireless,'' in *Proc. 17th IEEE Int. Conf. Factory Commun. Syst. (WFCS)*, Jun. 2021, pp. 151–158.

[40] T. Robert Doebbert, D. Krush, C. Cammin, J. Jockram, R. Heynicke, and G. Scholl, ''IO-Link Wireless device cryptographic performance and energy efficiency,'' in *Proc. 22nd IEEE Int. Conf. Ind. Technol. (ICIT)*, Mar. 2021, pp. 1106–1112.

[41] T. Doebbert, C. Cammin, and G. Scholl, ''Precision measurement of the application-dependent current consumption of a wireless transceiver chip,'' in *Proc. SMSI*, May 2021, pp. 281–282, doi: 10.5162/SMSI2021/D8.4.

[42] 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,'' *J. Sensors Sensor Syst.*, vol. 7, no. 1, pp. 183–192, Mar. 2018.

[43] C. Cammin, D. Krush, R. Heynicke, and G. Scholl, ''Employing correlation for wireless components and device characterization in reverberation chambers,'' *J. Sensors Sensor Syst.*, vol. 8, no. 1, pp. 185–194, May 2019.

[44] C. Cammin, D. Krush, R. Heynicke, and G. Scholl, ''Reproducibility of fading propability in a reverberation chamber for wireless device testing,'' in *Proc. IEEE Radio Antenna Days Indian Ocean (RADIO)*, Sep. 2019, pp. 1–2.

[45] C. Cammin, D. Krush, R. Heynicke, and G. Scholl, ''Deep fading in a reverberation chamber for wireless device testing,'' *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 766, Mar. 2020, Art. no. 012004.

[46] C. Cammin, D. Krush, R. Heynicke, and G. Scholl, ''Sensing reverberation chamber loading for IO-Link Wireless testing,'' in *Proc. Int. Conf. Electromagn. Adv. Appl. (ICEAA)*, Aug. 2021, pp. 087–091.

[47] *IO-Link Interface and System—Specification Version 1.1.3*, IO-Link Community, Karlsruhe, Germany, Jun. 2019. [Online]. Available: https://io-link.com/en/index.php

[48] *Programmable Controllers—Part 9: Single-Drop Digital Communication Interface for Small Sensors and Actuators (SDCI)*, Standard IEC 61131-9:2013, 2013.

[49] *Industrial Networks—Single-Drop Digital Communication Interface—Part 3: Wireless Extensions*, IEC Geneva Office Secretariat, Geneva, Switzerland, IEC New Work Item Proposal (65C/1070/NP) 61139-3 ED1, 2021. [Online]. Available: https://www.iec.ch/dyn/www/f?p=103:38:606242890486755::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1376,23,103578

[50] *Industrial Communication Networks—Profiles—Part 3: Functional Safety Fieldbuses—General Rules and Profile Definitions*, Standard IEC 61784-3:2021, 2021.

[51] R. Heynicke, D. Kruger, H. Wattar, and G. Scholl, ''Modular wireless fieldbus gateway for fast and reliable sensor/actuator communication,'' in *Proc. IEEE Int. Conf. Emerg. Technol. Factory Automat.*, Sep. 2008, pp. 1173–1176.

[52] *CC2650 SimpleLink Multistandard Wireless MCU Datasheet (Rev. B)*, Texas Instrum., Dallas, TX, USA, 2016.

[53] *VDI/VDE 2185 Blatt 2:2009-12 Radio Based Communication in Industrial Automation—Management of the Coexistence of Radio Solutions*, VDI/VDE, Berlin, Germany, 2009. Accessed: Aug. 26, 2021. [Online]. Available: https://www.beuth.de/de/technische-regel/vdi-vde-2185-blatt-2/121081189

[54] *American National Standard for Evaluation of Wireless Coexistence*, Standard ANSI C63.27-2017, 2017.

[55] *Industrial Communication Networks—Wireless Communication Networks—Part 1: Wireless Communication Requirements and Spectrum Considerations*, Standard IEC 62657-1:2017, 2017.

[56] *Industrial Communication Networks—Wireless Communication Networks—Part 2: Coexistence Management*, Standard IEC 62657-2:2017, 2017.

[57] *Industrial Communication Networks—Wireless Communication Networks—Part 2: Coexistence Management*, Standard IEC 62657-2:2017+AMD1:2019, CSV Consolidated Version, 2019.

