

# Design and Development of a Roaming Wireless Safety Emergency Stop

Henry Beuster<sup>1</sup>, Thomas Doebbert<sup>1</sup>, Christoph Cammin<sup>2</sup>, Dmytro Krush<sup>3</sup>, Gerd Scholl<sup>1</sup>

1 Electrical Measurement Engineering, Helmut-Schmidt-University, firstname.lastname@hsu-hh.de

2 Institute of Automation Technology, Helmut-Schmidt-University, christoph.cammin@hsu-hh.de

3 Electrical Measurement Engineering, Helmut-Schmidt-University, dmytro.krush@googlemail.com

KEYWORDS: functional safety, wireless, IO-Link Wireless, roaming

## ABSTRACT

Modern manufacturing is characterized by a high degree of automation, with autonomous systems also frequently being used. In such environments human intervention in the event of malfunctions or maintenance becomes a rare but also necessary task. When human workers are no longer an integral part of the production process, but only intervene when necessary, e.g., in the case of unexpected machine behavior, appropriate safety solutions will become even more important. This work describes a wireless communication system enabling a flexible and safe emergency stop function for multiple automation cells. A portable emergency stop switch allows seamless transition between different wireless cells, ensuring functional safety. The communication protocol combines IO-Link Wireless features with the safety requirements already implemented in IO-Link Safety. Security requirements are fulfilled through encryption and authentication. The IO-Link Wireless roaming functionality is used to extend the system across several manufacturing cells. An experimental setup confirms the suitability of the system for various applications. The results demonstrate the effectiveness of the handover mechanism and evaluate the potential of the system to improve flexibility, availability and security in dynamic production environments. Future extensions could include the use of AI based evaluation of the radio signals for an intelligent cell handover.

## 1 INTRODUCTION

In all areas of industrial automation, the need for secure, reliable, fast and flexible wireless communication solutions is ubiquitous. In contrast to previous wired communication solutions, wireless solutions offer greater local flexibility and a reduction of installation effort with significant cost savings (e.g., [1]). In addition to the consumer standards such as IEEE 802.11-based WLAN, Bluetooth, and in some cases, Zigbee, a number of specific wireless standards for predominantly industrial (sensor/actuator) data communication have become established (e.g., [1], [2], [3]). In the public funded project “Digital Sensor-2-Cloud Campus Platform” (DS2CCP) [4], in which IO-Link Wireless (IOLW) and 5G technology are implemented as future-oriented and cross-platform solutions, a reliable and robust wireless communication of sensors and actuators between the industrial shop floor and an edge cloud could be demonstrated [2], [5], [6]. The project aims for a consistent and holistic conception of an industrial DS2CCP for applications in the field of automation technology. Previous studies on requirements regarding safety, security and timing to aim for safety-related and security-for-safety applications are given in [2], [7] and the first IO-Link Wireless Safety (IOLWS) protocol concept evaluation is completed with a positive approval [8],[9]. Therefore, in this contribution, a further step is approached by adding more flexibility to IOLWS utilizing roaming within multiple automation cells.

This paper is organized as follows: After this general introduction to safe wireless communication, a focus is especially set on IOLWS in Section 2. Section 3 describes the roaming scenario and the measurement setup. The results are presented at the end of the section. The graphical evaluation and subsequent discussion follow in Section 4. Section 5 summarizes the results and suggests further research opportunities.

## 2 IO-LINK WIRELESS SAFETY

The functional safe wireless communication protocol in [9] combines the system architecture and basic communication algorithm of IOLW [10] and the safety requirements and principles of IO-Link Safety (IOLS) [11]. Recognizing the ongoing discussion and the inherent security challenges in wireless communication systems, especially in safety-critical applications, the proposed solution integrates encryption algorithms and authentication in an underlying security layer to follow security-for-safety requirements with a bit error rate up to 0.5, according to [8], [12].

In line with IEC 61784-3 [13] the security and safety communication layers within IOLWS are embedded into the software structure and the communication protocol. The Safety Process Data Unit with the concept of explicit

transmission of the safety measures for timeliness (Control&MCnt), authenticity (track/slot number), integrity as well as the point-to-point connection guaranteed by applying a cryptographic algorithm with sufficient entropy [8] is illustrated in Figure 1. Here, a Message Authentication Code (MAC) is employed to detect manipulations (guarantees integrity and authentication of the message) and a Cyclic Redundancy Check (CRC) to detect (stochastic) errors (data integrity) [8].