[58] D. Krüger, R. Heynicke, and G. Scholl, "Wireless sensor/actuator-network with improved coexistence performance for 2.45 GHz ISM-band operation," in *Proc. 9th Int. Multi-Conf. Syst., Signals Devices (SSD)*, Mar. 2012, pp. 1–5.

[59] D. Wolberg and N. E. J. Tal, "Last resort frequency mechanism in a wireless communication system," U.S. Patent 11 036 200 B2, Jun. 15, 2021.

[60] *Definitions of Software Defined Radio (SDR) and Cognitive Radio System (CRS)*, document Rep. ITU-R SM.2152 (09/2009), ITU, 2009.

[61] R. Hornung, R. Heynicke, and G. Scholl, "Low-cost spectrum analyzer for cognitive radio applications and coexistence management in the 2.4 GHz ISM-band," in *Proc. SENSOR*, May 2013, pp. 396–398.

[62] T. M. Chiwewe, C. F. Mbuya, and G. P. Hancke, "Using cognitive radio for interference-resistant industrial wireless sensor networks: An overview," *IEEE Trans. Ind. Informat.*, vol. 11, no. 6, pp. 1466–1481, Dec. 2015.

[63] R. Anderson, *What is Security Engineering?* Hoboken, NJ, USA: Wiley, 2020.

[64] J. Horalek and V. Sobeslav, "Cybersecurity analysis of IoT networks," in *Computational Collective Intelligence*, N. T. Nguyen, R. Chbeir, E. Exposito, P. Aniorté, and B. Trawiński, Eds. Cham, Switzerland: Springer, 2019, pp. 488–499, doi: 10.1007/978-3-030-28374-2_42.

[65] *Building Your Application With Security in Mind*, Texas Instrum., Dallas, TX, USA, 2020.

[66] *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*, Standard IEC 61508, 2010.

[67] *Safety of Machinery—Safety-Related Parts of Control Systems—Part 1: General Principles for Design*, Standard ISO 13849-1:2015, 2015.

[68] *IO-Link Safety System Extensions With SMI—Specification DraftV1.1.3 for Review*, IO-Link Community, Karlsruhe, Germany, Jun. 2021.

[69] *Guide to Bluetooth Security*, NIST Special Publication 800-121 Revision 2, NIST, Gaithersburg, MD, USA, May 2017.

[70] *Bluetooth Core Specification Revision V5.2*, Bluetooth Core Specification Working Group, Washington, DC, USA, Dec. 2019.

[71] *Approved Key Establishment Techniques for Fips Pub 140-2*, NIST, Gaithersburg, MD, USA, Aug. 2020.

[72] *IEEE Standard for Low-Rate Wireless Networks*, Standard IEEE 802.15.4-2020, IEEE SA-802.15.4-2020, 2020.

[73] *AN1233: Zigbee Security*, Silicon Labs, Austin, TX, USA. Accessed: Jul. 21, 2021. [Online]. Available: https://www.silabs.com/documents/public/application-notes/an1233-zigbee-security.pdf

[74] *AN1218: Series 2 Secure Boot With RTSL*, Silicon Labs, Austin, TX, USA. Accessed: Jul. 23, 2021. [Online]. Available: https://www.silabs.com/documents/public/application-notes/an1218-secure-boot-with-rtsl.pdf

[75] *WirelessHART and Wi-Fi Security Technical Note*, Emerson Wireless Secur., Sep. 2017. [Online]. Available: https://www.emerson.com/documents/automation/white-paper-emerson-wireless-security-wirelesshart-wi-fi-security-deltav-en-41260.pdf

[76] D. Raposo, A. Rodrigues, S. Sinche, J. S. Silva, and F. Boavida, "Securing wirelessHART: Monitoring, exploring and detecting new vulnerabilities," in *Proc. IEEE 17th Int. Symp. Netw. Comput. Appl. (NCA)*, Nov. 2018, pp. 1–9.

[77] *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, NIST Special Publication 800-38B, NIST, Gaithersburg, MD, USA, May 2005.

[78] *LoRaWAN Security Whitepaper*, LoRa Alliance, Fremont, CA, USA, 2017. [Online]. Available: https://lora-alliance.org/wp-content/uploads/2020/11/lorawan_security_whitepaper.pdf

[79] *LoRaWAN Security FAQ V2*, LoRa Alliance, Fremont, CA, USA, 2020. [Online]. Available: https://lora-alliance.org/wp-content/uploads/2020/11/lorawan_security_whitepaper.pdf

[80] *LoRaWAN is Secure (But Implementation Matters)*, LoRa Alliance, Fremont, CA, USA, 2021. Accessed: Aug. 15, 2021. [Online]. Available: https://lora-alliance.org/wp-content/uploads/2020/11/lorawan_security_whitepaper.pdf

[81] H. Noura, T. Hatoum, O. Salman, J.-P. Yaacoub, and A. Chehab, "LoRaWAN security survey: Issues, threats and possible mitigation techniques," *Internet Things*, vol. 12, Dec. 2020, Art. no. 100303.