Within the configuration, the communication of non-safety wireless process data from the Failsafe-(FS-)W-Master using one communication channel per FS-W-Device is also possible. In this case, the functional safety wireless process data output length is limited to 22 octets. For the input data, it is also feasible to separate the six octets of the functional safety wireless process data input and equivalently non-safety wireless process data, which, therefore, are not included in the calculation of the MAC and CRC.

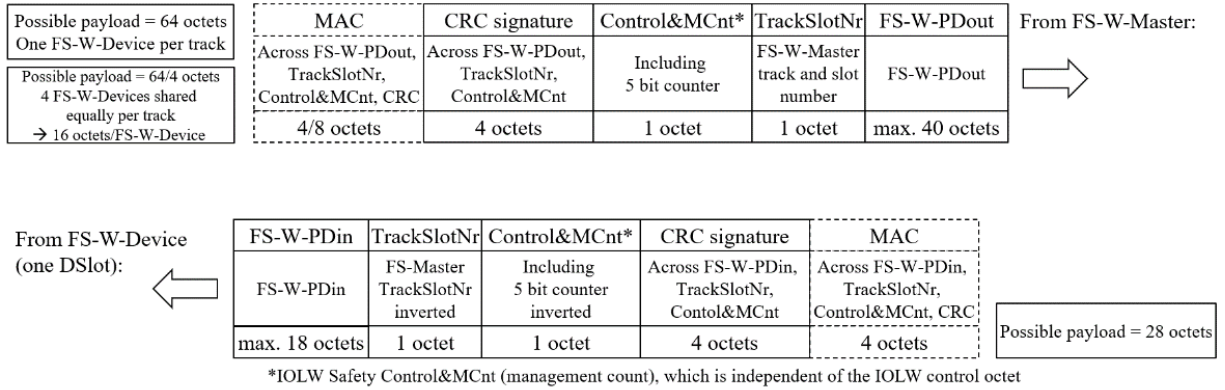


Figure 1. IOLWS Safety PDU. based on [8], [9].

### 3 ROAMING WITH IO-LINK WIRELESS SAFETY

A study on roaming, particularly in the context of IOLW, is given in [14], whereby the first published version of the IOLW standard already included the roaming feature. In this context, roaming describes the possibility that (FS-)W-Devices may connect to another cell (another (FS-)W-Master), when leaving the cell on purpose or disconnecting for any reason from the previous (FS-)W-Master [14].

In a simplified/reduced safety-related scenario, a mobile (FS-)W-Device (i.e., an emergency stop on a robot) moves from one cell to another, whereby the signal strength decreases at the boundary of the cell that is left and increases in the cell that is entered, as indicated by the grey scales in Figure 2 b). The measurement setup emulates the scenario depicted in Figure 2.

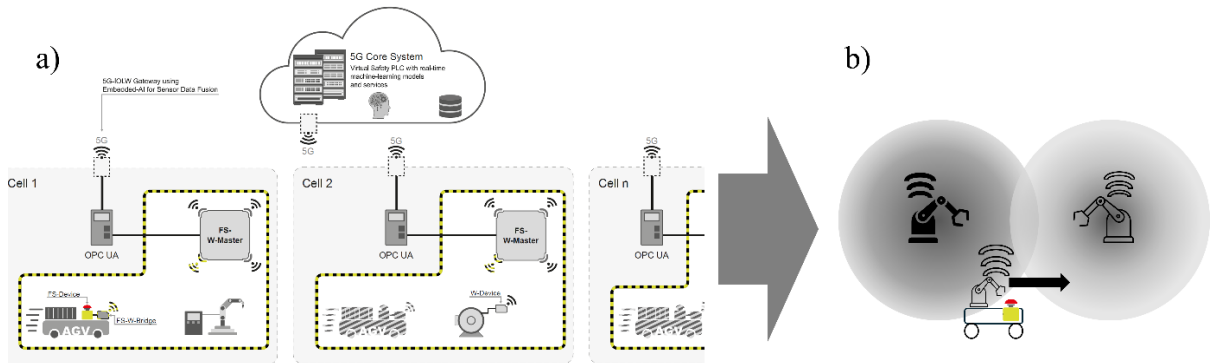


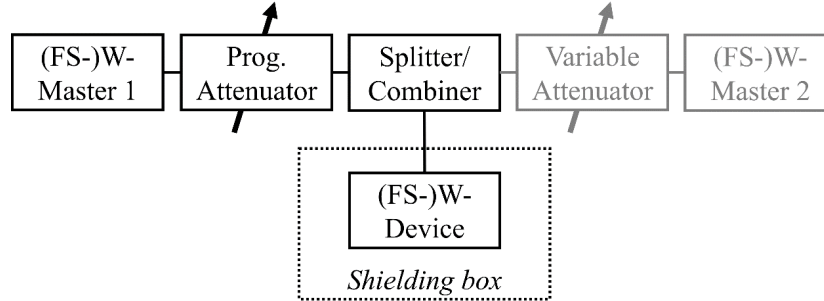
Figure 2. a) Modular sensor-2-cloud automation topology, based on [6]. b) Simplified scenario comparison of two wireless cells and one roaming (FS-)W-Device.

#### 3.1 Measurement Setup

Figure 3 illustrates a simplified setup for evaluation. In a wired shielded and reproducible setup, two (FS-)W-Masters are connected to a single (FS-)W-Device using a (resistive, i.e., non-directional) power splitter/combiner and variable/programmable attenuator. Controlling the attenuation of “(FS-)W-Master 2”, and thus adjusting the

receiving signal power of the (FS-)W-Device, the scenario of movement between the cells (as sketched in Figure 2 b) is emulated.

Utilizing output pins for status observations connected to an oscilloscope, the transition time for the cell handover is measured and recorded. For a better overview, the computer for controlling the entire setup and the oscilloscope for time measurement are not shown here.



**Figure 3.** Measurement setup, comprising of two (FS-)W-Masters and one (FS-)W-Device.

In total four measurement series are performed, two with a standard IOLW protocol stack and two with an IOLWS protocol stack. Two of them are carried out as “preliminary” measurements with only one (FS-)W-Master, as indicated by the (FS-)W-Master 1 box surrounded by the black solid line in Figure 3. The remaining two measurement series are performed with both (FS-)W-Master 1 and (FS-)W-Master 2 (grey box).

### 3.2 IO-Link Wireless Roaming Connection/Reconnection

In the first measurement series, the duration of establishing the connection between a roaming W-Device and a W-Master in track mode “Roaming” and port mode “RoamingAutoPairing” is evaluated as preparatory study without the safety stack. W-Master and W-Device are set to maximum transmission power level, corresponding to 10 dBm for the W-Master and 4 dBm for the W-Device. The programmable attenuator is switched between “ON” (an adjustable attenuation to emulate different distances) and “OFF” (103 dB, maximum attenuation), with a duration of two seconds each, i.e. four seconds in total for one measurement cycle. In the “ON”-state attenuations are chosen to emulate the following connection conditions:

- strong signal (30 dB attenuation resulting in Received Signal Strength Indicator (RSSI) of -37 dBm on the W-Master side, below any saturation effects),
- moderate connections (50 and 65 dB attenuation, RSSI of -53 and -67 dBm),
- weak connections (80 and 83 dB attenuation, RSSI of -83 and -87 dBm),
- bad connection (85 dB attenuation, RSSI of -89 dBm, just enough for a successful pairing).

Meanwhile, the duration for a reconnection is measured. In total 300 valid reconnections per setting are recorded with a sampling rate of 10,000 per second. The results for IOLW are given in Table 1. The mean IOLW roaming connect duration is always below 0.5 s for attenuations smaller than 80 dB, rapidly increasing beyond this limit.

### 3.3 IO-Link Wireless Safety Roaming Connection/Reconnection

Similar to the previous testcase, the procedure is repeated with the safety stack extension on both the FS-W-Master and the FS-W-Device. The results for IOLWS are given in Table 1.