[82] *System Specification—Security of EnOcean Radio Networks V 2.6*, EnOcean Alliance, San Ramon, CA, USA, 2020. Accessed: Aug. 2, 2021. [Online]. Available: https://www.enocean-alliance.org

[83] *BSI TR-02102-1 Cryptographic Mechanisms: Recommendations and Key Lengths*, BSI—Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security), Bonn, Germany, 2021.

[84] *National Vulnerability Database*, NIST, Gaithersburg, MD, USA, 2021.

[85] N. E. J. Tal, D. Wolberg, and A. Regev, "Secure communication encryption and decryption mechanism in a wireless communication system," U.S. Patent 2020 0 267 131 A1, Aug. 20, 2020.

[86] N. E. J. Tal, D. Wolberg, and A. Regev, "Secure pairing mechanism in a wireless communication system," U.S. Patent 2020 0 267 540 A1, Aug. 20, 2020.

[87] N. E. J. Tal, D. Wolberg, and A. Regev, "Secure key exchange mechanism in a wireless communication system," U.S. Patent 2020 0 267 547 A1, Aug. 20, 2020.

[88] R. Housley, W. Polk, W. Ford, and D. Solo, "Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile," Netw. Work. Group, Tech. Rep. RFC 5280, 2008. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc5280

[89] *Information Technology—Telecommunications and Information Exchange Between Systems—Near Field Communication—Interface and Protocol (NFCIP-1)*, Standard ISO/IEC 18092:2013, 2013.

[90] *Information Technology—Telecommunications and Information Exchange Between Systems—Near Field Communication—Interface and Protocol (NFCIP-1)—Technical Corrigendum 1*, Standard ISO/IEC 18092:2013/Cor 1:2015, 2015.

[91] *Identification Cards—Contactless Integrated Circuit Cards—Proximity Cards—Part 1: Physical Characteristics*, Standard ISO/IEC 14443-1:2016, 2016.

[92] *Cards and Security Devices for Personal Identification—Contactless Proximity Objects—Part 2: Radio Frequency Power and Signal Interface—Technical Corrigendum 1.*, Standard ISO/IEC 14443-2:2020/Cor 1:2021, 2020.

[93] *Cards and Security Devices for Personal Identification—Contactless Vicinity Objects—Part 1: Physical Characteristics*, Standard ISO/IEC 15693-1:2018, 2018.

[94] *Cards and Security Devices for Personal Identification Contactless Vicinity Objects Part 2: Air Interface and Initialization*, Standard ISO/IEC 15693-2:2019, 2019.

[95] *Cards and Security Devices for Personal Identification Contactless Vicinity Objects Part 3: Anticollision and Transmission Protocol*, Standard ISO/IEC 15693-3:2019, 2019.

[96] *Recommendation for Key Management—Part 1: General*, NIST Special Publication 800-57 Part 1 Revision 5, NIST, Gaithersburg, MD, USA, May 2020.

[97] *Recommendation for Key Management—Part 2: Best Practices for Key Management Organizations*, NIST Special Publication 800-57 Part 2 Revision 1, NIST, Gaithersburg, MD, USA, May 2019.

[98] *Recommendation for Key Management—Part 3: Application-Specific Key Management Guidance*, NIST Special Publication 800-57 Part 3 Revision 1, NIST, Gaithersburg, MD, USA, Jan. 2015.

[99] *OPC Unified Architecture for IO-Link Companion Specification, Release 1.0*, IO-Link Community OPC Found., Karlsruhe, Germany, Dec. 2018.

[100] C. Boyd, A. Mathuria, and D. Stebila, *Protocols for Authentication Key Establishment* (Information Security and Cryptography). Berlin, Germany: Springer, 2019.

[101] *Recommendation for Cryptographic Key Generation*, NIST Special Publication 800-133 Revision 2, NIST, Gaithersburg, MD, USA, Jun. 2020.

[102] E. Milanov, "The RSA algorithm," RSA Laboratories, Washington, DC, USA, Tech. Rep., Jun. 2009, pp. 1–11. [Online]. Available: https://sites.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf

[103] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[104] A. Menezes, "The elliptic curve discrete logarithm problem: State of the art," in *Proc. IWSEC*, Nov. 2008, p. 218.