**Table 1.** Results for IOLW and IOLWS roaming connection times.

Attenuation “ON” [dB]	RSSI [dBm]	Minimum duration [s]		Maximum duration [s]		Mean duration [s]		Standard deviation [s]	
		IOLW	IOLWS	IOLW	IOLWS	IOLW	IOLWS	IOLW	IOLWS
30	-37	0.429	0.454	0.487	0.512	0.450	0.475	0.015	0.015
50	-53	0.429	0.454	0.487	0.512	0.452	0.477	0.016	0.016
65	-67	0.429	0.454	0.486	0.512	0.455	0.480	0.017	0.017
80	-83	0.429	0.454	1.132	1.157	0.479	0.504	0.075	0.075
83	-87	0.457	0.482	2.080	2.105	0.812	0.837	0.244	0.244
85	-89	0.438	0.463	5.913	5.938	2.883	2.935	1.390	1.410

In comparison to the IOLW roaming connect testcase with the standard IOLW stack the results measured with the safety extension show an increased connection time of approx. 25 ms in the mean due to an additional parameter

exchange phase establishing the safety connection. This difference is less dependent on the attenuation than the duration of roaming connect itself because the safety layer connection is established via process data exchange of IOLW. This means that transmission errors are detected and avoided with a residual error probability of  $10^{-9}$  [10], while these mechanisms are not yet effective in establishing the IOLW connection.

### 3.4 IO-Link Wireless Handover

For the measurement of the IOLW handover, the setup is extended with a second W-Master, as shown in Figure 3. Also, the procedure is changed to emulate the intended use-case with a handover coordinated by the higher-level controller [14]. The programmable and variable attenuator are set to the same attenuation for each series of measurements. A script running on the measuring computer controls the simultaneous and alternating pairing and unpairing via the Standardized Master Interface (SMI) of both W-Masters. The duration between loss of communication of one W-Master and the establishment of the connection to the other W-Master is measured 300 times, again with 10,000 samples per second, for each attenuation setting. A series with an attenuation higher than 80 dB respectively an RSSI lower than -83 dBm is not included for this setup, as the handover would not be successful in a reasonable time. In turn, a series of measurements with 77 dB attenuation, RSSI of -80 dBm, was carried out to better analyze the behavior in the limit range of reliable handover tests. Table 2 shows the results of this testcase. The difference to the first two testcases results from the coexistence or shared use of the IOLW configuration channels by both W-Masters, which are needed to establish the connection.

### 3.5 IO-Link Wireless Safety Handover

The setup is the same for the last testcase, but with the safety stack used on both FS-W-Masters and the FS-W-Device. The results are given in Table 2. Also in this case a nearly constant difference of approx. 25 ms between the non-safety and the safety mode due to the additional communication load can be observed.

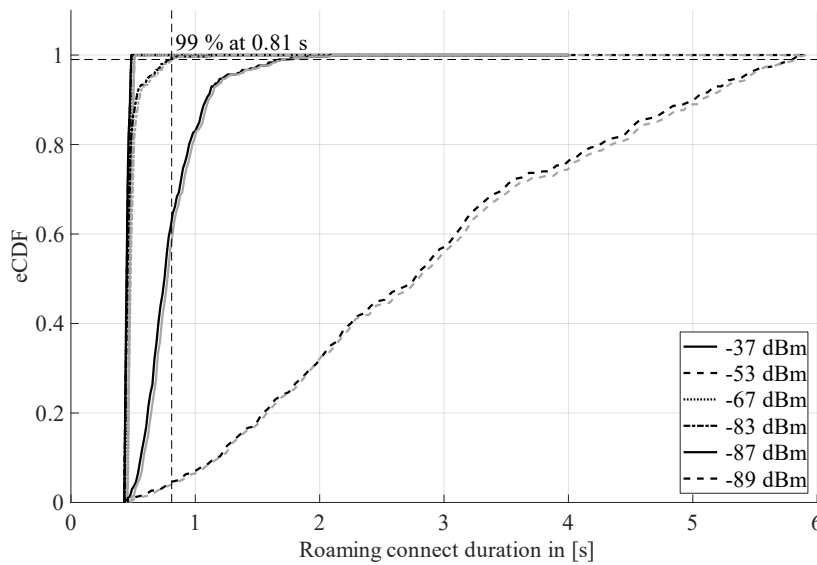
*Table 2. Results for IOLW and IOLWS handover.*

Attenuation "ON" [dB]	RSSI [dBm]	Minimum duration [s]		Maximum duration [s]		Mean duration [s]		Standard deviation [s]	
		IOLW	IOLWS	IOLW	IOLWS	IOLW	IOLWS	IOLW	IOLWS
30	-37	0.437	0.462	0.806	0.831	0.539	0.565	0.073	0.073
65	-67	0.437	0.464	2.574	2.599	0.580	0.607	0.172	0.172
77	-80	0.437	0.462	1.028	1.053	0.544	0.570	0.105	0.105
80	-83	0.443	0.469	5.736	5.761	0.977	1.002	0.892	0.892

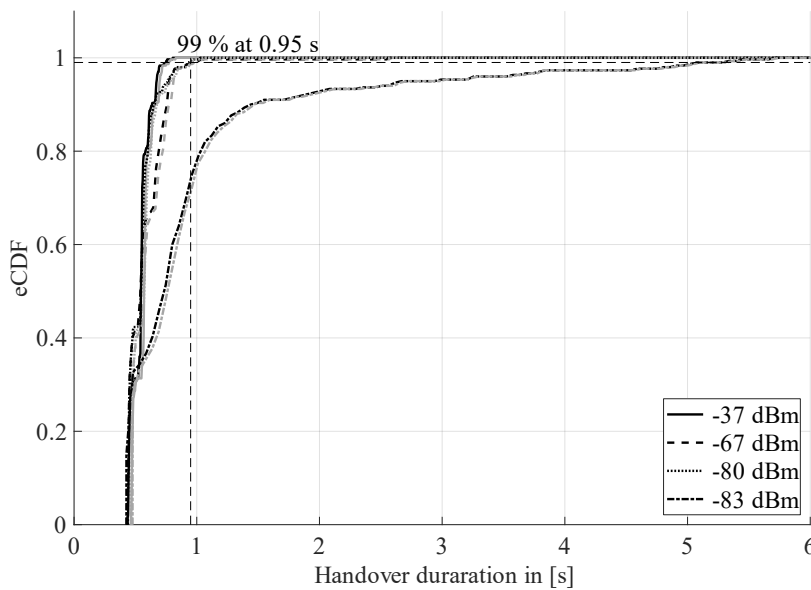
## 4 EVALUATION

The graphical evaluation for the one-sided roaming (re-)connection durations is given in Figure 4. Each line represents the connect duration for a given RSSI and safety mode as empirical Cumulative Distribution Function (eCDF). All graphs approach to one as the attenuation is chosen for successful pairing. The eCDFs for strong and moderate RSSIs are very similar and close to each other, showing that 100 % of the connections are established under 487 ms for non-safety and under 512 ms in safety mode. Pairing is also successful under poorer connection conditions, but more likely to take longer than 500 ms or even several seconds. A reference point is given at 99 % successful connections faster than 0.81 s at an RSSI of -83 dBm to mark a suitable measurement below one second. In Figure 5 the graphical illustration of Table 2 is carried out the same way. The graphs show the eCDFs of the measured durations for the handover from one (FS-)W-Master to the other in IOLW (non-safety mode) and IOLWS (safety mode) with the given RSSI. In these cases, the mean duration for good and moderate conditions is slightly increased by approx. 100 ms with some outliers up to approx. 2.6 s for the moderate condition. In contrast to establishing a single roaming connection to establish the handover connection, the original connection must be properly closed in the first step. The (FS-)W-Device is then unpaired and paired again with the other (FS-)W-Master. This causes additional delay. Another reason is the shared use of the configuration channels by both (FS-)W-Masters simultaneously. The reference point is given as 0.95 s for 99 % successful handovers at an

RSSI of -80 dBm. The average handover time nearly doubles with a decrease of the RSSI value for a stable connection by -3 dB, indicating that an RSSI of less than -80 dBm is insufficient for many applications.



**Figure 4.** Duration for roaming connect in non-safety (black) and safety (grey) mode for the given RSSI (flatter lines represent lower RSSIs).



**Figure 5.** Duration for handover in non-safety (black) and safety (grey) mode for the given RSSI.

## 5 CONCLUSION AND OUTLOOK

Under weak link conditions with up to an RSSI of -80 dBm, safe link establishment and handover can be achieved in less than one second with a success rate of over 99 %. These conditions are equivalent to the free-space path loss at a distance exceeding 67 m, while IOLW is rated for a maximum range of 10 m in industrial environments with multiple active (FS-)W-Masters. Thus, there is enough system margin available. Using IOLWS instead of IOLW adds a nearly constant offset of 25 ms and thus enables the usage of a functional safe wireless communication protocol in every use case IOLW roaming is suitable, e.g., in flexible and modular productions cells with a quick safety communication check after each line change is sufficient to re-arm the safety function. In case of a safety function response time greater than the handover duration, even a seamless handover could be possible with a sufficient signal strength. To meet safety requirements in a more dynamic and fast-moving use case further precautions are necessary. With additional location information, provided by, e.g., electronically

readable tags, light curtains or an intelligent location system, the handover can possibly be triggered at a safe moment, in a safe area or by an intelligent algorithm with movement prediction. A radio channel analyzer combined with live AI based evaluation is applicable to optimize the channel configuration of the FS-W-Masters, e.g., if not all roaming cells are needed. In an advanced and demanding application in terms of availability and timing it is also conceivable to equip one FS-W-Device with two radios to realize a seamless handover.