[105] N. Mehibel and M. Hamadouche, "A new approach of elliptic curve Diffie–Hellman key exchange," in *Proc. 5th Int. Conf. Electr. Eng. Boumerdes (ICEE-B)*, Oct. 2017, pp. 1–6.

[106] R. Alvarez, C. Caballero-Gil, J. Santonja, and A. Zamora, "Algorithms for lightweight key exchange," *Sensors*, vol. 17, no. 7, p. 1517, Jun. 2017.

[107] C. Costello and P. Longa, "FourQ: Four-dimensional decompositions on a Q-curve over the Mersenne prime," Cryptol. ePrint Arch., Microsoft Res., USA, Tech. Rep. 2015/565, 2015. [Online]. Available: https://eprint.iacr.org/2015/565

[108] *Sec 4: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV)*, Certicom Res., Mississauga, ON, Canada, 2014.

[109] P. Porambage, P. Kumar, C. Schmitt, A. Gurtov, and M. Ylianttila, "Certificate-based pairwise key establishment protocol for wireless sensor networks," in *Proc. IEEE 16th Int. Conf. Comput. Sci. Eng.*, Dec. 2013, pp. 667–674.

[110] E. Lee, "Release limitation unclassified unclassified," Tech. Rep., 2014.

[111] C. Govender and B. V. Niekerk, "Secure key exchange by NFC for instant messaging," in *Proc. Conf. Inf. Commun. Technol. Soc. (ICTAS)*, Mar. 2021, pp. 27–33.

[112] J. Song, R. Poovendran, J. Lee, and T. Iwata, *The AES-CMAC Algorithm*, document RFC 4493, Network Working Group, Jun. 2006.

[113] D. Whiting, R. Housley, and N. Ferguson, *Counter With CBC-MAC (CCM)*, document RFC 3610, Sep. 2003.

[114] *CC26XX SimpleLink Multistandard Wireless MCU Header and Source Files*, Texas Instrum., Dallas, TX, USA, 2019.

[115] *Recommendation for Block Cipher Mode of Operation: The CCM Mode for Authentication and Confidentiality*, NIST Special Publication 800-38C, NIST, Gaithersburg, MD, USA, May 2004.

THOMAS R. DOEBBERT received the B.Sc. degree from the Milwaukee School of Engineering, USA, in 2010, the Dipl.-Ing. (FH) degree in electrical engineering from the University of Applied Science Luebeck, Germany, in 2010, and the M.Sc. degree in IT engineering from the University of Applied Science, Wedel, Germany, in 2018.

He is currently a Research Assistant with the Institute for Electrical Measurement Engineering, Helmut Schmidt University, University of Federal Armed Forces Hamburg, Germany. His research interests include functional safety and security of wireless sensor networks in the context of industrial applications, especially protocol design for robust and reliable wireless communication.

CHRISTOPH CAMMIN (Member, IEEE) received the B.Sc. and M.Sc. degrees in electrical engineering from TUHH, Hamburg, Germany, in 2010 and 2014, respectively.

Since 2014, he has been a Research Assistant with the Institute for Electrical Measurement Engineering, Helmut Schmidt University, University of Federal Armed Forces Hamburg, Germany. His research interests include the conceptual design and realization of wireless communication systems and test procedures, especially for industrial use. He is a member of WG 16 "Wireless" of IEC TC65/SC65C and active in the standardization of IO-Link Wireless and the corresponding test specification.

GERD SCHOLL (Member, IEEE) received the Dipl.-Ing. and Dr.-Ing. degrees in electrical engineering from the Technical University of Munich, Germany, in 1989 and 1996, respectively.

From 1991 to 2000, he was with the Surface Acoustic Wave Technology and Wireless Sensors Group, Siemens Corporate Research and Technology Center, Munich, where he was engaged in the design of surface acoustic wave resonators and low-loss devices for mobile communications and wireless sensor systems. He was also responsible for the realization of RF identification and sensor systems. From 2001 to 2003, he was with the Surface Acoustic Wave Division, Department of Research and Development, EPCOS AG, where he was responsible for basic research and development of new components, modules, and system concepts for radio-based services. Since 2004, he has been the Chair of electrical measurement engineering with Helmut Schmidt University, University of Federal Armed Forces Hamburg, Germany. His current research interests include industrial sensor and communication systems and highly-automated unmanned aerial systems.