## ACKNOWLEDGEMENT

This research is funded by dtec.bw – Digitalization and Technology Research Center of the Bundeswehr. dtec.bw is funded by the European Union – NextGenerationEU (project “Digital Sensor-2-Cloud Campus Platform” (DS2CCP) with the project website [4]).

## REFERENCES

- [1] G. Scholl, R. Heynicke, D. Krüger, and R. Hornung, “Wireless Automation,” Proc. Sens. 2013, pp. 379–383, May 2013, doi: 10.5162/sensor2013/C3.1.
- [2] 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 2021 26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Sep. 2021, pp. 01–04. doi: 10.1109/ETFA45728.2021.9613484.
- [3] 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), Linz, Austria: IEEE, Jun. 2021, pp. 151–158. doi: 10.1109/WFCS46889.2021.9483594.
- [4] Helmut-Schmidt-University, “DS2CCP – Entwicklung einer digitalen Sensor-2-Cloud Campus-Plattform,” dtec.bw Project website. Accessed: Apr. 24, 2024. [Online]. Available: <https://dtecbw.de/home/forschung/hsu/projekt-ds2ccp>
- [5] C. Cammin, T. Doebbert, B. Solzbacher, and G. Scholl, “Concept of a 5G Hybrid Wireless Campus Network as Testbed for Industrial Applications,” in Advances in System-Integrated Intelligence, M. Valle, D. Lehnhus, C. Gianoglio, E. Ragusa, L. Seminara, S. Bosse, A. Ibrahim, and K.-D. Thoben, Eds., in Lecture Notes in Networks and Systems. Cham: Springer International Publishing, 2023, pp. 458–469. doi: 10.1007/978-3-031-16281-7\_43.
- [6] T. R. Doebbert, H. Beuster, G. Scholl, F. Fischer, and D. Merli, “Testbed for Functional Safety-Relevant Wireless Communication Based on IO-Link Wireless and 5G,” 2022, doi: 10.24405/14544.
- [7] 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, doi: 10.1109/ACCESS.2021.3128758.
- [8] T. R. Doebbert, “Contribution to IO-Link Wireless Safety–Architecture and System Extensions,” PhD Thesis, Universitätsbibliothek der HSU/UniBwH, 2024. [Online]. Available: <https://doi.org/10.24405/15290>
- [9] T. R. Doebbert, H. Beuster, G. Scholl, W. Schlögl, and P. Supavatanakul, “Contribution to Safety Extension of IO-Link Wireless,” Atp Mag., no. 9, pp. 80–86, Sep. 2023.
- [10] IEC 61139-3:2023 - Industrial networks – Single-drop digital communication interface – Part 3: Wireless extensions. International Electrotechnical Commission, Geneva, Switzerland, Jan. 11, 2023. Accessed: Jan. 24, 2024. [Online]. Available: <https://webstore.iec.ch/publication/67894>
- [11] IEC 61139-2:2022 - Industrial networks – Single-drop digital communication interface – Part 2: Functional safety extensions. International Electrotechnical Commission, Geneva, Switzerland, Aug. 19, 2022. Accessed: Jan. 24, 2024. [Online]. Available: <https://webstore.iec.ch/publication/65693>
- [12] F. Schiller, D. Judd, P. Supavatanakul, T. Hardt, and F. Wiczorek, “Enhancement of safety communication model: Preserving the black channel concept,” - Autom., vol. 70, no. 1, pp. 38–52, Jan. 2022, doi: 10.1515/auto-2021-0098.
- [13] IEC 61784-3:2021; Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions, International Electrotechnical Commission. 2021.
- [14] M. Rentschler, “Roaming in wireless factory automation networks,” in 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Sep. 2017, pp. 1–4. doi: 10.1109/ETFA.2017.8247723.